CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Identifying Obstacles of PQC Migration in E-Estonia

Jelizaveta Vakarjuk
Cybernetica AS and
Department of Software Science
Tallinn University of Technology
Tallinn, Estonia
jelizaveta.vakarjuk@cyber.ee

Nikita Snetkov
Cybernetica AS and
Department of Software Science
Tallinn University of Technology
Tallinn, Estonia
nikita.snetkov@cyber.ee

Peeter Laud
Cybernetica AS
Tartu, Estonia
peeter.laud@cyber.ee

Abstract: With the development of quantum technologies, there is an urgent need to secure existing IT infrastructure against quantum threats. Introducing post-quantum cryptography (PQC) to existing systems may protect them against future quantum computer attacks. Still, post-quantum migration is a cumbersome process that requires systematic planning and takes years. In this paper, we study Estonia's e-government ecosystem, outline systems and products that rely on potentially vulnerable cryptographic primitives, identify the main migration obstacles, and provide recommendations on how the migration process should be carried out.

Keywords: *post-quantum cryptography, e-governance, migration*

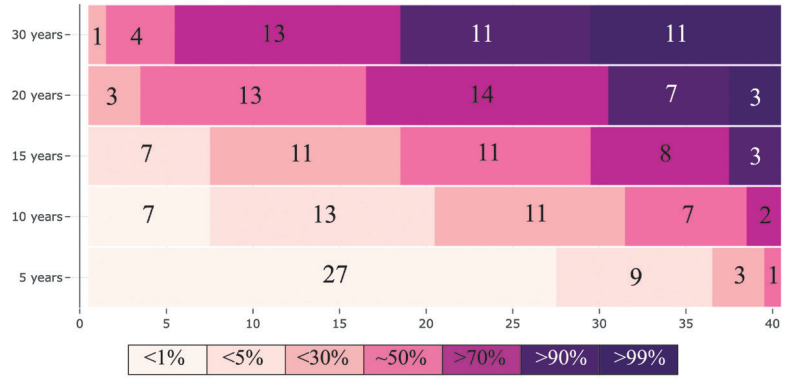
1. INTRODUCTION

In 1994, Peter Shor showed that sufficiently powerful quantum computers can solve integer factorization and discrete logarithm problems whose hardness is the foundation of many modern public-key cryptosystems. Therefore, we have to reckon with the emergence of cryptographically significant quantum computers (CSQCs) [1]. Such computers can eliminate the practical usage of most public-key primitives, such as (EC)DH,[1] RSA,[2] (EC)DSA,[3] and EdDSA[4] [2], and affect the key and/or output sizes of symmetric key schemes such as AES[5] and SHA[6] [3]. For that reason, several standardization agencies and industrial entities initiated the process of migration to post-quantum (also known as quantum-safe) cryptography [4].

One cannot reliably predict a date when a CSQC will be available. Several factors influence progress in this area. The first one is when the *circuit for Shor's algorithm* is optimized. There are different ways in which the quantum circuit for Shor's algorithm can be built [5]–[7]; some require fewer qubits,[7] while others require fewer operations or fewer specific gates. There may be further optimizations of circuits that can influence how soon breaking RSA with keys of practical length becomes feasible. Another is progress in *error correction*, since realizing physical qubits is a non-trivial task. As physical qubits interact with each other, errors appear. Correcting these errors is hard due to the non-cloning theorem [8]. Therefore, the number of physical qubits needed to implement Shor's algorithm is much higher than the number of logical (error-corrected) qubits [9]. This is currently an active research area; reducing the ratio between the logical and physical qubits is an important goal. Finally, *chip architecture* is progressing. There are different types of qubits (e.g., ion traps, photonics, and superconducting qubits) [10], each requiring a different architecture when assembled into chips. Moreover, this architecture may be different even for the same type. All these aspects show that judging the progress of quantum technology development by just the number of announced qubits is not accurate. Instead, leading experts can be surveyed to determine their opinions on how long it will take before a CSQC is built. Such surveys have already been carried out; we have cited the results of one of them [1] in Figure 1.

1 Elliptic Curve Diffie-Hellman (ECDH).
2 Rivest-Shamir-Adleman (RSA).
3 Elliptic Curve Digital Signature Algorithm (ECDSA).
4 Edwards-curve Digital Signature Algorithm (EdDSA).
5 Advanced Encryption Standard (AES).
6 Secure Hash Algorithm (SHA).
7 Qubit is a basic unit of quantum information.

FIGURE 1: OPINION OF 40 EXPERTS ON THE LIKELIHOOD OF HAVING A QUANTUM COMPUTER ABLE TO FACTORIZE A 2048-BIT NUMBER IN 24 HOURS



Estonia is known for its success in e-government, including citizen ID cards, interoperability services, i-voting, and e-taxes. A significant amount of Estonian infrastructure relies on the security of used cryptographic primitives. The process of migrating these services to quantum-safe cryptographic schemes and protocols is a non-trivial task, because post-quantum algorithms have properties different from those of the algorithms currently used. For example, there is no drop-in replacement for the Diffie-Hellman key exchange, or for RSA, that can be used as both a digital signature and an encryption algorithm. The key sizes, signature, and ciphertext sizes are increased, complicating their use with constrained devices such as smart cards.

Related work. Kampanakis et al. [11] identify research gaps and possible standard updates that are required for the PQC migration process. The work focuses mostly on the impact of PQC on authentication in transport protocols and proposes sixteen open questions for the research. Attema et al. [12] created a handbook for the PQC migration process to help different organizations to organize and plan the PQC migration process. It explains concrete steps in the process and gives advice on how to mitigate the threat of quantum computers to their systems. Additionally, there is the Open Quantum Safe (OQS) project [13], which supports the post-quantum migration process by helping with the implementation and evaluation aspects of PQC. OQS maintains a library for the post-quantum cryptographic algorithms, as well as their integration into various protocols and applications, such as OpenSSL.

In this work, we discuss the main obstacles to migrating cryptography-reliant e-Estonia technologies to PQC. We outline the current status of research in post-quantum cryptography and provide recommendations for software/security architects and decision-makers.

2. PRELIMINARIES

A. Priorities in Transitioning to PQC

One of the main goals of e-government services is to assure the confidentiality, integrity, and authenticity of the information exchanged between the governmental institutions, citizens, and businesses. A service provides these properties by relying on various cryptographic primitives (e.g., encryption for confidentiality, signatures for integrity and non-repudiation, etc.). For interoperability between services and their clients, the use of cryptography has to be sufficiently standardized, such that all stakeholders understand the relevant data structures and encodings in the same way.

A breakthrough in the cryptanalysis of contemporary cryptographic primitives, achieved by, for instance, a CSQC, affects whether a system achieves all the security goals mentioned above, but it affects them in quite different ways. The used authentication protocols must be updated before a CSQC is available, but currently, we can continue using existing protocols, because authentication happens in the moment. The evidentiary value of a signature on a digital document can be preserved if someone takes the necessary steps to show that the signature was created before a CSQC came into being. The secrecy of a message encrypted today may be breached if the adversary stores the ciphertext and manages to obtain a CSQC and to recover the plaintext while the obligation of confidentiality remains valid. While the goal of transitioning to PQC is to make sure that a system continues to provide its security properties, this analysis shows that different priorities may be assigned to different properties and to subsystems ensuring these properties.

B. Quantum Key Distribution and PQC

Quantum key distribution (QKD) is a technology that enables parties to establish a shared secret key for exchanging encrypted data [14]. QKD is based on the laws of quantum physics, implying that information exchanged over quantum channels cannot be copied. Any interference in the communication will be noticeable by protocol participants, since the to-be-transferred quantum state is destroyed. Hence QKD is affected by denial-of-service attacks. QKD requires the creation and management of specific and costly infrastructure. For longer QKD networks, several trusted intermediate nodes are necessary. In 2023, the European Quantum Flagship initiated the EuroQCI project to construct quantum communication infrastructure within the European Union.[8] Estonia participates in EuroQCI through the sub-project EstQCI, led by the Ministry of Economic Affairs and Communication.[9]

PQC, however, helps to solve a wider range of problems, offering key establishment, encryption, digital signatures, and so on. Deploying PQC algorithms and testing their performance in the currently used protocols is much easier than QKD, because

8 https://petrus-euroqci.eu
9 https://www.riks.ee/kvantside/estqci-kvantside-projekt

they run on classical hardware. Therefore, experimenting with and deploying PQC is currently more urgent than building QKD networks.

C. NIST Standardization

The National Institute of Standards and Technology (NIST) initiated a standardization competition for post-quantum algorithms in 2016 and received submissions of twenty-three signature schemes and fifty-nine key establishment mechanisms (KEM) built on a variety of mathematical problems.[10] The main families of post-quantum algorithms are lattice-based, code-based, isogeny-based, hash-based, multivariate-based, and based on MPC-in-the-head.[11]

After the third round of NIST standardization competition, seven finalist schemes and eight alternate schemes were selected [15]. Four schemes were selected to become future standards: Crystals-Kyber [16] for the KEM category and Crystals-Dilithium, Sphincs+, and Falcon for the signature category.[12] Crystals-Kyber, Crystals-Dilithium, and Falcon are lattice-based schemes, while Sphincs+ is hash-based. Crystals-Dilithium [17] is considered the primary signature scheme, suitable for all use cases. Sphincs+ [18] is more conservative security-wise but the least efficient. Falcon [19] has the smallest key and signature sizes but requires floating point arithmetic.

Since most of the selected schemes rely on structured lattices, the NIST decided to continue the standardization competition to find alternative schemes. The candidates for the KEM category were selected from the schemes in the fourth round of competition—Classic McEliece [20], BIKE[13] [21], and HQC[14] [22] (all of them code-based). The isogeny-based candidate SIKE[15] was broken. For signature schemes, the NIST announced a new call, receiving fifty submissions.[16] The NIST expects two candidates at most to be selected for the standardization. No candidate is expected to replace Crystals-Dilithium as the primary signature scheme.

The NIST also initiated a separate process for standardizing *stateful* hash-based signatures: Leighton-Micali Signature (LMS) and eXtended Merkle Signature Scheme (XMSS) [23]. Both LMS and XMSS are considered to be secure against quantum computers, but they are less practical than Sphincs+, Falcon, or Crystals-Dilithium. Their main limitation is that the signer must keep track of a state. Protecting the state and backing it up along with the private key is still an open question. One potential solution could be threshold cryptography [24].

10 https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms
11 Multi-party computation in the head (MPC-in-the-head) is a paradigm that allows to create digital signature that is a non-interactive zero-knowledge proof of knowledge of the secret key.
12 https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
13 Bit Flipping Key Encapsulation (BIKE).
14 Hamming Quasi-Cyclic (HQC).
15 Supersingular Isogeny Key Encapsulation (SIKE).
16 https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf

D. European Standardization and Security Agencies

European organizations like BSI,[17] ANSSI,[18] ETSI,[19] ENISA,[20] and NCSC[21] have also published reports on the transition to post-quantum cryptography, listing algorithms they recommend using and explaining how they should be used. Some of the recommended algorithms are different from the recommendations of the NIST. Table I indicates which algorithms are recommended by which organization.

TABLE I: AGENCY RECOMMENDATIONS

Organization	KEM	Signatures
NIST	Crystals-Kyber	Crystals-Dilithium, Falcon, Sphincs+, XMSS, LMS
BSI [25]	FrodoKEM, Classic McEliece, Crystals-Kyber*	LMS/HSS, XMSS/XMSS MT, Crystals-Dilithium,* Sphincs+*
ANSSI [26]	Crystals-Kyber, FrodoKEM	Crystals-Dilithium, Falcon, XMSS, LMS, Sphincs+
NCSC [27]	Crystals-Kyber	Crystals-Dilithium, Falcon, Sphincs+, XMSS, LMS

* After NIST standards are available

FrodoKEM [28] is a lattice-based KEM that was submitted to the NIST competition but, due to its performance, was not selected. FrodoKEM and Classic McEliece are recommended due to their more conservative and well-understood security. However, both schemes are less efficient than Crystals-Kyber and may not suit all the applications. Additionally, post-quantum cryptography is recommended for use only in *hybrid mode*. Only hash-based signature schemes may be used as standalone solutions. Managing the state of XMSS or LMS is an important concern; it must not be copied or backed up to the other device, because this may lead to a forked state, potentially resulting in security breaches.

E. Hybrid Schemes

In the context of PQC, hybrid mode refers to the usage of post-quantum algorithms together with classical algorithms. Hybrid mode is used to guarantee security even if one of the algorithms gets broken or if an implementation vulnerability is found.

Using a KEM in hybrid mode is theoretically straightforward; one would use a KEM *combiner* that takes as input both ECC[22]/RSA key material and PQC key

17 German Federal Office for Information Security (BSI).
18 French Cybersecurity Agency (ANSSI).
19 European Telecommunications Standards Institute (ETSI).
20 European Union Agency for Cybersecurity (ENISA).
21 National Cyber Security Centre (NCSC).
22 Elliptic Curve Cryptography (ECC).

material and outputs a symmetric key that is computed from both key materials. BSI recommendations for KEM combiners are CatKDF[23] and CasKDF[24] [29] and the NIST's Keccak (SHA3, KMAC[25]) and HMAC[26]-based KDFs [30].

Combining PQC with pre-quantum cryptography in public key certificates is more complicated. Multiple variants have been proposed [31], all with their own limitations (Table II). The most straightforward solution is to use *multiple certificates*, that is, having separate certificates with post-quantum keys and with pre-quantum keys. With this setup, all entities (CA, subCA, client) have two distinct key pairs for the same identity. This solution makes it possible to keep the existing infrastructure and supplement it with a mirror copy based on post-quantum algorithms.

Another option is to use the *AltPublicKey* extension [32] of X.509 certificates, adding a post-quantum key and the corresponding signature. This approach can be used with legacy systems, such that the main signature on the certificate is pre-quantum and verifiable by any device, and the alternate signature may be verified by the parties supporting PQC.

The *chameleon* [33] approach makes it possible to hide one certificate inside another and extract the inner certificate when needed. With this approach, the system can decide whether both signatures should be verified or just one of them.

The *composite* [34] approach makes it possible to define key and signature objects, each of which internally consists of two keys and signatures. This approach allows for adopting post-quantum schemes without changing the logic of application when it is used but instead by changing the cryptographic library that specifies these composite objects and operations with them. The specification [34] was designed to consider composite algorithms to be FIPS[27]-approved even when one of the component algorithms is not. When choosing an appropriate hybrid mode, it is important to understand the system requirements and limitations.

23 Concatenate Key Derivation Function (CatKDF).
24 Cascade Key Derivation Function (CasKDF).
25 Keccak Message Authentication Code (KMAC).
26 Hash-based Message Authentication Code (HMAC).
27 US Federal Information Processing Standard (FIPS).

TABLE II: HYBRID APPROACHES

Approach	Advantages	Disadvantages
Multi-certificate	• No changes to the existing infrastructure (a copy is created). • Can choose when to transmit large post-quantum certificates and signatures.	• Difficult to use with protocols or architectures supporting a single signature or certificate. • Difficult to manage layers.
AltPublicKey	• Compatible with legacy systems. • Compatible with applications that are limited to a single certificate.	• Large keys for post-quantum primitives need to be transmitted even if not used. • Requires updating protocols to verify/ produce multiple signatures.
Chameleon	Large post-quantum keys can be dropped if not used.	Requires updating protocols to verify/ produce multiple signatures.
Composite	• Both keys are used at the same time, offering the best security. • Satisfies regulatory requirements.	Not compatible with legacy systems.

F. Migration to PQC

Migration from classical cryptography to PQC is a resource- and time-consuming process, with a timeline that might exceed five years [12]. Therefore, the migration process should begin as soon as possible. The migration framework introduced in [35] and used later in [12] consists of three main stages:

1) compilation of cryptographic inventory;
2) preparation of the migration plan;
3) execution of the migration plan.

The first stage consists of identifying all locations where cryptographic technologies are being used, including, but not limited to:

1) confidentiality and integrity of data at rest or in transit;
2) authentication of users or other system elements;
3) access control to resources of the system [35].

One must identify what data should be protected and for how long. This makes it possible to determine the urgency of PQC migration and the priorities of migrating different systems. The questions in Annex A.1 of [35] can help in compiling a cryptographic inventory.

In the second stage, the main challenge is to choose which post-quantum schemes should be implemented and how. Not all post-quantum algorithms are suitable for all use cases; one must choose suitable algorithms based on the systems' limitations, constraints, and requirements. Implementing PQC may also require new hardware that supports those algorithms.

In the third stage, the migration plan from the previous stage is executed. In this step, it is crucial to avoid introducing new vulnerabilities during the implementation. Attention should be paid to side-channel resistance of the implemented schemes [36]–[39]. Additionally, it is important to maintain cryptographic agility, which allows for switching between different post-quantum algorithms.

3. CRYPTOGRAPHIC INVENTORY

Many of the services underlying the infrastructure of e-Estonia rely heavily on different cryptographic algorithms; some of them even go beyond regular digital signatures and encryption. Migrating all those services to post-quantum cryptography while preserving interoperability is a non-trivial task, given the challenges of PQC. We start by identifying the systems of e-Estonia that rely on cryptography and the parts of them that a CSQC would break.

We see that for many applications listed in Table III, data privacy needs to be ensured for a long time. These applications may be targets of *harvest attacks*, where the adversary collects encrypted data now and decrypts it later, when quantum computers become available. It may already be too late to prevent harvest attacks, since PQC is not used in current protocols, and adversaries could already be collecting the traffic. Still, the impact of those attacks can be mitigated.

For some digital signature use cases (e.g., signing long-term contracts), the forgery protection must be long-term. Once the adversary is able to forge a user's signature, the authenticity of data protected by this signature is questionable and one has to be careful when accepting signatures under this key pair. We know what it takes to extend the validity period of signatures. Some of it is reflected in the current AdES formats [40] for archival signatures; to achieve the rest, the entity interested in preserving the evidentiary value refreshes the time stamps [41].

TABLE III: USAGE OF CRYPTOGRAPHIC PRIMITIVES WITHIN ESTONIAN INFRASTRUCTURE

Cryptographic scheme	Function	Post-quantum security	Applications in e-Estonia
RSA	Encryption, signature	Broken	Smart-ID, ID card, X-Road
ElGamal	Encryption	Broken	I-voting
ECDSA	Signature	Broken	ID card, Mobile-ID
ECDH	Key establishment	Broken	TLS
AES	Encryption	Key size increase required [42], [43]	TLS, ID card

4. TRANSITION TO QUANTUM-SAFE ALTERNATIVES

The migration process to post-quantum cryptography is more challenging and resource-consuming than the previous cryptographic migrations (e.g., DES to AES, SHA1 to SHA2, RSA to ECDSA after the Estonian ID card crisis[28]). Unfortunately, PQC has no drop-in replacement for ECDH or RSA. There is no post-quantum scheme that offers both encryption and signing functionality as RSA. No scheme with properties similar to the Diffie-Hellman key exchange was submitted to the NIST standardization competition.

As the key and signature sizes of algorithms grow, protection against side-channel attacks increases in importance. Therefore, each application should be handled separately, and an appropriate quantum-safe alternative should be chosen on the basis of its requirements and limitations. For use cases that rely on multiple cryptographic primitives or use non-standard techniques like threshold cryptography for Smart-ID, the transition to quantum-safe primitives is more challenging and time-consuming. In this section, we will identify the main challenges of migrating services to post-quantum cryptography and suggest which post-quantum algorithms are most suitable.

The following challenges and propositions are grouped according to the technologies they apply to, where the technologies we focused on are the most fundamental ones for Estonian e-governance. Indeed, Lips et al. [44], referencing UN e-government surveys [45], [46], identify X-Road as the backbone of Estonian e-government. On top of it, a large number of diverse services have been built in both the public and the private sector. These services use the identification methods provided by X-Road to

28 https://news.err.ee/616732/potential-security-risk-could-affect-750-000-estonian-id-cards

interact with each other, while the end users depend on e-ID and underlying PKI to access them. To this mix we add another significant application: internet voting.

A. Smart-ID

Smart-ID provides users with authentication and digital signing functionality. These are both achieved using the RSA multi-prime signature scheme [47], which has separate key pairs for authentication and signing. Smart-ID protocol relies on threshold cryptography [48], meaning that the private (signing) key is split into two shares: one is stored on the user's mobile device, and the other is stored on the server. To create a signature, the mobile device and the server interact to apply their shares of the private key, producing a single signature that can be verified using a single public key. The main goal of the solution is to offer protection for the private key: an adversary obtaining only one private key share cannot create valid signatures.

The current protocol is built around the RSA signature scheme, because its mathematical structure supports the creation of such protocols. Unfortunately, the structure of post-quantum signature schemes does not allow such protocols to be created easily. Out of the three (future standard) signature schemes, Crystals-Dilithium has the best mathematical structure but includes a few challenging parts. First, it has the rejection sampling step, which aims to verify that the final signature does not leak information about the private key. If the verification does not pass, signing is restarted and repeated until a valid signature is created. The number of restarts is three or four (on average) for the to-be-standardized parameters. When the signing process is split into two parts, both the mobile device and the server must perform rejection sampling, increasing the number of restarts. Second, due to a more complicated signing algorithm, the number of communication rounds needed to produce a signature will be increased (compared to RSA). Vakarjuk et al. [49] attempt to create an alternative to the Smart-ID protocol using a lattice-based signature scheme similar to Crystals-Dilithium. However, unlike the current Smart-ID protocol, the verification algorithm is not the same as that of the standardized scheme.

For authentication, one does not necessarily have to use a standardized cryptographic algorithm. Hence a signature scheme with suitable properties may be chosen more freely. But for signing, compliance with standards is a strict requirement. Therefore, a threshold signature protocol should produce signatures that are verified using the verification algorithm in the standard.

Another approach toward quantum-safe Smart-ID is to use a "threshold-friendly" signature scheme. The NIST may standardize such a scheme in the future [50],[29] but waiting would delay post-quantum migration.

29 https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf

B. ID Card

The ID card is a state-issued identity document that allows using different e-services. The ID card is a compulsory document for Estonian citizens and European Union citizens who reside permanently in Estonia. The ID card gives its users different functionalities: providing authentication to various services, creating qualified electronic signatures, and encrypting/decrypting documents. The ID card contains two key pairs with corresponding certificates: one for digital signatures and the other for authentication and decryption. ID cards have limited memory and computational power, making the running of PQC algorithms difficult. Table IV presents a key and signature size comparison of pre-quantum and post-quantum algorithms that provide approximately the same level (approx. 128-bit) of security.

TABLE IV: SIZES IN BYTES

Algorithm	Public key	Private key	Signature
RSA3072	400	384	384
ECDSA P-256	32	32	64
Dilithium2	1312	2528	2420
Falcon-512	897	1281	666
XMSS-SHA2_16_256	64	2093	2692
Sphincs+	32	64	7856

For smartcards, protection against side-channel attacks is crucial. However, adding protection against side-channel attacks to the post-quantum cryptographic schemes adds complexity to the algorithms and increases the amount of random-access memory (RAM) needed to execute operations.

If migration via the hybrid approach is chosen, then ID cards would need to support the creation of both post-quantum and pre-quantum signatures, storing all the keys and certificates. Not all solutions from Section 2.E are suitable for smart cards. Memory limits the use of a multi-certificate solution, as it would require storing four certificates on a card. AltPublicKey or chameleon solutions are more suitable, as both allow interoperability with legacy systems while also permitting the creation of post-quantum signatures for updated systems.

The same considerations apply to Mobile-ID, as it also relies on a tamper-resistant chip to protect the key material. Furthermore, reducing the size of the signatures is important, because the communication with servers is SMS-based.

Moreover, the Estonian ID card uses the same key pair for both authentication and decryption [51]. Since we do not have an RSA post-quantum drop-in replacement, we would have to introduce an additional key pair. This leads to one more certificate being stored on the ID card.

C. X-Road

X-Road provides secure data exchange between different information systems in the public and private sectors. The identity of each organization is verified using certificates issued by the certification authorities. Data exchanged using X-Road is protected both at rest and at transit. Since X-Road is used to exchange data between the public sector information systems, long-term data protection is necessary. To hinder harvesting attacks, it is essential to start protecting data using the key derived with a post-quantum key establishment algorithm as soon as possible. BSI, ANSSI, and ETSI recommend using the Crystals-Kyber scheme in hybrid mode with ECDH to provide security against both classical and quantum adversaries.

A main component of the X-Road infrastructure is a *security server* that manages service calls and responses between different information systems. Each security server holds an authentication key pair to establish secure communication channels with other security servers and a signing key pair to sign all outgoing messages. Choosing the right hybrid mode for signing is less straightforward than for the key establishment. Signing and verification should be fast and the signature should be short, due to how signing is used in X-Road. A straightforward way is the concatenation of a pre-quantum (RSA or ECDSA) and a post-quantum (Crystals-Dilithium) signature. Using concatenation to combine two signatures guarantees unforgeability if at least one of the signature schemes is unforgeable [52]. This approach requires modifying security servers to produce and verify two signatures instead of one.

D. Public Key Infrastructure

For PKI, choosing a suitable post-quantum algorithm for digital signatures on the certificates is a challenging task. The hybrid modes for certificates are outlined in Section 2.E. There is also a *mixed architecture* solution that can be considered for the certificate chains. In mixed architecture, algorithms with stronger security guarantees are chosen for the long-lived objects such as root CAs; more efficient algorithms are selected for short-lived objects such as end-entity certificates or TLS handshakes. For example, hash-based signatures like Sphincs+ or XMSS/LMS can be used for root CAs, since they rely only on the security of underlying hash functions. For the other

certificates, schemes like Crystals-Dilithium or Falcon providing smaller signatures can be used. This type of solution would require services to support all the mentioned signature schemes.

The main obstacle Estonia faces in transferring to quantum-safe PKI is that it must rely on the other parties who contribute to the change—hardware security module vendors, certificate authorities, policymakers, and browser vendors.

E. I-voting

In the Estonian internet voting protocol, asymmetric cryptography is used to encrypt and sign the votes [53]. Further cryptographic techniques—mix-nets [54]—are used to break the visible links between individual votes that were cast and those that were counted. In this setting, the signature mechanisms are largely independent of the other used cryptographic constructions, while vote encryption and mix-nets are tightly coupled.

The signatures for votes are generated using the signature creation devices described above and obtain their legal meaning through the public-key infrastructure also described above. Hence, no adaptations specific to i-voting are necessary. The situation is quite different for encryption. Currently, the votes are encrypted using ElGamal encryption, and the mix-net protocol in use [55] has been designed to mix them. Neither the encryption nor the mix-net are post-quantum secure. The migration to PQC primarily involves the introduction of a post-quantum mix-net, which will fix the encryption algorithm that it can support. Constructions exist for such mix-nets, but they either do not have sufficient performance [56] or impose a significant change on the format of the votes and the design of the whole voting protocol [57].

The lack of suitable protocols becomes even more debilitating when considering hybrid approaches. We would need an encryption scheme whose security can be derived either from a well-studied pre-quantum hardness assumption or from a post-quantum hardness assumption. While such schemes can be constructed compositionally, the accompanying mix-nets probably cannot. We are also not aware of any research toward mix-nets for hybrid encryption schemes. Using a hybrid encryption scheme with a mix-net that is able to mix only a single layer of encryption defeats the purpose of using that scheme. At a minimum, it would leak the links between cast and counted votes if/when one of the encryption layers becomes insecure.

5. COMMONALITIES AND DIFFERENCES

Only a few obstacles are common to all the analyzed systems, which have different architecture, security, and regulatory requirements. Changes influencing all systems and applications are the increased size of keys, signatures, and ciphertexts. Additionally, our analysis shows that there is no one scheme that suits all use cases; thus, appropriate quantum-safe alternatives must be chosen based on the requirements and constraints of each individual system.

The following obstacles were identified in this paper:

1) The urgency of starting the post-quantum migration is not well understood by decision-makers and those outside the cryptographic community. Multiple parties from the private and public sectors are not contributing enough to the migration process, causing stagnation.
2) EuroQCI focuses attention on QKD technology, whose functionality is more limited than that provided by PQC.
3) Standardized post-quantum schemes are computationally more complex and storage-heavy and therefore less compatible with smart cards.
4) Side-channel attack protection for the post-quantum schemes is underdeveloped.
5) PQC in hybrid mode limits which hybrid certificate solutions can be deployed on smart cards.
6) The absence of an RSA-like scheme providing both signing and encryption requires changing decryption functionality on ID cards, increasing the code footprint.
7) Choosing suitable hybrid modes for signature schemes is more challenging, as certain security guarantees need to be ensured.
8) Some unexpected obstacles to implementing post-quantum schemes become obvious only in the later stages of the migration process—the implementation and testing phases.
9) Research is lacking on post-quantum cryptography for esoteric use cases such as i-voting and distributed signing (Smart-ID).

6. NEXT STEPS

In Section 4, we have identified the most suitable post-quantum schemes that can be used to replace the currently used cryptography. This can be used to prepare a full migration plan for Estonian e-services, also taking into account services not analyzed in this paper. The proposed post-quantum alternatives (including different

hybrid modes) should be tested within the systems to identify further challenges that are not obvious from the primary analysis. If necessary, other post-quantum schemes can be implemented to verify whether they fit better under the limitations identified during the testing phase. We propose that the (soon-to-be) standardized schemes be considered, because their security has been studied more carefully by the cryptographic community. The migration plan should also outline the order in which the various services are transitioned to PQC. The services dealing with more sensitive data that must stay secret for a long time should be the first to switch to quantum-safe alternatives.

In Section 2.A, we indicated that the migration of confidentiality mechanisms to PQC was the most urgent. Fortunately, it is also the easiest, at least from the point of view of coordination among the stakeholders (i.e., standardization). Indeed, to protect the data at rest, the party holding it may select the mechanisms alone. To protect data in transit, the two parties must agree on the algorithms and formats. They also must have a mechanism to authenticate each other.

Authentication is similar, requiring only the client and the relying party to coordinate. Indeed, proprietary solutions for authentication (e.g., Mobile-ID or Smart-ID) are proliferating even today. Digital signatures for non-repudiation, however, are very different. Here any solution must be compliant with legislation, which requires standardization, certification, and so on.

ACKNOWLEDGMENTS

This research has been supported by the Estonian Research Council, Grant No. PRG1780, and by the European Union under Grant Agreement No. 101087529. The views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

[1] M. P. Michele Mosca. “Quantum threat timeline report 2022.” Global Risk Institute. Accessed: Mar. 11, 2024. [Online]. Available: https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

[2] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, IEEE, 1994, pp. 124–134.

[3] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.

[4] NIST Computer Security Division. “Announcing request for nominations for public-key post-quantum cryptographic algorithms.” NIST. Dec. 20, 2016. [Online]. Available: https://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms
[5] S. Beauregard, “Circuit for Shor’s algorithm using 2n+3 qubits,” *Quantum Info. Comput*., vol. 3, no. 2, pp. 175–185, Mar. 2003.
[6] U. Skosana and M. Tame, “Demonstration of Shor’s factoring algorithm for N=21 on IBM quantum processors,” *Scientific Reports*, vol. 11, p. 16599, Jan. 2023.
[7] C. Gidney and M. Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” *Quantum*, vol. 5, p. 433, 2021, doi: 10.22331/Q-2021-04-15-433.
[8] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982, doi: 10.1038/299802a0.
[9] I. Georgescu, “25 years of quantum error correction,” *Nature Reviews Physics*, vol. 2, no. 10, p. 519, Oct. 2020, doi: 10.1038/s42254-020-0244-y.
[10] J. Dargan, “What types of quantum computers exist in 2023?” *Quantum Insider*, Jun. 2023. [Online]. Available: https://thequantuminsider.com/2023/06/06/types-of-quantum-computers/
[11] P. Kampanakis and T. Lepoint, “Vision paper: Do we need to change some things? Open questions posed by the upcoming post-quantum migration to existing standards and deployments,” in *Security Standardization Research – 8th International Conference*, SSR 2023, Lyon, France, Apr. 22–23, 2023, pp. 78–102, doi: 10.1007/978-3-031-30731-7_4.
[12] “The PQC Migration Handbook. Guidelines for Migrating to post-quantum cryptography,” Dutch Organization for Applied Scientific Research, Dec. 2023. [Online]. Available: https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/
[13] D. Stebila and M. Mosca, “Post-quantum key exchange for the Internet and the Open Quantum Safe project,” in *Selected Areas in Cryptography (SAC) 2016*, vol. 10532, R. Avanzi and H. Heys, Eds., Springer, 2017, pp. 1–24. [Online]. Available: https://openquantumsafe.org
[14] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014.
[15] G. Alagic et al., “Status report on the third round of the NIST post-quantum cryptography standardization process,” U.S. Department of Commerce, National Institute of Standards and Technology, Jul. 2022, doi: 10.6028/NIST.IR.8413-upd1.
[16] “Module-lattice-based key-encapsulation mechanism standard (initial public draft).” FIPS PUB 203. [Online]. Available: https://csrc.nist.gov/pubs/fips/203/ipd, Aug. 2023.
[17] “Module-lattice-based digital signature standard (initial public draft).” FIPS PUB 204. Aug. 2023. [Online]. Available: https://csrc.nist.gov/pubs/fips/204/ipd
[18] “Stateless hash-based digital signature standard (initial public draft).” FIPS PUB 205. Aug. 2023. [Online]. Available: https://csrc.nist.gov/pubs/fips/205/ipd
[19] P.-A. Fouque et al. “Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Specification v1.2.” Falcon. Oct. 2020. [Online]. Available: https://falcon-sign.info
[20] D. J. Bernstein et al. “Classic McEliece: conservative code-based cryptography: Cryptosystem specification.” Classic McEliece. Oct. 2022. [Online]. Available: https://classic.mceliece.org
[21] N. Aragon et al. “BIKE – Bit Flipping Key Encapsulation. Round 4 submission,” Bike. Oct. 2022. [Online]. Available: https://bikesuite.org/
[22] C. Aguilar Melchor et al. “Hamming quasi-cyclic (HQC). Fourth round submission.” PQC HQC. Apr. 2023. [Online]. Available: https://pqc-hqc.org
[23] “Stateful hash-based signatures.” NIST. Accessed: Mar. 11, 2024. [Online]. Available: https://csrc.nist.gov/projects/stateful-hash-based-signatures
[24] J. Kelsey, S. Lucks, and N. Lang, “Coalition and threshold hash-based signatures,” Cryptology ePrint Archive, Paper 2022/241, 2022. [Online]. Available: https://eprint.iacr.org/2022/241
[25] BSI, “Cryptographic mechanisms: Recommendations and key lengths,” BSI Technical Guideline TR-02102-1, Jan. 2023. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.html
[26] ANSSI. “ANSSI views on the Post-Quantum Cryptography transition (2023 follow up).” French Cybersecurity Agency (ANSSI). Oct. 2023. [Online]. Available: https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography
[27] John H. “Migrating to post-quantum cryptography.” National Cyber Security Centre blog post. Nov. 2023. [Online]. Available: https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc
[28] E. Alkim et al. “FrodoKEM: Learning with errors key encapsulation. preliminary standardization proposal.” FrodoKEM. Mar. 2023. [Online]. Available: https://frodokem.org

[29] “ETSI TS 103 744. CYBER; Quantum-safe hybrid key exchanges.” Dec. 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.01.01_60/ts_103744v010101p.pdf
[30] E. Barker, L. Chen, and R. Davis, “Recommendation for key-derivation methods in key-establishment schemes,” National Institute of Standards and Technology, Aug. 2020, doi: 10.6028/nist.sp.800-56cr2.
[31] M. Ounsworth, “Post-quantum multi-key mechanisms for PKIX-like protocols: Problem statement and overview of solution space,” Internet Engineering Task Force, Internet-Draft draft-pq-pkix-problem-statement-01, Sep. 2019. [Online]. Available: https://datatracker.ietf.org/doc/draft-pq-pkix-problem-statement/01/
[32] “X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.” International Telecommunication Union (ITU). Oct. 2019. [Online]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509
[33] C. Bonnell, J. Gray, D. Hook, T. Okubo, and M. Ounsworth, “A mechanism for encoding differences in paired certificates,” Internet Engineering Task Force, Internet-Draft draft-bonnell-lamps-chameleon-certs-03, Jan. 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-bonnell-lamps-chameleon-certs/03/
[34] M. Ounsworth, J. Gray, M. Pala, and J. Klaußner, “Composite signatures for use in Internet PKI,” Internet Engineering Task Force, Internet-Draft draft-ounsworth-pq-composite-sigs-11, Dec. 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-ounsworth-pq-composite-sigs/11/
[35] “CYBER; Migration strategies and recommendations to Quantum Safe schemes,” ETSI, 2020. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf
[36] H. M. Steffen, G. Land, L. J. Kogelheide, and T. Güneysu, “Breaking and protecting the crystal: Side-channel analysis of dilithium in hardware,” in *Post-Quantum Cryptography – 14th International Workshop, PQCrypto 2023*, College Park, MD, USA, August 16–18, 2023, pp. 688–711, doi: 10.1007/978-3-031-40003-2_25.
[37] S. Marzougui, V. Ulitzsch, M. Tibouchi, and J.-P. Seifert, “Profiling Side-Channel Attacks on Dilithium: A Small Bit-Fiddling Leak Breaks It All,” Cryptology ePrint Archive, Paper 2022/106, 2022. [Online]. Available: https://eprint.iacr.org/2022/106
[38] Y. Ji, R. Wang, K. Ngo, E. Dubrova, and L. Backlund, “A side-channel attack on a hardware implementation of CRYSTALS-Kyber,” in *IEEE European Test Symposium*, ETS 2023, Venice, Italy, May 22–26, 2023, pp. 1–5, doi: 10.1109/ETS56758.2023.10174000.
[39] A. Wagner, V. Wesselkamp, F. Oberhansl, M. Schink, and E. Strieder, “Faulting Winternitz one-time signatures to forge LMS, XMSS, or SPHINCS+ signatures,” in *Post-Quantum Cryptography – 14th International Workshop, PQCrypto 2023*, College Park, MD, USA, Aug. 16–18, 2023, pp. 658–687, doi: 10.1007/978-3-031-40003-2_24.
[40] “ETSI EN 319 132-1. Electronic signatures and infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures.” ETSI. Feb. 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.02.01_60/en_31913201v010201p.pdf
[41] M. Geihs, “Long-term protection of integrity and confidentiality—security foundations and system constructions,” PhD thesis, Darmstadt University of Technology, Germany, 2018. [Online]. Available: http://tuprints.ulb.tu-darmstadt.de/8094/
[42] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, G. L. Miller, Ed., Philadelphia, Pennsylvania, USA, May 22–24, 1996, pp. 212–219, doi: 10.1145/237814.237866.
[43] L. Chen et al., “Report on post-quantum cryptography,” National Institute of Standards and Technology Internal Report 8105,” Apr. 2016, doi: 10.6028/NIST.IR.8105
[44] S. Lips, V. Tsap, N. Bharosa, R. Krimmer, T. Tammet, and D. Draheim, “Management of national eID infrastructure as a state-critical asset and public-private partnership: Learning from the case of Estonia,” *Inf. Syst. Frontiers*, vol. 25, no. 6, pp. 2439–2456, 2023, doi: 10.1007/S10796-022-10363-5.
[45] UN Department of Economic and Social Affairs, “United Nations e-government survey 2018 – Gearing e-government to support transformation towards sustainable and resilient societies,” United Nations, New York, 2018.
[46] UN Department of Economic and Social Affairs, “E-government survey – Digital government in the decade of action for sustainable development,” United Nations, New York, 2020.
[47] A. Buldas, A. Kalu, P. Laud, and M. Oruaas, “Server-supported RSA signatures for mobile devices,” in *Computer security – ESORICS 2017*, Cham: Springer International Publishing, 2017, pp. 315–333.
[48] Y. Desmedt, “Society and group oriented cryptography: A new concept,” in *Advances in Cryptology—CRYPTO ’87*, Berlin, Heidelberg: Springer, 1988, pp. 120–127.

[49] J. Vakarjuk, N. Snetkov, and J. Willemson, "DiLizium: A two-party lattice-based signature scheme," *Entropy*, vol. 23, no. 8, p. 989, 2021.
[50] R. Peralta and L. T. A. N. Brandão, "NIST first call for multi-party threshold schemes," NIST – National Institute of Standards and Technology, Jan. 2023, doi: 10.6028/nist.ir.8214c.ipd.
[51] "CDOC 2.0 spetsifikatsioon. v0.9." Cybernetica AS. Jan. 2023. [Online]. Available: https://installer.id.ee/media/cdoc/cdoc_2_0_spetsifikatsioon_d-19-12_v1.9.pdf
[52] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," Cryptology ePrint Archive, Paper 2017/460, 2017. [Online]. Available: https://eprint.iacr.org/2017/460
[53] S. Heiberg, T. Martens, P. Vinkel, and J. Willemson, "Improving the verifiability of the Estonian internet voting scheme," in *Electronic Voting – First International Joint Conference, e-Vote-ID 2016*, Bregenz, Austria, Oct. 18–21, 2016, pp. 92–107, doi: 10.1007/978-3-319-52240-1_6.
[54] M. Abe, "Universally verifiable mix-net with verification work independent of the number of mix-servers," in *Advances in Cryptology – EUROCRYPT '98, International Conference on the Theory and Application of Cryptographic Techniques*, Espoo, Finland, May 31 – Jun. 4, 1998, pp. 437–447, doi: 10.1007/BFB0054144.
[55] D. Wikström, "A sender verifiable mix-net and a new proof of a shuffle," in *Advances in Cryptology – ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security*, Chennai, India, Dec. 4–8, 2005, pp. 273–292, doi: 10.1007/11593447_15.
[56] V. Farzaliyev, J. Willemson, and J. K. Kaasik, "Improved lattice-based mix-nets for electronic voting," *IET Inf. Secur.*, vol. 17, no. 1, pp. 18–34, 2023, doi: 10.1049/ISE2.12089.
[57] X. Boyen, T. Haines, and J. Müller, "A verifiable and practical lattice-based decryption mix net with external auditing," in *Computer Security – ESORICS 2020: Proceedings of the 25th European Symposium on Research in Computer Security, Part II*, Guildford, UK, Sep. 14–18, 2020, pp. 336–356, doi: 10.1007/978-3-030-59013-0_17.