Realizing quantum-safe information sharing

Implementation and adoption challenges and policy recommendations for quantum-safe transitions

Kong, Ini; Janssen, Marijn; Bharosa, Nitesh

DOI
10.1016/j.giq.2023.101884

Publication date
2024

Document Version
Final published version

Published in
Government Information Quarterly

Government Information Quarterly 41 (2024) 101884

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions

Ini Kong *, Marijn Janssen, Nitesh Bharosa

Faculty of Technology, Policy, and Management, Delft University of Technology, Building 31, Jaffalaan 5, Delft 2628 BX, the Netherlands

ARTICLE INFO

Keywords:
Quantum-safe transition
Post-quantum cryptography
Information infrastructures
Information sharing
Digital government
Policy recommendations
Adoption
Implementation

ABSTRACT

By utilizing the properties of quantum mechanics, quantum computers have the potential to factor a key pair of a large prime number and break some of the core cryptographic primitives that most information infrastructures depend on. This means that today's widely used cryptographic algorithms can soon become unsafe and need to be modified with quantum-safe (QS) cryptography. While much work is still needed in developing QS cryptographic algorithms, the institutional, organizational, and policy aspects of transitioning the current infrastructures have received less attention. This paper provides an empirical analysis of QS transition challenges and policy recommendations for moving to a QS situation. We analyzed the data collected through interviews with experts and practitioners from the Dutch government. The results reveal that institutional, organizational and policy aspects of QS transitions are interconnected, and solutions for QS transitions are scattered. Consequently, organizations may face a *Catch-22* loop without further actionable approaches and planning for QS transitions.

1. Introduction

Since the 20th century, the significant developments of quantum theory have continuously fuelled new understandings of quantum computing research (Bohr, 1913; Feynman, 1948; Heisenberg, 1927; Planck, 1900; Schrödinger, 1926). The research on the properties of quantum mechanics is ongoing, and significant progress is being made to minimize calculation errors in quantum computers (Sood & Chauhan, 2023). One of the latest breakthroughs includes a 127-qubit Eagle quantum computer doing quantum calculations that classical computers could not manage (Daley et al., 2022; Kim et al., 2023). In 2022, IBM unveiled the 433-qubit Osprey processor, just one year after breaking the 100-qubit barrier with their 127-qubit Eagle chip.[1]

As quantum technology research accelerates, scientists across disciplines anticipate using quantum computers to tackle complex problems and unlock new frontiers of innovation. Their application can extend a wide range of fields, including, yet not limited to, AI technology, transport modelling, and solving optimization problems in the pharmaceutical and finance industry (Bova, Goldfarb, & Melko, 2021; Brooks, 2023; de Wolf, 2017; Dowling & Milburn, 2003; Ménard, Ostojic, Patel, & Volz, 2020).

At the same time, the development of quantum computers also poses security threats to critical information infrastructures in various sectors, including public services, telecommunication, financial services, electric power grids, and many other cyber-physical systems and services (Covers & Doeland, 2020; Krause, Ernst, Klaer, Hacker, & Henze, 2021; Lewis & Travagnin, 2022).

Peter Shor presented one of the first practical uses for a quantum computer in 1994 (Shor, 1994). Shor presented a quantum algorithm that – assuming the availability of a powerful enough quantum computer - could be exponentially faster than a classical computer at finding the prime number factors of large numbers.

Today, these primes are the secret keys that keep most of the encrypted information sent over the internet confidential. As the number of qubits increases, so does the quantum threat – using Shor's algorithm to break the confidentiality, integrity and availability safeguarded by current cryptographic systems (Grover, 1996; Shor, 1994). Moreover, a recent improvement of Shor's algorithm, known as Regev's algorithm, could be more efficient than 30-year-old Shor's algorithm, demanding fewer qubits to hack internet encryption (Kramer, 2023).

Various efforts are being made to protect critical information infrastructures across academia, industries, and government. An important initiative is the standardization of *quantum-safe* (QS) cryptographic

* Corresponding author.
E-mail addresses: i.kong@tudelft.nl (I. Kong), m.f.w.h.a.janssen@tudelft.nl (M. Janssen), n.bharosa@tudelft.nl (N. Bharosa).

[1] https://www.ibm.com/quantum/roadmap.

https://doi.org/10.1016/j.giq.2023.101884
Received 17 February 2023; Received in revised form 18 October 2023; Accepted 8 November 2023
Available online 24 November 2023

algorithms, an ongoing effort coordinated by the National Institute for Standards and Technology (NIST). A recent publication by NIST (2022) announced the list of QS cryptographic algorithms from the third round of the standardization process (e.g., CRYSTALS-KYBER for public key encryption, and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures).

Yet, it is unclear which of these algorithms will survive the testing phase and be implemented in hardware and software solutions. Due to backward compatibility and interoperability issues, a simple 'drop-in method' of new QS algorithms may not be feasible in the existing infrastructures (Barker, Souppaya, & Newhouse, 2021; Bernstein & Lange, 2017; NIST, 2021). There are many uncertainties regarding QS algorithms.

Moreover, the recent discussions at the White House indicate that preparatory steps are needed for agencies to begin QS transitions (The White House, 2022). In Europe, the European Commission announced a new call on the transition towards QS cryptography as a part of the Horizon Europe Framework Programme (European Commission, 2022). In the Netherlands, the Dutch General Intelligence and Security Service has recently published a generic migration manual for QS transition, recognizing the importance of protecting public and private organizations (AIVD, 2021; NCTV, 2022; TNO et al., 2023).

As the topic of QS transition begins to surface in governments, it raises awareness about the complexity of implementing and adopting QS solutions in the current critical information infrastructures (Kong, Janssen, & Bharosa, 2022). Here QS solutions refer to a range of technical solution components, including QS cryptographic algorithms, as well as software and hardware components that can run these QS algorithms. While the standardization of QS cryptographic algorithms is not yet finalized, multiple actors with varying urgency, interest, and expectations facilitate the infrastructures (Lovic, 2020; Tibbetts, 2019; TNO, 2020; Vermaas, 2017). For organizations, there is a lack of clarity on addressing socio-technical predicaments when implementing and adopting QS solutions.

While much attention is given to the development of QS cryptographic algorithms, there is a lack of research on institutional, organizational, and policy aspects of QS transition (Giron, 2023; Joseph et al., 2022; Käppler, Schneider, & Bettina, 2022; Kumar, 2022). The research objective of this paper is threefold: i) to identify implementation and adoption challenges that organizations may encounter, ii) to validate challenges with a series of interviews empirically, and iii) to provide policy recommendations. The main academic contribution is the empirically grounded assessment of transition challenges, solution directions and policy recommendations that can inspire theory building on QS transitions.

The paper is structured as follows: Section two presents a background on critical communication infrastructures and QS transition. Section three discusses the research approach. A long list of QS transition challenges is presented in section four. Section five discusses the results of the interview and further extends the discussions. Finally, section six presents the main conclusions and provides some directions for future research.

2. Background

This section is divided into three parts. The first part scrutinizes the importance of asymmetric cryptography in facilitating secure information sharing. The second part delves into quantum threats in critical information infrastructure, and the third part further explains solution areas for quantum-safe (QS) cryptography.

2.1. Asymmetric cryptography in secure information sharing

An ever-increasing dependency on secure information sharing has made critical information infrastructures vital for governments and industries (Kong, Janssen, & Bharosa, 2023). There are dozens of examples of critical information infrastructures, including digital infrastructures supporting tax filing and customs declarations, border control, electricity distribution, traffic control, internet services, banking and online payments, and so on. These types of infrastructures are critical for the functioning of societies. Therefore, these infrastructures' security (e.g., confidentiality, integrity and availability) is imperative.

Encryption algorithms can prevent unauthorized parties from accessing sensitive and vulnerable data to maintain security (Adams & Lloyd, 1999; Linn, 2000). The cryptographic keys, randomly generated characters' strings, are used in encryption algorithms, and the decryption time can be affected by the length of these cryptographic keys. Depending on different features of cryptography, the keys used to encrypt the data may or may not be used to decrypt it (Linn, 2000). Two different types of cryptographic keys (e.g., symmetric cryptography and asymmetric cryptography) are shown in Fig. 1.

In symmetric cryptography, data is encrypted and decrypted using the same key that is shared. The shared key must remain private, and the complexity of the key strengthens the cryptographic algorithm (Adams & Lloyd, 1999; Hunt, 2001). However, distributing the keys in private is difficult in symmetric encryption, which makes it impractical for widespread commercial use. In asymmetric cryptography, also known as Public Key Cryptography (PKC), data is encrypted and decrypted using a key pair that is mathematically tied together. PKC consists of one public key that must be verifiably authentic and one private key that must remain private (Adams & Lloyd, 1999; Hunt, 2001). The encrypted information can only be decrypted by the private key corresponding to its public key. Unlike symmetric cryptography, using different keys for encryption and decryption for asymmetric cryptography addresses the key distribution problem. Many critical information infrastructures employ asymmetric cryptographic systems to facilitate secure information exchange and digital network communication.

2.2. Quantum threats to secure information sharing

While multiple security vulnerabilities are coming from malicious software updates and data breaches, the introduction of quantum computers poses a new level of security threats to critical information infrastructures. The foundational layer with cryptographic primitives and encryption algorithms that provide the security of infrastructures may no longer be reliable.

By utilizing the properties of quantum mechanics, factoring a key pair of large prime numbers may no longer be difficult for quantum computers. Using Shor's Algorithm, a quantum computer can perform calculations and analyze complex cryptographic keys much faster than today's computers. Thus, the computation power of quantum computers can potentially break the widely known PKC schemes such as Rivest-Shamir-Adleman (RSA), Diffie-Hellmann key exchange (DHKE), and Elliptic Curve Cryptography (ECC) (Csenkey & Bindel, 2023; Mosca & Piani, 2022; Paar & Pelzl, 2010; Shor, 1994). A recent article on *Science* discussed Oded Regev's work, who proposed a method of multiplying numbers with different dimensions that may substantially improve Shor's algorithm and break the encryption faster with fewer qubits (Kramer, 2023; Regev, 2023). For other cryptographic algorithms not affected by Shor's Algorithm, quantum computers can use Grover's algorithm to speed up the search process to decrypt the encryption (Grover, 1996).

Once current PKCs become compromised, critical information infrastructures' confidentiality, integrity, and availability (CIA) can no longer be guaranteed (NSA, 2022). This also means that any damage, vulnerability, or unavailability of one critical information infrastructure (e.g., public services or telecom) can bring cascading risks to other critical infrastructures (e.g., health or banking). While the noise surrounding quantum technologies and the reality of developing useful quantum computers come with multiple uncertainties, *Store Now, Decrypt Later* attacks can already occur today without needing large-

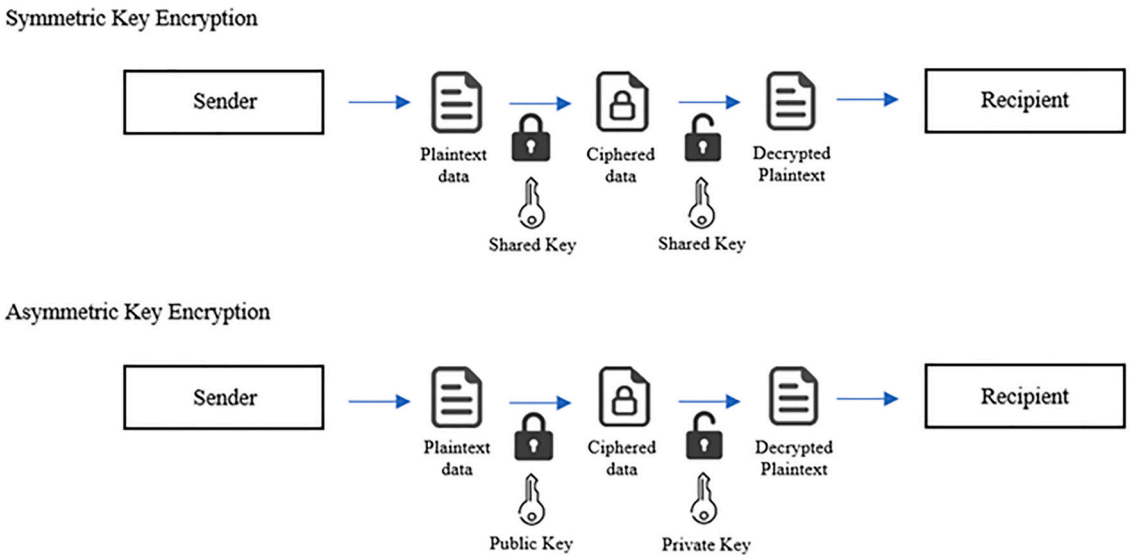

Fig. 1. Symmetric cryptography vs. asymmetric cryptography.

scale quantum computers (Mavroeidis, Vishi, Zych, & Jøsang, 2018; Mosca & Piani, 2022; NIST, 2021). Data that must remain confidential for the next 10–20 years (e.g., healthcare, finance, and national security information) can be harvested, stored, and decrypted later once quantum computers become available (AIVD, 2021; McKinseyDigital, 2022; Mosca, 2015).

2.3. Quantum-safe solutions & QS transition

Although it is uncertain when quantum computers will be strong enough to break PKC schemes, modifications are now being studied to replace the existing PKCs with ones resistant to quantum computers. Two different solution areas for quantum-safe (QS) cryptography are currently being researched.

The first QS solution area is called *Quantum Key Distribution* (QKD), which uses the properties of quantum physics called quantum bits (qubits) (Gibney, 2019; Hong, Foong, & Low, 2016). The unique properties of qubits, such as *Superposition* and *Entanglement,* provide QKD with the possibility of creating unbreakable algorithms (Gibney, 2019; Hong et al., 2016). While *Superposition* can represent 0 and 1 simultaneously, which allows more operations to be performed at the same time, *Entanglement* shows that two particles are connected, reflecting each other and sharing a physical state despite the physical distance that separates them (Brooks, 2023; Gibney, 2019). Since any external interference (e.g., man-in-the-middle attack, side-channel attacks, etc.) in generating and distributing QS cryptographic keys can destroy the quantum states, which can allow users to detect the interference, QKD has the potential to provide a new approach to security over networks. However, at the time of writing, QKD cannot yet be used for QS solutions as it requires quantum communication infrastructures with specialized equipment and fibre optic cables (Lovic, 2020; NSA, 2022; QED-C, 2021; Yunakovsky et al., 2021). This may be impractical for critical information infrastructures with complex and interconnected systems of multiple organizations. Thus, more research is needed for the QKD approach to secure the entire infrastructure beyond generating and distributing QS keys (NSA, 2022; QED-C, 2021).

The second area of QS solutions is called *Post Quantum Cryptography* (PQC), which suggests upgrading the existing PKC using technologies such as code-based cryptosystems, lattice-based encryption, and hash-based digital signatures (Bernstein & Lange, 2017; NIST, 2021). Since 2016, the National Institute for Standards and Technology (NIST) has initiated the selection process for PQC to standardize quantum-safe (QS) solutions (NIST, 2016, 2022). The list of PQC for standardization from a recent publication from NIST (2022) includes CRYSTALS-KYBER for public key encryption and CRYSTALS–Dilithium, FALCON, and SPHINCS+ for digital signatures (NIST, 2022). While the first PQC standards are expected to be completed in 2024, NIST has advised organizations to explore these algorithms and practical use cases in their applications (NIST, 2022). The QS solutions for critical information infrastructure must facilitate key exchange mechanisms and encryption and perform authentication and digital certification (Amadori, Duarte, & Spini, 2022). Thus, algorithm selection, compatibility, and the performance of PQC solutions must be closely monitored.

Although this paper recognizes the potential of QKD as a QS solution, we only focus on PQC as a QS solution. QKD is not feasible yet, and PQC is already moving towards standardization, implementation, and adoption (Amadori et al., 2022;NIST, 2022; TNO et al., 2023). Going forward, several options for using QS cryptographic algorithms based on PQC exist, and many implementation decisions are still to be made (NIST, 2021, 2022). While technological dependencies among actors make QS transition complex, it is not yet clear how the cryptographic layer of existing systems should be modified (NIST, 2022; TNO et al., 2023).

3. Research methodology

Although there is much research on the technical aspects, less attention has been given to the implementation and adoption challenges of QS solutions in organizations and the policies needed to realize the transition to PQC. Drawing on these knowledge gaps, we formulated two research questions to help us understand the practical challenges and identify policy recommendations for QS transition.

RQ1. What are implementation and adoption challenges for QS transitions?

RQ2. What are policy recommendations for QS transitions?

The first research question examines QS transition challenges in practice by interviewing experts and practitioners to empirically validate the list of challenges found in the literature. The second research question seeks to identify policy recommendations that may help address QS transition challenges in practice.

For our study, we conducted semi-structured interviews to triangulate our data collection process qualitatively. Triangulation is a well-recognized technique in research methodology, allowing for a more thorough understanding of our research context and reducing biases in the research (Heale & Forbes, 2013; Lowery & Evans, 2004). Prior to the interviews, a wide variety of data was collected from documents (e.g.,

policy documents, grey literature, and white papers). By utilizing cross-reference information from the data triangulation process, the robustness of our data is ensured, and the depth of data analysis is strengthened.

3.1. Scope: public key infrastructure

Many critical information infrastructures use *Public Key Infrastructures* (PKIs) for ensuring secure digital communication and information sharing (Kong et al., 2023). To verify users' authenticity, digital certificates that consist of PKC and digital signatures act as digital passports over networks (Bindel, Herath, Stebila, & McKague, 2017; Mosca, 2015). These digital certificates are issued from a certification path formed under the Root Certificate Authority (Root CA) with all the intermediate CAs chained together (Bharosa, van Wijk, de Winne, Janssen, & Eds.)., 2015). Once the self-signed Root CA certificate is established, the Root CA-signed certificate is issued to intermediate CAs, which are trusted by lower-level CAs (Linn, 2000). The lowest layers of CAs issue certificates to people, applications, or devices. The certificate path in a CA hierarchy is illustrated in Fig. 2.

By managing these digital certificates, PKI provides strong credentials for digital identity management (Bharosa et al., 2015; Hunt, 2001; Linn, 2000). Through the process of verification, issuance, and revocation of digital certificates, a security framework of PKI ensures a high degree of authentication, message integrity, and non-repudiation (Adams & Lloyd, 1999; Danquah & Kwabena-Adade, 2020; Huang & Nicol, 2017; Hunt, 2001; Nazario & van Oosten, 2001). All aspects of information sharing between government-to-government, government-to-business, government-to-citizens, and business-to-citizens rely on the secure functioning of PKIs.

As governments increasingly use Information Communication Technologies (ICT) and networks to provide accessible governmental information and efficient public services, PKIs have become an essential part of the public sector, enabling user authentication, message integrity, and message non-repudiation services (Innovalor, 2019; Kong et al., 2022). Examples range from sharing information on public policy, regulations, government documents, and forms to maintaining services, filing taxes, applying for permits, study loans, and social benefits, using PKIs (Coursey & Norris, 2008; Jansen & Ølnes, 2016; Lindgren & Jansson, 2013). Fig. 3 illustrates secure information sharing in government using PKI. In the Netherlands, the main governmental PKI - known as PKIoverheid - provides strong credentials for information sharing using PKIoverheid certificates (Innovalor, 2019; Logius, 2020). PKIoverheid certificates support various functions, from the authentication of users and organizations and signing documents using digital signatures to setting up digital tunnels for secure message exchange.

Logius acts as Policy Authority (PA) and manages service providers that issue and revoke digital certificates for PKIoverheid (Innovalor, 2019; Logius, 2020; NCSC, 2020). With the government as a frontrunner in managing and regulating the facilitation of a national and cross-sectoral PKI system, the case of PKIoverheid is selected in the paper to examine implementation and adoption challenges for QS transition and propose policy recommendations. All public service provisioning and many information-sharing efforts depend on PKIoverheid. PKIoverheid is essential for the proper functioning of other infrastructures that provide maintenance, reliability, and safety in government communication and service delivery processes. Likewise, there is a high dependency on PKIoverheid, which – like other PKIs – has a high vulnerability to quantum threats. To identify practical challenges that organizations may encounter and policy recommendations for QS transitions, purposive sampling is used to select organizations that are part of the PKI systems in the Dutch government that use government certificates.

3.2. Data collection

Since we focused on examining the practical challenges of QS transition with institutional, organizational and policy aspects, we conducted semi-structured interviews. Semi-structured interviews are used as a data collection method to ask questions within a predetermined thematic framework. While the interviewer prepares a set of questions to guide the conversation, more in-depth information about a particular topic can also be discussed in open-ended responses from interviewees (Creswell, 2018). The interviews facilitated an in-depth discussion about the challenges and opportunities of a QS transition. We used purposive sampling and identified 12 respondents in the Netherlands. The main selection criteria of industry experts and practitioners is their involvement in the PKIoverheid system and the prior knowledge affiliated with the topic of QS transition and the security of PKI systems. The number of potential respondents was limited as there are only a few experts in this area. The list of respondents is shown in Table 1; the list contains all the key persons involved in the government with PKI systems and QS transitions.

The interview was structured in three parts. First, we asked the respondents to introduce themselves and their organizations. This part of the interview showed the relevance of their experience and knowledge related to PKIs. The interviews were categorized between regulatory organizations, PKI users, and external experts providing PKI-related services and products. Second, we asked respondents for a general understanding of QS transition and challenges that may hinder the transition from the current PKIs. This was done to introduce QS transition topic and allow respondents to share their views on QS transition openly. Third, we showed the list of challenges found in the literature and asked the respondents whether they saw the challenges as relevant to their organizations. This step allowed respondents to provide in-depth responses and extend their views on QS transition challenges and opportunities needed to realize the transition to PQC.

3.3. Data analysis

The interviews were transcribed, and the documented transcripts of the interviews were uploaded to the program called ATLAS.ti to review and verify collected data sources in the process. We followed the Human

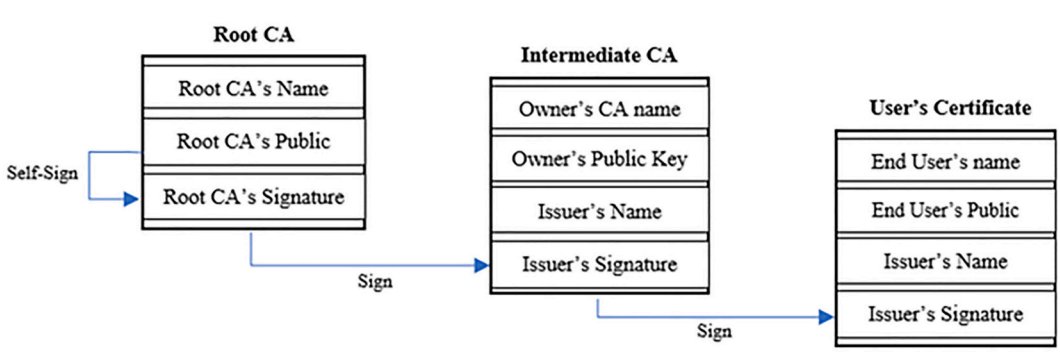

Fig. 2. Certification path in a CA hierarchy.

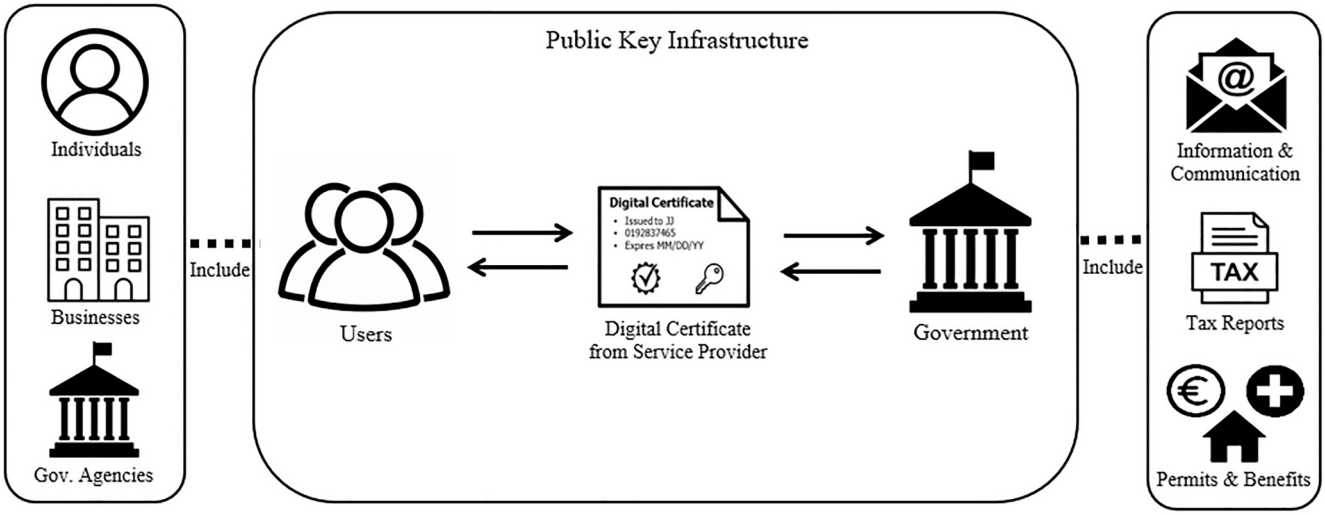

Fig. 3. Secure information sharing using public key infrastructure.

Table 1
List of respondents for the interviews.

Respondent #	Role	Organization	Perspective
1	Chief Architect	Government Agency	Regulatory organization
2	Information Sharing Architect	Bank	PKI user
3	Change Manager	Government Agency	Regulatory organization
4	Policy Officer	Government Agency	PKI user
5	Strategic Advisor	Research Institute	External experts
6	Chief Technology Officer	Service Provider	External experts
7	Architect	Tax Office	PKI user
8	Cryptographer	Research Institute	External experts
9	Policy Coordinator	Government Agency	Regulatory organization
10	General Manager	Software Company	External experts
11	Software Developer	Software Company	External experts
12	Vice President of Operations	Service Provider	External experts

Research Ethics Committee (HREC) ethical guidelines to protect participants' privacy. The dataset has been anonymized to eliminate any personally identifiable information such as names, addresses and affiliated organizations to reduce the risk of exposing individual's personal information. The initial analysis of the interviews was conducted by identifying relevant parts and open-coding these parts to the object of the study (Saldaña, 2013; Williams & Moser, 2019). Then, these parts were reread to extract relevant phases to understand QS transition more in-depth. The relevant phrases from the data were further abstracted into codes on ATLAS.ti by open coding. Through an interpretive process on the part of the researchers, categories of codes emerged for QS transition challenges and opportunities. The researchers prioritized making sense of QS transition challenges and opportunities by capturing the original language of respondents from their quotes. After a series of discussions, researchers further refined the categories of challenges for QS transition and clustered the list of policy opportunities that emerged throughout the interviews.

4. Long list QS transition challenges

We used the list of challenges previously identified in the literature to conduct the interviews. We used 12 challenges to guide our interviews because we wanted 1) to have sufficient interview time to discuss in-depth challenges in different technological, organizational and environmental contexts and 2) to provide more exploration for respondents to identify relevant and missing challenges in their field of practice. The challenges used in the interviews are marked in (X) in Table 2.

5. Results

Section 5 discusses the results of the interviews with experts and practitioners. Section 5.1 presents the categories of the main challenges for QS transition, whereas Section 5.2 provides the categories of policy opportunities that may address QS transition challenges.

5.1. Overview of main challenges

This section presents the challenges for QS transition clustered in four categories, which are 1) complex PKI interdependencies, 2) lack of urgency, 3) lack of certified hardware and software, and 4) unclear QS direction and governance.

5.1.1. Complex PKI interdependencies

One of the challenge categories for QS transition is complex PKI interdependencies. The issued digital signatures and certificates from PKIs are checked and validated by software implemented by market parties. The external experts providing products and services for PKIs also monitor communities of all the browser companies to discuss changes in PKIs (Respondent 1). The services they deliver need to be accepted by these parties and various standard bodies such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), European Telecommunication Standards Institute (ETSI), and NIST (Respondent 6). While external experts provide software to govern and manage certificates (abiding by European laws), the facilitation of PKIs must consider the whole certificate chain, which involves Root CA and all the intermediate CAs (Respondent 6). If the encryption level of the Root changes, all underlying certificates in the same stack would need to be revoked and reissued since they do not automatically inherit the new specification (Respondent 5). One of the external experts stated that,

> "If PKI systems use different encryption levels like classical cryptographic algorithms and PQC, the Root CA, intermediate CAs, user

Table 2
Overview of the challenges categorized in technological, organizational & environmental context.

Context	Challenges	References
Technological Context	Incompatible Legacy System (X)	(The Hague Security Delta, 2019), (ISARA, 2018), (Machatan & Heintzman, 2021), (Wiesmaier et al., 2021), (Lindsay, 2020b), (Accenture Labs, 2018), (CSIRO, 2021), (CCC, 2019), (Vermeer & Peet, 2020)
	Not-yet mature Standards from NIST	(NIST, 2021), (Accenture Labs, 2018), (CCC, 2019), (Niederhagen & Waidner, 2017), (Menezes & Stebila, 2021), (ENISA, 2021)
	No Universal QS Algorithm (X)	(NIST, 2016), (NIST, 2021), (CCC, 2019), (Vermeer & Peet, 2020), (ENISA, 2021), (Chen & Moody, 2020)
	Implementation Flaws and Side-channel Attacks	(Wiesmaier et al., 2021), (Menezes & Stebila, 2021), (Niederhagen & Waidner, 2017), (Macaulay & Henderson, 2019)
	Lack of Reliability in QS Cryptography	(ISARA, 2018), (CCC, 2019), (Vermeer & Peet, 2020), (Macaulay & Henderson, 2019), (Tibbetts, 2019), (ETSI, 2015)
	Vulnerable Root CA (X)	(ISARA, 2018), (Menezes & Stebila, 2021), (Thales, 2019), (Sjöberg, 2017), (Macaulay & Henderson, 2019), (ETSI, 2020)
	Complex PKI system & Interoperability (X)	(NIST, 2021), (ISARA, 2018) (Accenture Labs, 2018), (CSIRO, 2021), (CCC, 2019), (Vermeer & Peet, 2020), (ENISA, 2021), (Macaulay & Henderson, 2019), (Grote, Ahrens, & Benavente-Peces, 2019)
	Cost of Transition	(TNO, 2020), (ISARA, 2018), (Vermeer & Peet, 2020), (ETSI, 2015), (Thales, 2019), (NIST, 2018), (Petrenko, Mashatan, & Shirazi, 2019), (Ma, Colon, Dera, Rashidi, & Garg, 2021)
Organizational Context	Lack of Urgency (X)	(Lovic, 2020), (TNO, 2020), (Lindsay, 2020b), (Vermeer & Peet, 2020), (ETSI, 2015)
	Knowledge Gaps in Quantum Computing (X)	(Mulholland, Mosca, & Braun, 2017), (TNO, 2020), (CCC, 2019), (Niederhagen & Waidner, 2017), (Macaulay & Henderson, 2019), (Ma et al., 2021), (Vermaas, 2017)
	No one-size-fits-all Transition Process	(NIST, 2016), (NIST, 2021), (TNO, 2020), (CSIRO, 2021), (CCC, 2019), (ENISA, 2021), (ETSI, 2020), (Ma et al., 2021), (ETSI, 2017)
	Lack of Crypto-Agility	(NIST, 2021), (Wiesmaier et al., 2021), (Macaulay & Henderson, 2019), (ETSI, 2015), (ETSI, 2020), (Grote et al., 2019), (Ma et al., 2021), (Mehrez & Omri, 2018)
	Lack of In-house Management Support (X)	(Mosca, 2015), (The Hague Security Delta, 2019), (CCC, 2019), (NIST, 2018), (Buchholz, Mariani, Routh, Keyal, & Kishnani, 2020)
	Unclear QS Transition Benefits & Business Case	(Mosca, 2015), (Ménard et al., 2020), (The Hague Security Delta, 2019), (CSIRO, 2021), (Vermeer & Peet, 2020)
	No Technical Skills & Qualified Personnel	(TNO, 2020), (CSIRO, 2021), (NIST, 2018), (Peterssen, 2020)
	Unclear QS Governance (X)	(Mulholland et al., 2017), (NIST, 2021), (The Hague Security Delta, 2019), (Machatan & Heintzman, 2021), (Wiesmaier et al., 2021), (CSIRO, 2021), (Niederhagen & Waidner, 2017)
Environmental Context	Low level of Investment in the EU	(Ménard et al., 2020), (CCC, 2019), (Rasanen, Makynen, Mottonen, & Goetz, 2021), (Lewis & Travagnin, 2018), (Lewis, Ferigato, Travagnin, & Florescu, 2018)
	Lack of Awareness (X)	(Mulholland et al., 2017), (Lovic, 2020), (TNO, 2020), (Vermeer & Peet, 2020), (Macaulay & Henderson, 2019), (ETSI, 2015)
	No Clear Ownership & Operating Institution (X)	(Mulholland et al., 2017), (NIST, 2021), (Lindsay, 2020b), (Ma et al., 2021), (Lindsay, 2020a)
	Different Interpretation of QS Scenarios	(NIST, 2021), (ENISA, 2021), (Vermaas, 2017), (ETSI, 2017), (Smith, 2020)
	Lack of Policy Guidance (X)	(The Hague Security Delta, 2019), (Lovic, 2020), (Tibbetts, 2019), (Lewis & Travagnin, 2018), (Lewis et al., 2018), (Lindsay, 2020a), (Lewis, 2017)
	Need for Various Stakeholders (X)	(Mulholland et al., 2017), (The Hague Security Delta, 2019), (CCC, 2019), (Vermeer & Peet, 2020), (Chen & Moody, 2020), (Rasanen et al., 2021)
	Legal Issues	(Niederhagen & Waidner, 2017), (Ma et al., 2021), (ETSI, 2017), (Lewis, 2017)
	Bureaucratic Process	(Macaulay & Henderson, 2019), (Lewis & Travagnin, 2018), (Lindsay, 2020a)

> certificates, and a whole ecosystem behind may be affected, causing complex integration issues." (Respondent 12)

Due to the interdependencies in PKIs, organizations with old encryption levels and organizations with new encryption levels might not be interoperable. Since PKIs allow different organizations and entities to communicate securely, maintaining technical interoperability allows users to share information and use digital transactions over networks. The linkages facilitating PKI systems create inherently complex interoperability challenges (Respondent 8). Any changes in the current PKI systems for QS transition also need to consider the technical interdependencies that PKIs inherently have.

Moreover, PKI systems are heavily regulated (e.g., eIDAS regulations) and must comply with international standards (e.g., NIST, ETSI, X.509 standards, etc.). Since PKI in the Netherlands is ruled by laws and regulations, changes in the technical foundation of digital certificates cannot occur in isolation.

> "Organizations are not completely free to choose what they want and change the PKI systems." (Respondent 8)

Parties that provide PKI-related products and services for the Dutch government must follow international standards and EU regulations and meet the Programme of Requirement (PoR) to be recognized as service providers in the Netherlands (Respondent 9). The activities of these service providers are monitored, and audit communities also check the quality of PKI-related products and services (Respondent 9). Since new standards and regulations for QS solutions are not yet available for QS transitions, organizations find it challenging to modify the current PKI systems that are already compliant with existing standards and regulations.

5.1.2. Lack of urgency

Another challenge category for QS transition is a lack of urgency. Although the topic of QS transition has emerged in the public domain,

the respondents indicated that the level of urgency remains low. While regulatory organizations indicated a growing awareness, PKI users such as government agencies and banks do not have the same level of urgency (Respondent 1). One of the respondents pointed out that,

> "We expect only to come in 10 or 15 years. And that's far away. So the time horizon of an average bank for calculating security issues is about three years." (Respondent 2)

In the case of quantum threats, the respondent states that it is unlikely for such threats to occur tomorrow. The risk appetite was different for PKI users. Some think that a time horizon of 10–15 years can be considered not urgent, but there is disagreement about the time horizon. Likewise, government agencies using PKI systems did not see the urgency in their organizations. In their views, the high urgency would only mean that PKI systems would no longer work tomorrow (Respondent 7).

Moreover, there is a lack of understanding of what a QS transition means for organizations. While it may be impossible for organizations to opt for QS transition decisions to be single-handled by one organization, respondents stated that knowledge of quantum threats and PKIs is mainly missing in non-experts, and organizations are not aware of the technical complexity that PKIs inherently have.

> "If you 'don't understand, there will be no urgency because you don't understand the threat, what it does, or what impact it has. First, you need to understand." (Respondent 4)

The respondent from the regulatory organization also indicated that the QS transition topic is difficult for policy-makers to grasp. Even though the facilitation of PKIs is essential in securing businesses and public services in society, the level of fuzziness in quantum threats does not provide a clear view for policymakers to recognize the risks associated with PKIs (Respondent 9). The respondent added that it does not help when experts disagree because it would only make regulatory organizations not proceed with QS transition simply because experts do not agree. Nothing has yet been decided for QS transition (Respondent 9).

In addition, the urgency among different organizations is considered a challenge when the level of urgency varies in the PKI systems. While the level of urgency remains low in the PKI ecosystem as a whole, many organizations have varying levels of risk appetite and do not see the consequence of not transitioning to quantum-safe (Respondent 12). While there is a lack of understanding and knowledge on the topics of QS transition, the respondents also stated that the level of urgency might also differ for small government agencies and SMEs since they do not have enough resources to recognize quantum threats and the need for QS transition (Respondent 5).

5.1.3. Lack of certified hardware and software

The third challenge category for QS transitions is the lack of certified hardware and software. Suppose there are new updates in hardware and software. In that case, PKI service providers and PKI users in critical information infrastructures need to adopt new solutions to maintain interoperability and backward compatibility. In the case of QS transition, a hybrid structure that works with both classical cryptographic algorithms and QS solutions (e.g., PQC) is under discussion.

> "We could also look for a hybrid approach where we deliver both the old and new format or come up with a mixed format." (Respondent 6)

Having a hybrid structure would also mean that certified hardware and software may need to recognize two different encryption levels in the X.509 scheme (Respondent 5). Since the current PKI systems only recognize classical cryptographic algorithms, there is a need for hardware and software that can replace the existing systems. The current PKI systems for regulatory organizations require an HSM (Hardware Security Module) and a hybrid data model to issue certificates recognizing two different encryption levels, including classical cryptographic algorithms and QS solutions (Respondent 1).

> "For us, 'it's quite simple. We just need two things. We need to have like an HSM, We need to have a hybrid data model to create these new keys."(Respondent 1)

While the respondent emphasized that QS transitions for regulatory organizations are relatively easy, it may be difficult for PKI users such as banks, the tax office and other government agencies to change their systems (Respondent 1). This is because no currently certified hardware and/or software can run QS solutions yet. The respondents from external experts agreed that the development of certified products that implement QS solutions has not yet happened, and this would be a big challenge for organizations that need to change their systems.

> "QS transition is often compared to the transition from SHA-1 to SHA-2, but the difference would be that QS transition does not have hardware and software ready." (Respondent 6)

> "For the transition, we are very dependent on our suppliers. We cannot transition without them." (Respondent 11)

Moreover, another respondent from PKI users also indicated a lack of technical expertise and qualified personnel with the knowledge and experience to work with the hardware and software for QS transition (Respondent 7). Getting to certified products that support QS solutions, there may need to be some judgment that it is safe enough to rely on these new products in practice. This also requires a certification process that can be pretty intensive and time-consuming (Respondent 6). However, the standards for new QS solutions are not yet agreed upon. Commercial software providers also need to leverage those new specific algorithms to ensure that their software can generate certificates using the new QS encryption scheme. This is because service providers' existing commercial software only used classical encryption levels. This would not support the post-quantum encryption level (Respondent 12). There is a lack of technical expertise and qualified personnel who understand how the process of a QS transition works (Respondent 5). For PKI users who need to sign their emails and contracts, users of notary services, and organizations that use custom software to perform specific types of work, new certified hardware and software that can run QS algorithms are not yet available (Respondent 12).

5.1.4. Unclear QS direction and governance

The fourth challenge category of QS transition is unclear QS direction and governance. The respondents stated that organizations currently do not have directions for QS transition. The respondents from the PKI users category stated that organizations are all monitoring the development of QS solutions (which have not yet been finalized) and remain conservative towards the QS transition because security issues in the current PKI systems have not yet occurred.

> "Organizations are keeping their eyes on the development. They do not have an actual QS transition strategy or other actions that they have planned." (Respondent 7)

Within organizations, modifying PKI systems is considered as "under the hood" changes by the IT department, which often go unnoticed in user functionality (Respondent 7). Another respondent also emphasized that it would be more challenging for SMEs with insufficient resources to transit to QS PKI systems without recognizing the impact of quantum threats (Respondent 2). As long as the security remains status quo, no issues have emerged in the current PKI systems for organizations. Thus, without recognizing the impact of quantum threats in organizations, it is challenging to realize the scope of QS transition and organize what changes may be needed. The respondents also agreed that it might be easier for homogenous organizations, such as banks, to plan for a QS transition with the ECB as a regulator and DNB (Dutch National Bank) in the Netherlands. However, the respondent also emphasized that the direction for a QS transition is not yet available in the sector

(Respondent 2).

For regulatory organizations, IT and government in the Netherlands are very decentralized, and every ministry has responsibility for certain executive agencies falling under that ministry (e.g., energy, water management, education, national security, etc.) (Respondent 9). Mobilizing the governance of PKI systems to proceed with a QS transition may take a lot of time and requires convincing non-technical people (Respondent 9). The respondents agreed that the changes in the current PKI systems may extend to other critical infrastructures. However, there is no clear path to where and what to do with which technology.

> "It's very difficult on our operational level to organize change because we are waiting for the instructions on what to do." (Respondent 3)

Although PKIs have evolved immensely over the past decades, previous experience has shown that modifications in the PKIs are complex. Without a clear governance, it would be difficult for organizations to proceed with changes in the current PKI systems. For external experts, having organizational-level governance was not an issue. Since PKI-related changes are part of their core business, they stated that a governance structure is in place to address changes. However, they saw the most significant risk in cross-organization-level governance. Although Logius acts as a Policy Authority (PA) and manages the PKI system for the PKIoverheid certificates, the coordination and accountability for the QS transition remain unclear, and organizations were unsure of their roles and responsibilities. (Respondent 4).

> "It is not yet clear enough who is doing what and the main risks are cross-organizational." (Respondent 6)

> "Someone has to make costs to facilitate. Who is taking the burden? What will it do to the whole ecosystem?" (Respondent 10)

Since the facilitation of PKI systems requires multiple actors to secure information sharing and digital transactions, cross-organizational governance is crucial for the QS transition. However, no specific document provides guidelines and no national roadmap to move along the QS transitions.

> "The organizations do not know who is making the decisions for QS transition and who are collaborating, who to include paying for the cost of transition." (Respondent 5)

hile the existing PKI governance indicates a set of roles, security policies, encryption mechanisms, and procedures with diverse actors. This is not suitable for a QS transition since it requires clear responsibilities to follow and priority setting given scarce resources. With varying levels of urgency, interest and expectations for QS transition, organizations are waiting for each other, and it is unclear who should make the first moves (Respondent 8).

Table 3 shows various implementation and adoption challenges that organizations may encounter, and many uncertainties fuel QS transition challenges. The four categories of QS transition challenges also show institutional, organizational and policy aspects of QS transition are interconnected, and many dependencies among actors within the ecosystem also need to be considered for QS transition.

Table 3
Overview of categories and challenges.

Challenge Category	QS Transition Challenges
Complex PKI Interdependencies	-PKI systems are heavily regulated (e.g., eIDAS regulations) and must comply with international standards (e.g., NIST, ETSI, X.509 standards, etc.) -Various standard bodies need to be considered, such as IETF, WWW, W3C, ETSI, NIST -Changes in PKIs cannot occur in isolation & need to consider the whole certificate chain -Interoperability issues may arise between organizations with old encryption levels and organizations with new encryption levels -New standards and regulations for QS solutions are not yet available for QS transition
Lack of Urgency	-Quantum threats are viewed as unlikely to occur tomorrow -Level of urgency varies with different risk appetite -A lack of understanding of what QS transition means -No clear view for policy-makers to recognize the risks associated with PKIs -Level of urgency remains low in the PKI ecosystem as a whole
Lack of Certified Hardware &/ Software	-Updates & new solutions need to consider interoperability & backward compatibility -Certified hardware and/or software may need to recognize two different encryption levels in the X.509 scheme -A lack of technical expertise and qualified personnel with knowledge and experience -Agreements are needed for new QS solutions before software providers generate certificates using new QS encryption scheme.
Unclear QS Direction & Governance	-Organizations currently do not have directions for QS transition -Changes in the current PKI systems may extend to other critical infrastructures -External experts saw the biggest risk in cross-organization governance -IT & government are very decentralized, unsure of the roles & responsibilities -Organizations are waiting for each other, and it is not clear who makes the first moves

5.2. Policy recommendations

This section presents four main policy recommendations, eg., 1) assessment of organizational impact and readiness, 2) collaboration in organizational ecosystem, 3) financial incentives and 4) funding and policy guidance.

5.2.1. Assessment of organizational impact and readiness

The first category of policy opportunities centres around the need to assess organizational impact and readiness. Organizations need to be ready to implement and adopt QS technologies. One form of assessment mentioned in the interviews is cryptographic impact assessment. Organizations do not know their cryptographic assets and have a varying lifespan of legacy technology in the current PKI system (CCC, 2019; ETSI, 2017; Kong et al., 2022; NIST, 2016). By conducting cryptographic assessment, organizations can identify the scope of the QS transition (e.g., where they use cryptography, why they use cryptography, and how they can replace that to quantum-safe with what priorities) (Respondent 4).

> "Organizations need to know which processes need to be changed for QS transition, and they need to be aware of which of the cryptographic assets need to change to quantum-safe." (Respondent 5)

For organizations that do not have their core business in PKI-related services and products, cryptographic assessment in their inventory may create awareness and help organizations understand the impact of quantum threats in their businesses. Others echoed this, as one respondent stated that organizations need to realize the impact of the technology and how it will impact their business in the long run (Respondent 12). For policy-makers, the cryptographic assessment may provide a tool for identifying risks at societal levels once PKI systems become no longer reliable (Respondent 9). PKI users will need to be made aware of changes that are taking place, and check whether their systems are compatible and update them (Respondent 1).

Moreover, another form of assessment that can be taken is testing for QS solutions. Organizations should prepare pilot testing to assess the list of PQC algorithms. NIST has announced four candidate algorithms for standardization (e.g. CRYSTALS-KYBER for public key encryption and

CRYSTALS-Dilithium, FALCON, and SPHINCS$^+$ for digital signatures) (NIST, 2022). However, these algorithms have not yet been tested in real-life settings, and performance has not been applied to different use cases (CCC, 2019; Macaulay & Henderson, 2019; Machatan & Heintzman, 2021; Vermeer & Peet, 2020). Having multiple candidates for QS solutions may raise technological uncertainties and further delay the QS transition, which is expected to take a decade (Respondent 8). One of the respondents indicated,

> "First, create your own test environment to play around with the new certificates, then you can maybe make a new product." (Respondent 1)

By testing these PQC algorithms, organizations can further develop certified hardware and software for PKI systems. The technical uncertainties of QS solutions make it difficult for organizations to decide which PQC algorithms to use in the current infrastructure (Respondent 6). Thus, assessing the list of potential QS solutions, recognizing the use cases and fixing all the vulnerabilities are needed for organizations to proceed with the QS transition (Respondent 6).

5.2.2. Collaboration in organizational ecosystems

The second category for policy opportunities is coordinating collaboration in organizational ecosystems. Since the PKI systems do not operate in isolation, QS transition depends on many different influences and may require multiple actors in the process (Kong et al., 2022; The Hague Security Delta, 2019). The PKI systems in the Netherlands must comply with international standards, European and Dutch regulations, and a Programme of Requirement (PoR) that ensures a statement of compliance for third-party arrangements (Innovalor, 2019; Logius, 2018, 2020, 2022). As noted by a respondent, mapping out the current PKI environment and coordinating collaborations can mobilize QS transition with other organizations that are part of the PKI ecosystem.

> "I think you start with the part of certificates. What are the organizations? And you go top-down and roll it out. For instance, we have our Certificate Roots in the Netherlands.… I will go top down based on the CAs and all those kinds of companies." (Respondent 2)

The PKIoverheid certificates are generated and stored with the requirements laid in eIDAS regulations and follow ETSI's recommendation, which guarantees the document's authenticity with a digital signature (Logius, 2022; QuoVadis, 2022). Due to various regulatory bodies, standard bodies, service providers, hardware and software companies that facilitate PKIs, organizations may need to monitor the standard bodies (e.g., NIST, ETSI, etc.) and update policies based on the CAB forum (Respondent 1). Since PKIs are unique in the sense that there is inherent cooperation with organizations and across entities, it is crucial for organizations not just to wait for QS solutions to become available but to seek collaboration in the ecosystem to move fast enough for QS transitions (Respondent 6).

Moreover, collaboration can also take place by stimulating forums and open dialogues with industries and academia. While QS solutions are being standardized, the use cases still need to measure the performance and feasibility of QS solutions.

> "There's much more to be done. What you see at those standardization levels is that standardization organisations depend on other bodies' research. What is working? What have you experienced? What are your conclusions?" (Respondent 8)

The creation of consortiums and collaboration across sectors may provide opportunities for organizations to share up-to-date knowledge and expertise in cryptography and QS transition for the current PKI systems. Since there is not yet a solution to be implemented in current PKI systems, external experts saw that monitoring general market practices and solutions is also important (Respondent 10). Organizing forums and dialogues can engage organizations to share knowledge and best practices for QS transitions via seminars, webinars, MOOCs, and organize workplace training programs with higher education institutions and research institutes.

5.2.3. Financial incentives and funding

Subsidies and funding can nudge organizations to move towards QS solutions. Funding was one of the main categories for policy opportunities concerning QS transitions. Depending on the current PKI systems and the availability of resources, a QS transition may require additional costs for risk assessment, technical expertise, and changes in the legacy systems (ISARA, 2018; Kong et al., 2022; TNO, 2020). In the case of hybrid certificates, hardware and software may need to manage two or more different certificates with two levels of encryption (Ma et al., 2021; Thales, 2019). Since organizations do not have urgency for QS transition, the cost of transition for organizations is not yet determined. One of the respondents indicated that,

> "Hoping that they've already allocated some budget to do that because you have to buy new stuff, you have to replace things." (Respondent 5)

Small government agencies and SMEs are seen as most vulnerable due to scarce resources for QS transition. The respondents indicated that to better address QS transitions for organizations, financing QS transition needs to be discussed, and if so, who will make the cost to facilitate QS transition (Respondent 10). Perhaps allocating budgets for QS transitions or stimulating organizations to apply for subsidies may provide additional incentives for QS transitions.

Furthermore, incentivizing cross-sectoral research and upscaling the market for hardware and software may be needed. The cross-sectoral organizational research can not only promote collaboration but also may generate a market for QS transition. If hardware and software are not available for QS transition, this may hinder organizations from modifying current PKI systems. As stated by a respondent,

> "Once a choice is made for the algorithms, then the industry, the suppliers delivering all kinds of technology will need to start working." (Respondent 5)

Suppose a vendor supports a certain QS solution standard, and it has been certified. In that case, PKI users who need to change the system will choose the hardware and software vendor that offers the standard that meets their needs and will be the robust standard for the future. (Respondent 7). Since getting QS solutions tested, implemented and certified in hardware and software can be an extensive process, vendors must be at the forefront of taking a bold step to have hardware and software ready. Without commercial viability testing, changes in the current PKI systems can result in the high technology switching cost trap (ETSI, 2015).

In addition, cross-sectoral research may help accelerate the research on QS transition to protect the current PKI systems. While much attention is paid to QS building blocks for fundamental components such as encryption and digital signatures, further research is still needed for more complex protocols (Respondent 8).

> "It's not that we think that research is done and uncovered. We think there's still some room there, plenty more. The momentum is only in the more fundamental research… Some internal protocols are also very hard to upgrade. Also, very interconnected, think of payment systems. The clock is also ticking." (Respondent 8)

There needs to be sufficient movement in the cryptographic protocols used for many different things in telecommunication and banking systems (Respondent 8). By providing the financial budget for international/ EU projects, QS solutions can be further studied, and organizations may develop complex protocols involving different QS solutions applications. These kinds of cross-sectoral research can provide up-to-date knowledge and learning opportunities and keep the available information for organizations to implement QS solutions in their PKI services and products to better maintain the secure facilitation of PKI

systems.

5.2.4. Policy guidance

Policy guidance is another main category of policy opportunities. There is a void in knowledge on how to transit towards QS PKI systems, and organizations do not know how to coordinate the process of QS transition (CSIRO, 2021; Kong et al., 2022; NIST, 2021). Since the modification in the current PKI systems needs to ensure interoperability and backward compatibility, establishing a set of policy guidance is considered necessary for a QS transition (Respondent 11).

> "We can see it with the eIDAS. That has helped a lot for everybody to have guidance and clarify what a digital signature is, what is allowed, and what's not. If you have something similar regarding QS solutions, it will help a lot." (Respondent 10)

The organizations that are part of PKI systems should follow ETSI standards and the eIDAS regulation and monitor standard bodies such as NIST, ETSI, IETF and other market parties such as CAB Forum that also influence PKI systems (Respondent 6). These standardization bodies strongly impact ensuring QS solutions are considered seriously by users (ETSI, 2015).

While upgrades in the current PKI systems need to comply to several regulations, there is no regulation on QS transition for organizations to follow. Existing cryptographic algorithms used in the current PKI systems may be technically broken but legally compliant. As one of the respondents stated,

> "For instance, a signature that is set with classical cryptography is legally still valid but technically broken. So what does that mean?" (Respondent 5)

The existing regulations that govern PKI systems raise legal implications for the QS transition. Organizations remain conservative when changing the current PKI systems because no regulations clarify the legality of the QS solutions. If changes are made in the Root, a whole PKI ecosystem that is behind it will be affected. (Respondent 12). Currently, the policy guidance for the QS transition only outlines generic advice for organizations to start inventorying the cryptographic systems and extend the length of the asymmetric path to be quantum-safe (Respondent 5). Since the QS transition cannot be single-handled by one organization, policy guidance is necessary to clarify what needs to be taken into account and what changes organizations do not have an influence on.

> "If you look at the ecosystem, there are multiple interacting policies. What is important here is that next to a policy statement requirement, there should be on the right levels of hierarchy to plan and what order to implement things best." (Respondent 6)

Since PKI systems are heavily regulated and PKI-related services and products need to be certified and audited, organizations find it challenging to choose the QS transition (Respondent 6). The respondent further emphasized that the policy guidance should provide clear roles and responsibilities for QS transition and a vision for how to implement changes for the QS transition (Respondent 6). Otherwise, the complex hierarchy of existing policies and new changes needed for the QS transition may misalign, and organizations may find themselves making changes with regulations competing with other regulations and laws in the Netherlands (Respondent 7).

Moreover, policy guidance should be available to clarify what the hybrid structure for QS solution refers to. The term hybrid structure has been mentioned repeatedly by respondents. One of the respondents indicated that,

> "What can help here is focusing a lot on the hybrid part. Typically, when we say hybrid, at least one of the definitions we discussed. Cryptographically, when you say hybrid, the system is secure as long as one of the two components is." (Respondent 8)

The term is an umbrella term to describe the PKI system that uses classical and quantum-safe primitives. If one of the two primitives remains secure, not degrading the security, and PKI systems are still in compliance, the hybrid part could be a way to speed up the regulation process (Respondent 8). However, there is no clear guidance yet, and the term hybrid structure remains more of a concept. No agreement was made for the QS standards and procedures on what to prioritize and what steps organizations should take for the QS transition not addressed (Respondent 4). The policy guidance should clearly indicate what the hybrid structure means for organizations to minimize interoperability and backward compatibility issues.

Based on the policy recommendations of the four categories in Table 4, much research is needed to tackle the socio-technical predicaments of QS transition. This also indicates that transitioning critical information infrastructures remains complex, and solution components for the transition challenges are scattered and unclear.

Policy recommendations in the assessing organizational impact and readiness category include conducting an impact assessment of quantum threats in their businesses, making QS implementation obliged for certain (sensitive) data, preparing pilot testing to assess the list of PQC algorithms, and identifying different use cases for QS solutions. Policy recommendations for collaboration in the organizational ecosystem category include mapping out the current PKI environment and coordinating collaborations, stimulating forums & open dialogues, creating consortiums and collaboration across sectors, and providing subsidies to stimulate the adoption of QS solutions. Policy recommendations for the financial incentives and funding category include incentivizing cross-sectoral research, extending research on more complex protocols, and upscaling the market for hardware and software. Finally, for the policy guidance category, policy recommendations include raising legal implications of QS transitions, defining clear roles and responsibilities, developing a vision for implementing changes, and clarifying what the hybrid structure of QS solutions refers to.

6. Conclusion

One day, the looming threats of quantum computers may become a reality. While security issues over networks are often considered a never-ending game of cat and mouse, the impact of the quantum threat on critical information infrastructures may be much more catastrophic. With the ever-growing dependence on critical information

Table 4
Overview of possible policy recommendations.

Policy Category	Policy Recommendations
Assessment of Organizational Impact & Readiness	-Conduct impact assessment of quantum threats in their businesses -Make QS implementation obliged for a certain data -Prepare pilot testing to assess the list of PQC algorithms -Identify different use cases for QS solutions
Collaboration in the Organizational Ecosystem	-Map out the current PKI environment and coordinating collaborations -Stimulate forums & open dialogues -Create consortiums and collaboration across sectors -Provide subsidies to stimulate the adoption of QS solutions
Financial Incentives & Funding	-Incentivize cross-sectoral research -Extend research on more complex protocols -Upscale the market for hardware and software
Policy Guidance	-Raise legal implications for the QS transition. -Define clear roles and responsibilities for QS transition -Develop a vision for how to implement changes for the QS transition -Clarify what the hybrid structure for QS solution refers to

infrastructures, failure to recognize the urgency for QS transitions and assess cryptographic assets may have far-reaching consequences across a wide range of sectors. Organizations may be unable to address the socio-technical predicaments of a QS transition overnight.

Although NIST is leading the standardization of QS solution algorithms that may be implemented in current PKI systems, our research reveals that the availability of QS algorithms alone is insufficient for preparing and guiding organizations for a QS transition. The implementation and adoption challenges for QS transition include complex technological interdependencies, lack of urgency, lack of certified hardware and software, and unclear QS direction and governance. These four categories of QS transition challenges show that institutional and organizational challenges may also need to be addressed next to the technical challenges, and many dependencies among actors exist in critical information infrastructures. This also implies that challenges for QS transition are interconnected and the current emphasis on technical standardization only partly supports QS transitions.

Moreover, the list of policy recommendations for QS transition includes assessing organizational impact and readiness, collaboration in the organizational ecosystem, financial incentives and funding, and policy guidance. The recommendations show that solutions for QS transition challenges are scattered and not yet clearly identified. Although a QS transition is a massive operation that requires collaboration beyond organizational boundaries, there is no central coordination, and organizations do not have well-defined roles and responsibilities. Many uncertainties signal a *Catch-22* loop where a delay in one challenge may further lead to delays in other challenges. Government agencies might be waiting for QS software to arrive. In contrast, software vendors do not develop SQ solutions as there is no urgent demand today and uncertainties regarding the availability date of sufficiently powerful quantum computers. For policy-makers, it also implies that they must understand the gravity of the challenges, and actionable approaches are needed to prepare for the QS transition.

As the paper lays the empirical foundation for QS transition research on challenges, it seems crucial that researchers take the next step in unravelling how to address socio-technical challenges that are both complex and interconnected. By doing this, it may lead to a situation where countries and organizations take different paths of QS transition to become quantum-safe. Given the impact of quantum threats and the importance of critical information infrastructure in our societies, the QS transition topic offers many research opportunities left to investigate. While the limited sample size of respondents in this study highlights potential future research opportunities to expand the sample size, it also suggests exploring strategies to increase awareness and bridge the knowledge gap for QS transition. Moreover, the direction and roadmaps for QS transition are still undefined and much research is needed to understand the QS solutions in various use cases. "How can we coordinate QS transition and move together as a whole?" may be a crucial question with many unknowns that we must answer in time to realize a QS future.

CRediT authorship contribution statement

Ini Kong: Conceptualization, Methodology, Validation, Investigation, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Marijn Janssen:** Conceptualization, Supervision, Writing – review & editing. **Nitesh Bharosa:** Conceptualization, Supervision, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Marijn Janssen and Nitesh Bharosa (co-authors of this paper) are both on the editorial board of the journal.

Acknowledgements

This publication is part of the HAPKIDO research project with project number NWA.1215.18.002 of the research programme Cybersecurity, which is (partly) financed by the Dutch Research Council (NWO).

References

Adams, C., & Lloyd, S. (1999). *Understanding public-key infrastructure: Concepts, standards, and deployment considerations*. Macmillan Technical Publishing.
AIVD. (2021). *Bereid je voor op de dreiging van quantum computers*.
Amadori, A., Duarte, J. D., & Spini, G. (2022). *Literature overview of public-key infrastructures, with focus on quantum-safe variants deliverable 4.1, HAPKIDO project*.
Barker, W., Souppaya, M., & Newhouse, W. (2021). *Migration to post-quantum cryptography*.
Bernstein, D., & Lange, T. (2017). Post-quantum cryptography. *Nature, 549*, 188–194. https://doi.org/10.1038/nature23461
Bharosa, N., van Wijk, R., de Winne, N., Janssen, M. F. W. H. A., & (Eds.).. (2015). *Challenging the Chain: Governing the automated exchange and processing of business information*. Logius & Thauris. https://doi.org/10.3233/978-1-61499-497-8-i
Bindel, N., Herath, U., Stebila, D., & McKague, M. (2017). *Transitioning to a quantum-resistant public key infrastructure*.
Bohr, N. (1913). *On the constitution of atoms and molecules*.
Bova, F., Goldfarb, A., & Melko, R. G. (2021). Commercial applications of quantum computing. *EPJ Quantum Technnology, 8*(1), 2. https://doi.org/10.1140/epjqt/s40507-021-00091-1
Brooks, M. (2023). Quantum computers: What are they good for? *Nature, 617*, S1–S3. https://doi.org/10.1038/d41586-023-01692-9
Buchholz, S., Mariani, J., Routh, A., Keyal, A., & Kishnani, P. (2020). *The realist's guide to quantum technology and national security: What nontechnical government leaders can do today to be ready for tomorrow's quantum world*.
CCC. (2019). *Identifying research challenges in post quantum cryptography migration and cryptographic agility*.
Chen, L., & Moody, D. (2020). New mission and opportunity for mathematics researchers: Cryptography in the quantum era. *Adv. Math. Commun., 14*(1), 161–169. https://doi.org/10.3934/amc.2020013
Covers, O., & Doeland, M. (2020). *How the financial sector can anticipate the threats of quantum computing to keep payments safe and secure*.
Creswell, J. W. (2018). *Research design: Qualitative, quantitative and mixed methods approaches* (third edition).
Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity, 9*(1). https://doi.org/10.1093/cybsec/tyad001
CSIRO. (2021). *The quantum threat to cybersecurity: Looking through the prism of post-quantum cryptography*.
Daley, A. J., Bloch, I., Kokail, C., Flannigan, S., Pearson, N., Troyer, M., & Zoller, P. (2022). Practical quantum advantage in quantum simulation. *Nature, 607*(7920), 667–676. https://doi.org/10.1038/s41586-022-04940-6
Danquah, P., & Kwabena-Adade, H. (2020). Public key infrastructure: An enhanced validation framework. *Journal of Information Security, 11*(04), 241–260. https://doi.org/10.4236/jis.2020.114016
Dowling, J. P., & Milburn, G. J. (2003). *Quantum technology: The second quantum revolution*.
ENISA. (2021). *Post-quantum cryptography: Current state and quantum mitigation*.
ETSI. (2015). *Quantum safe cryptography and security: An introduction, benefits, enablers and challenges*.
ETSI. (2017). *Quantum safe cryptography*. Case Studies and Deployment Scenario.
ETSI. (2020). *CYBER; migration strategies and recommendations to quantum safe schemes*.
European Commission. (2022). Transition towards quantum-resistant cryptography. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-cs-01-03.
Feynman, R. P. (1948). Space-time approach to non-relativistic quantum mechanics. *Reviews of Modern Physics, 20*(2), 367–387.
Gibney, E. (2019). *The quantum gold rush*.
Giron, A. A. (2023). *Migrating applications to post-quantum cryptography: Beyond algorithm replacement SECrypt 2023*.
Grote, O., Ahrens, A., & Benavente-Peces, C. (2019). Paradigm of post-quantum cryptography and crypto-agility: Strategy approach of quantum-safe techniques. In *Proceedings of the 9th international conference on pervasive and embedded computing and communication systems*.
Grover, L. K. (1996). *A fast quantum mechanical algorithm for database search*.
Heale, R., & Forbes, D. (2013). *Understanding Triangulation in Research, 16*(4), 98.
Heisenberg, W. (1927). *The physical content of quantum kinematics and mechanics*.
Hong, K.-W., Foong, O.-M., & Low, T.-J. (2016). Challenges in quantum key distribution. In *Proceedings of the 4th international conference on information and network security - ICINS '16*.
Huang, J., & Nicol, D. M. (2017). An anatomy of trust in public key infrastructure. *International Journal of Critical Infrastructures, 13*(2/3). https://doi.org/10.1504/ijcis.2017.088234
Hunt, R. (2001). Technological infrastructure for PKI and digital certification. *Computer Communications, 24*, 1460–1471.
Innovalor. (2019). *PKIoverheid: Onderzoek naar mogelijkheden om gebruik te vergroten bijvoorbeeld via verplichtstelling*.
ISARA. (2018). *Enabling quantum-safe migration with crypto-agile certificates*.

Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., … Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*(7909), 237–243. https://doi.org/10.1038/s41586-022-04623-2
Käppler, S. A., Schneider, & Bettina. (2022). Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms. In *Proceedings of the Society 5.0 Conference 2022 - Integrating Digital World and Real World to Resolve Challenges in Business and Society*.
Kim, Y., Eddins, A., Anand, S., Wei, K. X., van den Berg, E., Rosenblatt, S., … Kandala, A. (2023). Evidence for the utility of quantum computing before fault tolerance. *Nature, 618*(7965), 500–505. https://doi.org/10.1038/s41586-023-06096-3
Kong, I., Janssen, M., & Bharosa, N. (2022). *Challenges in the transition towards a QS government*. https://doi.org/10.1145/3543434.3543644
Kong, I., Janssen, M., & Bharosa, N. (2023). *Analyzing dependencies among challenges for quantum-safe transition*. EGOV-CeDEM-EPart2023. Hungary: Corvinus University of Budapest.
Kramer, A. (2023). Quantum algorithm offers faster way to hack internet encryption. *Science, 381*(6664), 1270. https://doi.org/10.1126/science.adk9443
Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors (Basel), 21*(18). https://doi.org/10.3390/s21186225
Kumar, M. (2022). Post-quantum cryptography Algorithm's standardization and performance analysis. *Array, 15*. https://doi.org/10.1016/j.array.2022.100242
Labs, A. (2018). *Cryptography in a post-quantum world: Preparing intelligent enterprises now for a secure future*.
Lewis, A. M. (2017). *The impact of quantum technologies on the EU's future policies: Part 1 quantum time*.
Lewis, A. M., Ferigato, C., Travagnin, M., & Florescu, E. (2018). *The impact of quantum technologies on the EU's future policies: Part 3 perspectives for quantum computing*.
Lewis, A. M., & Travagnin, M. (2018). *The impact of quantum technologies on the EU's future policies: Part 2 quantum communications: From science to policies*.
Lewis, A. M., & Travagnin, M. (2022). *A secure quantum communications infrastructure for Europe: Technical background for a policy vision*.
Lindsay, J. R. (2020a). Demystifying the quantum threat: Infrastructure, institutions, and intelligence advantage. *Security Studies, 29*(2), 335–361. https://doi.org/10.1080/09636412.2020.1722853
Lindsay, J. R. (2020b). *Surviving the quantum cryptocalypse*.
Linn, J. (2000). *Trust models and management in public-key infrastructures*.
Logius. (2018). *Programme of requirements part 1: Introduction*. Logius.
Logius. (2020). *Certification Practice Statement (CPS): Policy Authority PKIoverheid for Private Root CA certificates to be issued by the Policy Authority of the PKI for the Dutch government*.
Logius. (2022). *Programme of requirements part 3: Basic requirements PKIoverheid*.
Lovic, V. (2020). Quantum key distribution: Advantages, challenges and policy. *Cambridge Journal of Science and Policy, 1*(2).
Lowery, D., & Evans, K. G. (2004). The iron cage of methodology: The vicious circle of means limiting ends limiting means. *Administration and Society, 36*(3), 306–327. https://doi.org/10.1177/0095399704265298
Ma, C., Colon, L., Dera, J., Rashidi, B., & Garg, V. (2021). CARAF: Crypto agility risk assessment framework. *Journal of Cybersecurity, 7*(1). https://doi.org/10.1093/cybsec/tyab013
Macaulay, T., & Henderson, R. (2019). *Cryptographic agility in practice: Emerging use-cases*.
Machatan, A., & Heintzman, D. (2021). *The complex path to quantum resistance*.
Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications (IJACSA), 9*(3).
McKinseyDigital. (2022). *When—and how—to prepare for post-quantum cryptography*.
Mehrez, H. A., & Omri, O. E. (2018). *The crypto-agility properties*.
Ménard, A., Ostojic, I., Patel, M., & Volz, D. (2020). *A game plan for quantum computing*.
Menezes, A., & Stebila, D. (2021). Challenges in cryptography. *IEEE Security and Privacy, 19*(2), 70–73. https://doi.org/10.1109/msec.2021.3049730
Mosca, M. (2015). *Cybersecurity in an era with quantum computers: Will we be ready?*.
Mosca, M., & Piani, M. (2022). *Quantum threat timeline report* (p. 2022).
Mulholland, J., Mosca, M., & Braun, J. (2017). The day the cryptography dies. *IEEE Security and Privacy*, 14–21.
Nazario, N., & van Oosten, M. (2001). *Real-world application of public key infrastructures deployment methodology*.
NCSC. (2020). *PKIoverheid is changing*.
NCTV. (2022). *Nederlandse cybersecuritystrategie 2022–2028*.
Niederhagen, R., & Waidner, M. (2017). *Practical post-quantum cryptography*.
NIST. (2016). *Report on post-quantum cryptography*.
NIST. (2018). *The economic impacts of the advanced encryption standard, 1996–2017*. https://doi.org/10.6028/nist.Gcr.18-017
NIST. (2021). *Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms*. https://doi.org/10.6028/nist.Cswp.04282021
NIST. (2022). PQC standardization process: Announcing four candidates to be standardized, plus fourth round candidates. Retrieved 08-08 from https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4.
NSA. (2022). Quantum key distribution (QKD) and quantum cryptography (QC). https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.
Paar, C., & Pelzl, J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Berlin Heidelberg: Springer-Verlag.
Peterssen, G. (2020). *Quantum technology impact: The necessary workforce for developing quantum software*.
Petrenko, K., Mashatan, A., & Shirazi, F. (2019). Assessing the quantum-resistant cryptographic agility of routing and switching IT network infrastructure in a large-size financial organization. *Journal of Information Security and Applications, 46*, 151–163. https://doi.org/10.1016/j.jisa.2019.03.007
Planck, M. (1900). *On the theory of the energy distribution law of the Normal Spectrum*.
QED-C. (2021). *A Guide to a Quantum-Safe Organization: Transitioning from today's cybersecurity to a quantum-resilient environment*.
QuoVadis. (2022). *Certification practice statement for PKIoverheid certificates*.
Rasanen, M., Makynen, H., Mottonen, M., & Goetz, J. (2021). Path to European quantum unicorns. *EPJ Quantum Technnology, 8*(1), 5. https://doi.org/10.1140/epjqt/s40507-021-00095-x
Regev, O. (2023). *An efficient quantum factoring algorithm*. arXiv preprint arXiv: 2308.06572.
Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). Sage Publications.
Schrödinger, E. (1926). Quantisierung als Eigenwertproblem. *Annalen der Physik, 384*(4), 361–376. https://doi.org/10.1002/andp.19263840404
Shor, P. W. (1994). *Polynomial time algorithms for discrete logarithms and factoring on a quantum computer*.
Sjöberg, M. (2017). *Post-quantum algorithms for digital signing in public key infrastructures*.
Smith, F. L. (2020). Quantum technology hype and national security. *Security Dialogue, 51*(5), 499–516. https://doi.org/10.1177/0967010620904922
Sood, V., & Chauhan, R. P. (2023). Archives of quantum computing: Research Progress and challenges. *Archives of Computational Methods in Engineering*. https://doi.org/10.1007/s11831-023-09973-2
Thales. (2019). *Upgrading existing security systems to agile quantum-safe with SafeNet Luna HSMs and SafeNet High Speed Encryptors*.
The Hague Security Delta. (2019). *Understanding the strategic and technical significance of technology for security: Implications of quantum computing within the cybersecurity domain*.
The White House. (2022). *Migrating to post-quantum cryptography*.
Tibbetts, J. (2019). *Quantum computing and cryptography: Analysis, risks, and recommendations for decisionmakers*.
TNO. (2020). *Migration to quantum-safe cryptography: About making decisions on when, what and how to migrate to a quantum-safe situation*.
TNO, CWI, & AIVD. (2023). *The PQC migration handbook: Guidelines for migrating to post-quantum cryptography*.
Vermaas, P. E. (2017). The societal impact of the emerging quantum technologies: A renewed urgency to make quantum theory understandable. *Ethics and Information Technology, 19*(4), 241–246. https://doi.org/10.1007/s10676-017-9429-1
Vermeer, M. J. D., & Peet, E. D. (2020). *Securing communications in the quantum computing age: Making the risks to encryption*.
Wiesmaier, A., Alnahawi, N., Grasmeyer, T., GeifBler, J., Zeier, A., BauspieIB, P., & Heinemann, A. (2021). *On PQC migration and crypto-agility*.
Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review, 15*.
de Wolf, R. (2017). The potential impact of quantum computers on society. *Ethics and Information Technology, 19*(4), 271–276. https://doi.org/10.1007/s10676-017-9439-z
Yunakovsky, S. E., Kot, M., Pozhar, N., Nabokov, D., Kudinov, M., Guglya, A., … Fedorov, A. K. (2021). Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology, 8*(1). https://doi.org/10.1140/epjqt/s40507-021-00104-z

Ini Kong is a PhD candidate in the Department of Engineering Systems and Services at the Faculty of Technology, Policy and Management of Delft University of Technology. She holds a master's degree in Environment and Society at Radboud University and an undergraduate degree with honours in Political Science and Sociology from the University of Toronto. Her research interests include transition governance, digital security in critical information infrastructures, and Quantum-safe (QS) transition.

Marijn Janssen is a full professor in ICT & Governance and head of the Engineering Systems and Services department at the Faculty of Technology, Policy, and Management of Delft University of Technology. He is also an honorary visiting professor at Bradford university, UK and KU-Leuven, Belgium. He is listed as one of the world's 100 most influential people in digital government in 2018 and 2019. He has published over 500 publications, an h-index of over 60 and more than 15 K citations.

Nitesh Bharosa is a full professor in GovTech in the Department of Engineering Systems and Services at the Faculty of Technology, Policy, and Management of Delft University of Technology. He is the academic director of Digicampus – a quadruple helix innovation ecosystem for future public services. He has successfully led research projects in GovTech design and governance. He has published in several high-ranking journals, including Government Information Quarterly, Information Systems Frontiers, Decision Support Systems and the Journal of Cognition, Technology & Work.