JeDEM Issue 16 (3): 50-79, 2024
ISSN 2075-9517
http://www.jedem.org
Date of submission: 31.05.2024
Date of acceptance: 30.09.2024
Article DOI: 10.29379/jedem.v16i3.928

An electoral exception? Quantum computing - readiness and internet voting

Adrià Rodríguez-Pérez

ORCID Nr: 0000-0002-5581-1340
CNSC Research Group, Universitat Oberta de Catalunya, Rambla del Poblenou, 156, 08018 Barcelona, arodriguezperez4@uoc.edu

Núria Costa

ORCID Nr: 0000-0003-2204-5069
Information and Communication Technologies Engineering (ETIC), Universitat Pompeu Fabra, Roc Boronat, 138, 08018 Barcelona, nuria.costa@upf.edu

Tamara Finogina

ORCID Nr: 0000-0003-4771-0635
Internxt, Edificio Lanzadera, Carrer del Moll de la Duana, s/n, Poblados Marítimos, 46024 Valencia, tamara@internxt.com

Abstract: Developments in quantum computing may jeopardize the security of internet voting. Such developments could compromise important electoral requirements, including integrity, eligibility, or the secrecy of the vote. Even the contents of a vote cast online today, when quantum computers are not yet known to be available, could be revealed tomorrow. Countries are already working on a post-quantum setting, but elections seem to remain an exception. In this paper, we explore the existing strategies to mitigate the quantum threat or their lack thereof, as well as the views of different stakeholders on these matters. To do so, we have conducted a mix of desk research as well as interviews with 24 experts in different fields, from electoral administrations to cybersecurity agencies, vendors, and academia. We assess their perceptions about quantum computing, its impact on internet voting, and on transitioning towards quantum-resistant cryptography, as well as on interagency cooperation and trust issues. Whereas we initially assumed that elections were an exception in regards to the transition towards post-quantum cryptography, this research shows that the electoral field is neither alone nor the most adequate one to start the implementation of this kind of cryptography.

Keywords: internet voting, i-voting, electronic voting, e-voting, quantum computing, post-quantum cryptography, cybersecurity, standardization

1. Introduction

Quantum computing is a technology that leverages the laws of quantum mechanics to solve problems too complex for classical computers. The first significant contribution to the development of quantum computing occurred in the eighties when Richard Feynman (1982) postulated that to simulate the evolution of quantum systems efficiently, we would need to build quantum computers (computational machines that use quantum effects). Nevertheless, it was not until 1994 that the view on quantum computing changed. Peter Shor (1994) developed a polynomial time quantum algorithm, allowing quantum computers to efficiently factorize large integers exponentially quicker than the best classical algorithm on traditional machines. This turned a problem that is computationally intractable by conventional computers into one that can be solved in just a few hours by a large enough quantum computer. It is widely known that key exchange protocols based on variants of the Diffie-Hellman and the RSA protocols, which are the basis for the security of most of today's computers and networks, would be insecure if a fault-tolerant large-scale quantum computer is ever built.

For this reason, although quantum computing has been a topic of interest for scientists and researchers for many years, it is currently attracting considerable attention from other sectors. Large tech companies are intensively working to build a large-scale quantum device. IBM (Hackett, 2020) predicts having a 1 million qubits quantum computer by 2030 and Google (Wang, 2021) by 2029, both working on superconducting qubits. Also, the start-up PsiQuantum (Wang, 2020) is planning to make a one million photonic qubits quantum computer with error correction (about 1000 error-corrected qubits) by 2025. Renowned organizations such as the National Institute of Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA) in the United States (US), and the French Agence nationale de la sécurité des systèmes d'information (ANSSI) are strongly recommending to start preparing for the quantum era by transitioning to post-quantum cryptography, and governments are investing millions on this emerging technology. Nevertheless, although it seems that quantum computing is getting closer to becoming a stable technology, there are still several challenges to overcome that generate some skepticism. Quantum skeptics argue that, although experimental research is beneficial and may lead to a better understanding of complicated quantum systems, it is physically impossible to build scalable quantum computers (NASEM, 2019).

As it has been studied elsewhere (Rodríguez-Pérez, Costa & Finogina, forthcoming) the field of elections, and more specifically that of internet voting, finds itself amidst these two positions: on the one hand, national cybersecurity agencies (including in countries where internet voting is being used) are already working on quantum-resistant alternatives; on the other hand, internet voting systems used in politically binding elections remain vulnerable to the threat of quantum computing, which could jeopardize the basic requirements of democratic elections: principles such as secrecy, integrity, eligibility, and (in the case of internet voting) verifiability are at stake.

This paper explores views and positions among electoral and non-electoral stakeholders when it comes to the developments of quantum computing and its potential impact in the electoral field. To do so, we explore how electoral and non-electoral administrations, as well as private actors, such as companies and academia, foresee these technological developments, are preparing themselves to address the risk posed by quantum computers, and have different views on these topics based on their unique perspectives. To do so, the next section of the paper provides an overview of mitigation strategies against the development of quantum computing worldwide. We pay special attention to how non-electoral stakeholders (i.e., cybersecurity and standardization agencies) in countries where internet voting is currently being used in governmental elections are preparing to address potential challenges. More specifically, we look at the strategies in Canada, Estonia, France, and Switzerland. Following, we summarize the findings stemming from 18 interviews with 24 experts in different fields, from electoral administrations to cybersecurity agencies and vendors, to try to grasp their (different) perceptions on these issues as well as to understand the reasons for such heterogeneous views.

2. Is quantum computing an actual threat? Assumptions, theoretical attacks, and the transition toward quantum-resistant cryptography

Views on quantum computing are, today, still quite heterogeneous. As shown, private for-profit companies claim to have advanced substantially in developing quantum computers or even aim at commercializing quantum-resistant solutions. In contrast, academia often assumes a more skeptical stance. In turn, and despite the diversity of opinions, the position of key cybersecurity agencies evidence that the field of quantum computing is in constant evolution, opening up new technological horizons and that we should be prepared in case a useful quantum computer is built since the transition to post-quantum algorithms is far from immediate. Moreover, it is not only about being prepared the day someone announces the first quantum computer but also about securing data now, which must be protected long-term. Harvest now, decrypt later attacks, also known as store now, decrypt later, or retrospective decryption, refers to a cybersecurity attack in which encrypted data is collected today and decrypted in the future when quantum computing achieves a maturity level capable of breaking the underlying mathematical problem of the encryption scheme. In a survey (Riley, 2020) conducted by Deloitte of 400 professionals from organizations that have considered quantum computing benefits, half considered their organizations vulnerable to this kind of attack.

In the internet voting context, this threat directly affects secret suffrage and, more specifically, long-term privacy since an adversary could learn how a person voted some years ago, which may have political as well as personal implications (e.g., in the case of in-family coercion). Voting data can be intercepted either because it has been published in a public bulletin board or accessed by auditors or because it has somehow been eavesdropped or leaked by internal attackers. As we will show in the next sections, internet voting systems, and especially those that are end-to-end verifiable, are vulnerable to such attacks. In this context, why is end-to-end verifiability explored by governments, whilst long-term privacy is not? This section aims to take stock of the wider developments

across the globe to prepare for the arrival of quantum computing and its capabilities to break conventional cryptography.

2.1. The NIST competition, the US National Security Memorandum, and the Recommendation from the European Commission

The importance of advancing quantum-resistant solutions is not just an academic concern. However, standardization efforts have been advanced in this regard, and in recent months we have also seen important steps being taken by governments around the World. In this section, we provide an overview of the NIST competition for the standardization of post-quantum cryptographic primitives[1], as well as initiatives taken by the US federal government as well as the EU to understand their views on the threat posed by quantum computing.

NIST's concern about the threat of quantum computing can be traced back probably before 2015, when, being aware that quantum computers would break a few of NIST's standardized crypto algorithms, the organization tasked a team of researchers to find new ones to replace them (Moody, 2020). After reading about the topic, talking to experts, and doing some research, in 2015, the agency organized a first seminar on 'cybersecurity in a post-quantum world'[2]. The result of this seminar was a report (Chen et al., 2016) that called for organizing a public competition to standardize a new set of post-quantum cryptographic algorithms. In their report, the organization acknowledges the progress that quantum computing has made in recent years and the risk it represents for crucial communication protocols whose security relies on the discrete logarithm and the factorization problem. While estimating the precise timing when scalable quantum computers will be ready is challenging, experts have already started making predictions. Therefore, the report suggested that we must start preparing our information security systems sooner rather than later to withstand quantum computing. The proposal consisted of switching to new post-quantum cryptosystems, although the organization recognized the difficulty of this transition, particularly due to the fact that quantum-resistant algorithms require larger key sizes compared to traditional algorithms and therefore, they "...emphasizes the need for agencies to focus on crypto agility". Recognizing the significant effort put into developing quantum-resistant technologies, NIST recognized the urgency for standardizing new post-quantum public key cryptography. The preliminary details of the NIST PQC Standardization Process were announced in a presentation at PQCrypto 2016 (Moody, 2016).

NIST published the submission requirements and evaluation criteria on 2 August 2016, and then, on 20 December 2016, the agency launched the process to request, evaluate, and standardize one or

[1] Since the paper was submitted for review, NIST has published the Federal Information Processing Standards (FIPS) for post-quantum cryptography. Therefore, the standards were yet available at the time of conducting the review. This is important both for this section as well as in regards to the interviews conducted and explained below. See: NIST Releases First 3 Finalized Post-Quantum Encryption Standards, https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[2] NIST Workshop on Cybersecurity in a Post-Quantum World, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2-3, 2015, https://csrc.nist.gov/Events/2015/Workshop-on-Cybersecurity-in-aPost-Quantum-World

more quantum-resistant public-key cryptographic algorithms (NIST, 2016). Eighty-two schemes were submitted during the first round[3], and, out of these, 69 passed the first evaluation: 20 digital signature schemes and 49 public-key encryption or key encapsulation mechanisms. After the first round, 26 schemes were approved, and this number was reduced to seven after the second round (four public key encryption and key establishment algorithms and three digital signature algorithms), plus eight alternate algorithms[4]. The third round began in July 2020 and, as in the previous rounds, both the candidates and the alternates were invited to present and update on their candidate algorithm in the NIST PQC Standardization Conference, which was held virtually in June 2021[5]. During this round, the theoretical and empirical data that supported the candidates' security were examined in greater detail. Additionally, meticulous benchmarking was done.

After the three iterations, NIST selected four algorithms to be standardized: CRYSTALS-KYBER as the public-key encapsulation mechanism (KEM) and CRYSTALS-Dilithium[6], FALCON[7], and SPHINCS+[8] as the digital signature schemes, being the former the primary algorithm recommended to be implemented. Cost and performance were important selection criteria when deciding which algorithms to standardize. In selecting the most appropriate KEM algorithm, NIST also considered the security assumption underlying each algorithm, which in the case of CRYSTALS-KYBER was more convincing than NTRU or Saber (there may be more evidence supporting the MLWE problem compared to the NTRU or MLWR assumptions). In terms of signature schemes, NIST decided to prioritize the standardization of CRYSTALS-Dilithium due to its high efficiency, simple design, and strong security guarantees. However, the organization recognizes4 that this could be a barrier to moving to post-quantum signature schemes for some applications. For this reason, they have also chosen FALCON as the algorithm to be standardized, which requires more resources than Dilithium but gives better overall performance on unconstrained devices. Finally, in order not to rely entirely on lattices, NIST selected a stateless hash-based signature scheme (SPHINCS+) also to be standardized. However, it is worse in terms of cost and performance than the lattice-based candidates.

Regarding the alternate candidates, only four of the KEM algorithms (BIKE[9], Classic McEliece[10], HQC[11], and SIKE[12]) advanced to the fourth round of evaluation. Nevertheless, the latter was proven insecure in 2022 by Castryck and Decru (Castryck & Decru, 2022), who presented a key recovery attack on the Supersingular Isogeny Diffie-Hellman protocol[13]. In parallel to the fourth round, NIST

[3] Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303
[4] Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf
[5] Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf
[6] Cryptographic Suite for Algebraic Lattices, https://pq-crystals.org/
[7] Fast-Fourier Lattice-based Compact Signatures based on NTRU, https://falcon-sign.info/
[8] Stateless Hash-based signatures, https://sphincs.org/
[9] Bit Flipping Key Encapsulation, https://bikesuite.org/
[10] Classic McEliece, https://classic.mceliece.org/
[11] Hamming Quasi-Cyclic, https://pqc-hqc.org/
[12] Supersingular Isonegy Key Encapsulation, https://sike.org/
[13] Round 4 Submissions, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

announced a new call for additional digital signature schemes for the post-quantum cryptography standardization process[14]. The submission period closed on the first of June 2023, and after the first round, 40 proposals were accepted. Finally, last August, NIST released three draft FIPS for public comments: Module-Lattice-based Key-Encapsulation Mechanism Standard (FIPS 203) (NIST, 2023a), Module-Lattice-based Digital Signature Standard (FIPS 204) (NIST, 2023b) and Stateless Hash-based Digital Signature Standard (FIPS 205) (NIST, 2023c). The comment period lasted four months, and the next steps consisted of revising the draft based on comments, a final review, approval, and the promulgation process.

The NIST competition for the standardization of quantum-resistant algorithms is not an isolated effort by the US government to future-proof its digital infrastructure and support its industries. Likewise, NIST is only one of the entities authorized by the National Quantum Initiative Act (NQI Act) to strengthen Quantum Information Science (QIS) Programs, Centers, and Consortia. The NQI Act was signed into law by then-President Trump on December 21st, 2018, to accelerate quantum research and development for the economic and national security of the United States. It calls for coordination through the National Science and Technology Council (NSTC) Subcommittee on Quantum Information Science (SCQIS) and the NSTC Subcommittee on Economic and Security Implications of Quantum Science (ESIX). It also legislates the formation of the National Quantum Initiative Advisory Committee (NQIAC) and establishes the National Quantum Coordination Office. The NQIAC was originally set up in 2019 by President Trump in Executive Order 13885 (Exec. Order No. 13885, 2019) and reconstituted by President Biden in Executive Order 14073 on May 4, 2022 (Exec. Order No. 14073, 2022), elevating "the committee to a presidential advisory committee, highlighting that the National Quantum Initiative is a whole-of-government effort that rises above any one Federal agency"[15].

At the same time, the US Office of Management and Budget (OMB) issued a National Security Memorandum which "[...] describes preparatory steps for agencies to undertake as they begin their transition to PQC by conducting a prioritized inventory of cryptographic systems. Further, this memorandum provides transitional guidance to agencies in the period before PQC standards are finalized by the National Institute of Standards and Technology (NIST) [...]" (Young, 2022). The memorandum also requires all Federal Agencies to submit an inventory of their cryptographic systems susceptible to artificial intelligence (AI) by May 4, 2023, and then annually until 2035. The main motivation behind all these initiatives is that encrypted data can be recorded now and decrypted later using quantum computers, i.e., retrospective decryption. As Dylan Presman, the office's Director for Budget and Assessment, explained during the ATARC's Quantum Speaker Series "Quantum computers will be mature enough in 20 to 30 years [...] However, it's not just about when quantum computers will be ready, it's about the shelf life of data."

[14] Post-Quantum Cryptography: Digital Signature Schemes. Call for proposals, https://csrc.nist.gov/Projects/pqc-dig-sig/standardization/call-for-proposals

[15] National Quantum Initiative Advisory Committee (NQIAC), https://www.quantum.gov/about/nqiac/

On the other side of the Atlantic, the EU has also stepped up its efforts to prepare for the quantum threat. In April 2024, the European Commission recently adopted a Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. The Recommendation upholds "encryption as a key technology for achieving resilience, technological sovereignty and for building operational capacity to prevent cyberattacks" (European Commission, 2024: para. 2) and acknowledges that "[t]he race pursued by various countries and private entities for developing quantum computing capabilities, and unlocking new potentially rewarding opportunities, poses threats to current cryptographic standards" (European Commission, 2024: para. 2). Therefore, the Commission calls for "switching to Post-Quantum Cryptography as swiftly as possible" (European Commission, 2024: para. 3) as a potential alternative. Among the key recommendations, establishing a sub-group on Post-Quantum Cryptography within the NIS Cooperation Group and publishing a Post-Quantum Cryptography Coordinated Implementation Roadmap by April 2026 should be noted. As is the case for the U.S.' strategies, the Recommendation builds on previous initiatives, spanning from research and innovation funding into post-quantum to, and possibly more importantly, a previous report on quantum computing and post-quantum cryptography by its cybersecurity agency, ENISA (Beullens et al., 2021).

2.2. The electoral exception? On the (absent) remedies to quantum computing in four case studies

Internet voting systems remain highly vulnerable despite the steps being taken to prepare for the quantum threat. Their protocols are built based on public-key cryptography to ensure the secrecy of the vote, the eligibility of the voters, and the integrity of the process, to mention just a few examples. Therefore, their security is based on conventional mathematical problems that will not withstand a quantum computer. This is striking because, as we have seen, cybersecurity agencies are already working on quantum-sage alternatives – also in the countries where internet voting is being used. Why is that so? Is there maybe an "electoral exception" when it comes to future-proofing internet voting systems? In this section, we aim to answer this conundrum by exploring the developments in four case studies: Canada, France, Estonia, and Switzerland.

2.2.1. Canada

Several steps are being taken in the North American country in order to address the challenges posed by quantum computers, which considers itself "one of the first countries in the world to prioritize quantum research" (National Research Council Canada, 2021). For example, back in 2021, the Canadian Centre for Cyber Security published some guidance on how to protect digital infrastructures against quantum computing published guidance (2021). The guidance is rather short, but several points are worth highlighting. For example, according to their estimates, quantum computers could be available as soon as 2030, meaning six years from now (9 years since the report was published). The Center also identifies retrospective decryption as a potential technique leveraged by an attacker and stresses that data that needs to be protected in 10 or more years (i.e., what they refer to as their lifespan) could be compromised. Additionally, they also note that a quantum computer would allow an attacker "to impersonate trusted systems (e.g., app store or

trusted vendor) to deliver fake software updates and gain access to systems of interest" (Canadian Centre for Cyber Security, 2021).

Whereas the 2021 guidance felt short of prescribing a transition towards post-quantum algorithms, they recommended an eight-step mitigation plan for quantum-preparedness, spanning from evaluating the sensitivity of the information to determine its lifespan to developing plans to transition to quantum-resistant cryptography once it becomes available. Amongst others, they suggest budgeting for potential software and hardware updates, educating on the emerging quantum threat and future quantum technologies, as well as asking vendors about their plans to implement quantum safe cryptography. More recently, in a presentation at the 2023 Post-Quantum Cryptography Conference held in March, it seems that the Centre for Cyber Security was planning to start its transition already in 2026-2027, not excluding the use of hybrid encryption[16].

In parallel, the Canadian Forum for Digital Infrastructure Resilience (CFDIR) has also taken some steps to prepare for the quantum threat. Established by the Innovation, Science and Economic Development Canada, a federal institution, the CFDIR set up a Quantum-Readiness Working Group (QRWG) that, in July 2021, published a report on the Canadian National Quantum-Readiness, including best practices and guidelines. Likewise, the National Research Council also has a program on post-quantum cryptography.

2.2.2. Estonia

In the case of Estonia, important advances are being made in the development and quantum computing preparedness, especially in the last few years. In 2019, the Estonian Information System Authority Annual Cyber Security Assessment mentioned the need for quantum-related research. Shortly after, in 2020, Estonia joined the EU's Cooperation framework on Quantum Communication Infrastructure[17]. The declaration aims to explore, with other EU member states over the next 12 months, how to develop and deploy a quantum communication infrastructure (QCI) across the EU within the next ten years. More recently, Estonia has also signed the European Declaration on Quantum Technologies. The declaration recognizes the strategic importance of quantum technologies for the scientific and industrial competitiveness of the EU and commits to collaborate on the development of a world-class quantum technology ecosystem across Europe.

Notwithstanding, the key players in these endeavors are academia and private companies. For example, in 2021, The University of Tartu's Institute of Computer Science and the company Cybernetica started a collaboration to create new data security solutions that would also protect data in

[16] How the Canadian Government is Preparing for PQC, https://pkic.org/events/2023/post-quantum-cryptography-conference/pkic-pqcc-how-gc-preparing-for-pqc-melanie-anderson-jonathan-hammell-canadian-government.pdf

[17] Estonia joined the EU's Cooperation framework on Quantum Communication Infrastructure, https://www.mkm.ee/en/news/estonia-joined-eus-cooperation-framework-quantum-communication-infrastructure

the era of quantum computers[18]. As part of the collaboration, they opened an industrial doctorate position focusing on new cryptographic algorithms for internet voting. In April 2022, a new project, NordIQuEst, started. It stands for Nordic-Estonian Quantum Computing e-Infrastructure Quest, and its purpose is to build a Nordic ecosystem that combines high-performance computing and quantum computing[19]. The idea behind the project is to join resources for the quantum race because none of them could alone match the bigger countries like the U.S. or China. In January 2023, Estonia and South Moravia started to develop a joint cross-border cybersecurity research and innovation strategy, focusing on six challenge areas: Internet of Secure Things (IoST), security certification, verification of trustworthy software, security preservation in blockchain, post-quantum cryptography and human-centric aspects of cybersecurity[20].

2.2.3. France

The quantum threat is attracting a great deal of interest in France. Academia is actively participating in the design and security analysis of protocols, the government is investing in research projects and quantum technologies, and the National Cybersecurity Authority (ANSSI) is closely following the progress on post-quantum cryptography and intensively working on publishing recommendations for making quantum-secure making products quantum secure.

In 2022, the ANSSI published their views on the transition to post-quantum cryptography (ANSSI, 2022), and one year later, a follow-up position paper (ANSSI, 2023) on the same topic. In this report, ANSSI declares that although post-quantum cryptography has gained much attention in past years, algorithms are still immature on different levels. For this reason, they propose a smooth transition from classical to post-quantum algorithms instead of a direct drop-in replacement. More concretely, they recommend using hybrid protocols in the short and medium term, combining well-known and well-studied classical public key algorithms based on factorization and discrete logarithm with post-quantum algorithms. The only exception ANSSI considers can be used without a hybrid approach is those systems where the security relies on hashed-based signatures since the underlying mathematical problem is well-studied.

The French agency proposed a gradual transition, which is well-detailed in a roadmap and consists of three phases. The idea of phase 1 is to start deploying the first post-quantum systems while using hybrid mechanisms to preserve pre-quantum security. Then, post-quantum security is considered as an optional "defense-in-depth", which changes during phase 2 (planned to start around 2024-2025), where quantum resistance could be claimed as a feature. Furthermore, during this second phase, ANSSI highly recommends the post-quantum transition of systems claiming long-term security. Finally, during phase 3, which is expected to start after 2030, it would be possible to use

[18] University of Tartu and Cybernetica cooperate to study quantum-safe cryptography, https://sciencebusiness.net/network-updates/university-tartu-and-cybernetica-cooperate-study-quantum-safe-cryptography

[19] See the NordIQuEst project, https://nordiquest.net/about; The Nordic e-Infrastructure Collaboration, https://neic.no/news/2022/08/19/nordiquest-has-started/

[20] Cyber-security Excellence Hub in Estonia and South Moravia, https://cordis.europa.eu/project/id/101087529

post-quantum schemes without hybridization (assuming they will provide at least the same security assurance level as classical algorithms). As ANSSI also mentions in their position paper (ANSSI, 2022), a particularly relevant feature for this post-quantum transition is crypto-agility, which refers to the ability of cryptosystems to "[...] update its cryptographic algorithms without recalling it or substituting it with a new one". The BSI (Federal Office for Information Security, 2020) and NCSC, the German and British counterparts of ANSSI correspondingly, have similar views on many issues, such as the migrations and the necessity to start using hybrid systems or crypto-agility.

Not only cybersecurity agencies but also governments are recommending preparing the post-quantum transition and actively contributing to it by investing in research projects and quantum computing. For example, in 2021, the French government announced a five-year investment plan of 1.8 million euros for quantum technologies[21].

2.2.4. Switzerland

Out of our sample of countries, Switzerland is the only case where the risk posed by quantum computers is explicitly acknowledged. The risk has been identified, consistently and in almost identical terms, in the Federal Chancellery's risk assessments since March 2023 (there have been follow-up reports published in July and November 2023, as well as in April 2024). Overall, the assessments acknowledge the risk posed by quantum computers but stress the difficulties in predicting the evolution of this technology. Notwithstanding, in the last assessment they mention that, according to IBM claims, the company could have a computer capable of breaking a 2048 bits RSA key as soon as in 2025. In any case, they still consider that the overall likelihood of such developments, together with the fact that Swiss Post's voting system uses keys that are 3072-bit long, render low the probability of this risk materializing. Likewise, because it is unfeasible to "predict the future", they suggest keeping an eye on technological developments and adopting the necessary technical measures once they become available.

Interestingly, a closer look at the examination of the Swiss Post's voting system shows that some experts already raised the issue of quantum computing as soon as November 2021. For example, in his assessment of the symbolic proofs for Swiss Post's voting system, David Basin already noted that "the verification neither considers low-level problems in the design and implementation of the cryptographic primitives nor the possibility that the adversary could break them, e.g., using quantum computers" (2021: 4). Likewise, Aleksander Essex pointed out the issue of quantum computing in up to two different reports. In his 2021 examination report, he suggested providing "a detailed description of which mathematical assumptions are broken by the existence of a sufficiently large quantum computer", having in mind both an ongoing electoral process and election historical data[22] (Essex, 2021: 22). In a later report, dated 2022, he kept on recommending to "[a]cknowledge and

[21] 1,8 M € en faveur des technologies quantiques, https://www.info.gouv.fr/actualite/18-m-eu-en-faveur-des-technologies-quantiques

[22] And even if he acknowledged that an implementation of Shor's algorithm reaching quantum supremacy, i.e., capable of, or comparable to computing discrete logarithms at jpj > 829-bits is highly unlikely in the next 10 years.

discuss the privacy and integrity implications if an at-scale implementation of Shor's algorithm becomes feasible" (Essex, 2022: 2). This recommendation came in spite of considering that a total redesign of the system with post-quantum cryptographic primitives is neither necessary nor feasible.

Interestingly, and also in contrast to the other three cases studied, there are not many country-wide initiatives to prepare for the quantum threat. In this regard, we found it curious that the estimates for the electoral risk assessment are not based on governmental studies or reports but on those made by private corporations, academia, or foreign standardization agencies. Looking at national strategies, for example, the National Cyberstrategy (NCS) does mention the challenge of quantum computing and the need for post-quantum algorithms but does not discuss these issues in much detail. As put forth in the strategy, these are "technological developments for which there is no immediate prospect of widespread application, but whose use could have a direct impact on cybersecurity" (Swiss Federal Council, 2023: 7). In view of recent experiments, the Swiss Federal Office for Defence Procurement also understand that also considers that "factoring 2048-bit numbers remains a distant goal"[23]. In this regard, the Swiss case is another exception to our findings.

2.3. Lattice-based cryptography: called into question? Risk and uncertainty as the underlying problems in ensuring long-term privacy in internet voting

In spite of lattice-based mathematical problems being the most common underlying constructions in post-quantum cryptographic standards, on 10 April 2024, Yilei Chen posted a preprint claiming to give a polynomial-time quantum algorithm to solve the decisional shortest vector problem (GapSVP[24]) and the shortest independent vector problem (SIVP[25]). Before that preprint, those problems were assumed to be extremely hard, and the best-known algorithm for solving them was exponential in n. If found true, Chen's algorithm (while not immediately breaking main lattice cryptosystems) would endanger all lattice-based cryptography, which is the best candidate for post-quantum public-key cryptography.

Due to the severity of the claim, the paper was undergoing peer reviews for more than a week until, on 18 April, Hongxun Wu and Thomas Vidick found (independently) a bug that invalidated the claim. In spite of Chen's claims, and as will be discussed in the next section, several interviews were conducted with cybersecurity and post-quantum cryptography experts during this period who expressed their concerns regarding the possible consequences if this preprint would withstand public scrutiny. Although it later turned out that the claim was not correct, it affected some participants' confidence in lattice-based cryptography, which could have resulted in a higher preference for hybrid schemes and the mention of alternative cryptographic approaches.

[23] Premières expériences d'informatique quantique réussies au Cyber Defence Campus, https://www.ar.admin.ch/fr/quantencomputing-experiences-cyber-defence-campus

[24] GapSVP ask to approximate the length of the shortest nonzero vector in a n-dimensional lattice within an approximation factor of ~n4.5.

[25] SIVP asks to find n linearly independent vectors in a n-dimensional lattice such that their length is within an approximation factor of ~n4.5 from the shortest nonzero vector.

Cases like this one evidence the difficulties of governing and regulating to mitigate uncertain risks: what impacts a technological development will have? When will it materialize, if ever? Which mitigation strategies will work against it? These questions are not easy to answer but are not unique to quantum computing and post-quantum cryptography. Technological innovations from Artificial Intelligence (AI) to neurotechnologies also raise ethical and legal challenges. In this regard, the Organization for Economic Cooperation and Development (OECD) has recently published a Framework for Anticipatory Governance of Emerging Technologies (2024). In this framework, they attempt to provide guidance on how to answer common questions about emerging technologies, such as: How to balance the risks and benefits of emerging technologies under conditions of political, technological, and economic uncertainty? How to adapt governance to converging technologies that cut across multiple regulatory categories? How to address the mismatch between the transboundary nature of technology and the jurisdictional boundaries of governance and regulation? How to engage a broader range of actors in the design of technology and governance to make emerging technology more inclusive, democratic, and effective? These questions seem pertinent when assessing the impact of quantum computing in internet voting and, more broadly, election technologies.

Whereas this paper does not attempt to conduct a detailed anticipatory governance assessment for quantum computing, this framework provides some interesting guidance on addressing some of the concerns these technological developments raise in the electoral field. More specifically, we rely on this framework to seek "consideration of potential concerns through open and inclusive processes to better align innovation and regulation trajectories with societal goals" (OECD, 2024: 11). To this end, the second part of the papers gathers views and insights from different stakeholders on developments in quantum computing, their perceived impact on internet voting, and the necessary strategies to mitigate them. More specifically, our analysis aims at showcasing the two following elements of the Framework:

- Guiding values: we aim at understanding whether a standard exists on the need for long-term privacy and, if so, how this is understood in different contexts.
- Stakeholder engagement: we gather insights from diverse actors in the qualitative analysis, spanning from the more traditional Electoral Management Bodies, including cybersecurity and standardization agencies, academia, and vendors, to name just a few examples. More importantly, these stakeholders should represent different national perspectives on the matter.
- Agile regulation: given the technological matter of the issue at stake and the fact that elections are a socio-political process, we aim to assess the dimensions of inter-agency cooperation and the development of forward-looking governance frameworks, especially those of a non-binding nature.

3. Exploring views and perceptions about quantum computing and long-term privacy in internet voting

To study what is the general feeling towards the challenges posed by the development of quantum computers and their possible future misuses, as well as to discern the causes for what we have labeled as "the electoral exception", we have conducted a series of semi-structured expert interviews

with different stakeholders. The aim of the interviews has been to verify our findings from the desk research, to identify if there are actual concerns about these potential risks or if the threat is still too theoretical, as well as whether we can find differences between different stakeholder groups (i.e., election administrators, cybersecurity agencies, academia, etc.). Additionally, we complemented the collected data by desk research to cross-check experts' opinions with other sources, some of them suggested by the interviewees.

In total, we conducted 18 interviews with 24 experts in electronic voting (6) from cybersecurity and standardization agencies (6), cybersecurity experts (4), post-quantum cryptography experts (2), election administrators (2) vendors (2), and international organizations (2)[26]. Most of the participants explained developments across countries, but interviews with some of them allowed for country-specific insights for our case studies, namely: Estonia (5), Switzerland (3), Canada (1), and France (1). The participants from vendors, international organizations, and post-quantum cryptography experts were selected from different countries while featuring only two participants per group. Similarly, we tried covering as many opinions as possible and interviewed electronic voting experts from five countries. Finally, we interviewed two different major cybersecurity and standardization agencies from two different countries as well. We created a pool of 36 questions based on our desk research, and we tailored each interview, selecting a subset of questions from this pool according to the interviewees' profiles and based on their answers to our initial questions. The list of questions and the mapping against each profile is provided in Appendix I.

This research has natural limitations concerning its design. It is hard to find an expert with in-depth knowledge about quantum computing-specifics and electronic voting contexts simultaneously. Notwithstanding, the interviews include a broad representation of electoral and cybersecurity stakeholders from different backgrounds and countries where internet voting is being used, allowing for including different insights into the research. We also acknowledge an uneven distribution among genders and geography (with a bias towards European and North American perspectives).

We also lack the ability to provide a granular analysis of our answers due to the conditions of the survey participation. All our interviews are supposed to be anonymous and not reveal participant identity. Unfortunately, our sample is limited since the profiles of the people we interviewed are specific and (with a few exceptions) require some degree of familiarity with the electronic voting field, which is a rather narrow area. Moreover, (in many cases) the interviewees' expertise is tightly linked to electronic voting in a particular country, which could easily deanonymize them if we are not careful with our generalizations. Hence, we frequently rely on expressions such as "most" or "few" when introducing the different ideas from the interviewees. It should not be understood as approximate measures of support or dissent, but rather as a way of introducing diverging views on specific matters.

However, we believe that our study is sufficient for identifying the differences and similarities in the perception of the quantum computer threat among different stakeholders, and that is why we study regions where internet voting has been used or discussed more extensively. In any case, we

[26] Some of the interviews were attended by more than one expert, hence resulting in 24 participants in total.

understand that the findings cannot be generalized globally, but we hope they could serve as a starting point to conduct additional research in this field. Given the novelty of the issue at stake, mapping the different views and showing and understanding the diversity of perspectives on how to deal with an uncertain risk, as well as where and when they overlap, is considered as a finding of utmost relevance at the intersection of digital technologies and electoral processes.

Out of the 36 questions in our pool, and for the sake of simplicity, we group the main findings of our interviews into five main categories: (1) perceptions about quantum computing as a threat; (2) the impact of quantum computing on internet voting; (3) transitioning towards post-quantum cryptography; (4) interagency cooperation; and (5) quantum computing and trust issues. We provide an overview of the answers received during the interviews for each category. Given the limitations of our sample, we also contrast the interviewees' views with a literature review on each of these topics, either challenging or supporting their main assumptions and conclusions. Lastly, for the longest sections, we provide a brief overview of the main takes on each of the findings.

3.1. Perceptions about quantum computing as a threat

All stakeholders interviewed are aware of the quantum threat and perceive it as a potential risk, mainly for public-key cryptography (less critical for symmetric cryptography). However, none considered themselves experts on quantum computers' state of the art. The vast majority of them do not consider quantum computing to be a hoax (only one expert said otherwise) but recognize that there are still some challenges that have to be solved before quantum computing becomes practical, such as the number of qubits or the temperature that certain quantum processors must be kept at. As one of the experts points out, this immaturity of quantum computers and the fact that we do not yet have a quantum computer capable of breaking today's cryptography generates more skepticism.

Experts disagree on the timeline when quantum computing will become a reality, thus challenging the foundations of public-key cryptography. Only a few experts felt comfortable providing specific timelines and, In turn, their forecasts spanned from 10 to 30 years. This is not unique to our sample. For example, the Global Risk Institute publishes a report (Mosca & Piani, 2023) each year that "aims at providing an educated perspective of how far away the quantum threat is, by collecting and examining the perspectives of global experts from academia and industry, involved in diverse facets of quantum computing." In the 2023 report, 37 leading experts on quantum computing (Jay Gambetta from IBM, Dave Bacon from Google Quantum AI, Peter Shor from MIT, etc.) were interviewed. A significant number of experts agree that, considering the goal of implementing a quantum computer with roughly 100 logical qubits in the next 15 years, the leading candidates are superconducting systems and trapped-ions. To the question, "Please indicate how likely you estimate it is that a quantum computer able to factorize a 2048-bit number in less than 24 hours will be built within the next five years, ten years, 15 years, 20 years, and 30 years.", just over half of the experts answered that within 20 years the likelihood is greater than 70% and in 30, greater than 95%.

However, despite this immaturity, almost all stakeholders agree that we should start to adapt our systems for the quantum era. When asked how well we are prepared to deal with quantum threats today, they are adamant that we are not. Experts are aware of all the work being done on standard-

ization, the implementation of software libraries for post-quantum cryptography, and some developments for specific protocols such as TLS, but recognize that we do not yet have the cryptographic agility to undertake a global migration[27]. So, what would be the necessary steps to prepare for such a transition?

Finally, it is worth noting that some stakeholders are also aware of the benefits that quantum computing can bring to chemistry, weather forecasting, artificial intelligence, healthcare, etc. These "quantum opportunities" will result from quantum computers' ability to perform calculations more efficiently.

3.2. Quantum computing, internet voting, and election technologies

Most interviewees agree that internet voting, and election technologies more broadly, would be at stake because of the potential of quantum computing to break conventional asymmetric cryptography (e.g., ElGammal, RSA, etc.). This would affect both internet voting systems and some of the non-voting protocols and applications on which internet voting relies, spanning from the TLS protocol to electronic electoral rolls, digital identification systems, etc. For the specific case of internet voting, the challenge lies mainly in long-term privacy, but integrity and eligibility could also be at stake. Therefore, some interviewees suggest that initial work could also be done to ensure these properties when quantum computers are available. Having said that, few interviewees perceive elections either as the main target of an attack by a potential quantum computer nor as the more adequate initial use case to implement quantum-resistant cryptography.

Notwithstanding, there is an important disagreement between the interviewees regarding the existence of a standard for long-term privacy in internet voting, the actual threat of quantum computing towards integrity and authenticity, as well as on (potential) mitigation measures.

3.2.1. Long-term privacy in internet voting

On the matter of long-term privacy as a standard for internet voting, not all the interviewees see it as an actual requirement. For example, some interviewees argued that the principle of secret suffrage is only expected to be observed during the electoral process or, more narrowly, during the voting and counting stages. They claim that this is the reason why most of the standards and mechanisms to ensure the secrecy of the vote deal with the physical and procedural guarantees at these two stages of an election: from the layout of the voting stations to the set-up of the voting booths, or the use of envelopes or folded ballots (or the double envelope method in postal voting).

Another expert, however, argues that this interpretation is inaccurate and stresses the problems of detailed regulations, which, in most cases, have been drafted with paper-based voting channels in mind. They suggest that it is important to understand the specific risks that internet voting faces

[27] See Google Chrome Adds Support for a Hybrid Post-Quantum Cryptographic Algorithm, https://www.thesslstore.com/blog/google-chrome-adds-support-for-a-hybrid-post-quantum-cryptographic-algorithm/

and develop measures that address them adequately[28]. This is particularly important because, as several interviewees point out, internet voting systems – and especially end-to-end verifiable ones – provide additional data about the conduct of an election, be it through a Public Bulletin Board (although, currently, it is only an academic proposal and none of the systems rely on it in practice) or by allowing auditors, representatives from political parties, etc. to inspect system logs and zero-knowledge proofs. Therefore, internet voting provides a unique setting in which long-term privacy becomes more relevant and needs to be balanced against some features that have no equivalent in paper-based voting channels.

To make things more complicated, among those interviewees who claim that secret suffrage should be preserved beyond the conduct of an e-election, the timelines they consider are clearly distinct. In their view, this period spans from two voting cycles (meaning around 8 years) to a voter's lifetime. In some discussions, it was even suggested that the secrecy of the vote should be observed after a voter's death in order to prevent their relatives from being blackmailed or threatened. What most experts do agree upon, however, is that periods for long-term privacy should be country-specific and take due account of the legal context as well as the political situation in the country (e.g., distinguishing between democratic and authoritarian countries, since knowing about someone's political choice could be a source of higher risks in the latter than in the former).

The issue of timelines is not unimportant since the timeline for preserving privacy is paramount in regard to the need to transition towards quantum-secure internet voting. For example – and recalling that there are no good estimates about the development of a quantum computing capable of breaking conventional cryptography –, if it is assumed that long-term privacy should be preserved for two election cycles, and quantum computers are only expected in a couple of decades, then the transition can be delayed for some years. However, if quantum computers are expected in half that time, the transition towards quantum-resistant internet voting should start now. There is no need to say that if long-term privacy should be preserved for the voter's lifetime, then internet voting should not be allowed until quantum-resistant internet voting systems are in place. The main issue with trying to identify a timeframe for long-term privacy is that this should be decided either by election administrators or lawmakers who, according to some interviewees, tend to be reluctant to provide specific timelines.

Interestingly, the risk of quantum computers being able to break asymmetric cryptography is not the only threat to long-term privacy. For example, in the case of Estonia, this issue was already raised when discussing the key length for the ElGammal encryption algorithm. In this case, the decision was made based on the recommendation of international standard-setting and cybersecurity agencies, as well as the advice of the cryptographic community, such as NIST, ENISA, or eCrypt. In our view, this case shows how election administrations usually defer to technology stakeholders' decisions that are intrinsically legal or political (more on this specific subject is discussed in section 3.4 below).

[28] This is also related to the need to interpret electoral regulations not by analogy to paper-based voting channels, but according to a teleological approach, i.e., by looking at the aims behind the electoral principles. In this regard, see for example previous work by Rodríguez-Pérez (2022a and 2022b).

3.2.2. Beyond long-term privacy in internet voting

Some experts also raised the issue of integrity and eligibility (also referred to as authenticity), as well as verifiability, being potentially at stake because of the development of quantum computing. In this regard, they noted that the digital signatures used to ascertain the integrity of the process or the digital identity of the voter and/or the election administration rely on digital signatures that depend on asymmetric cryptography. Likewise, in the case of verifiability, zero-knowledge proofs could be compromised, and therefore, universal verifiability would be at stake.

At the same time, the feasibility of such attacks is called into question by some experts. For example, some suggest that the short timeline in which online voting is usually offered would prevent an attacker from actually tampering with the signatures (either from voters and/or the election administration) by the time the voting period ends[29]. More importantly, and in contrast to the discussions about long-term privacy, no interviewee claims that there are any such requirements as long-term integrity and long-term verifiability. In fact, one interviewee even argued that they do not exist. Therefore, this problem does not need to be addressed at the moment (although one expert suggests that using distributed ledger technologies to avoid tampering with digital signatures could be studied.). Lastly, in some countries, there are even additional guarantees, like the use of a well-established digital identification system, which prevent the publication of the electoral roll and therefore mitigate any such risks.

3.2.3. Quantum computing, electoral processes, and retrospective decryption

While it is true that quantum computing will affect electronic voting, interviewees generally do not see elections as the primary target of an attacker with a quantum computer. The quantum threat is much wider than just elections, and areas like finance, healthcare, etc., would be more lucrative goals. Furthermore, most interviewees remarked that elections are a unique case, which only happens for a short period, rather infrequently, and do not require continuous availability as many other services. Moreover, voting relies on pre-existing infrastructure for managing voter rolls, etc., which should migrate before any changes to the voting software are done.

Hence, electronic voting is not the best use case for an early transition to post-quantum algorithms (as will be further discussed in the next section). Furthermore, some stakeholders argued that, if necessary, it would be possible to cancel the option to vote online and go fully paper-based, although there was some disagreement regarding this option between electoral administrations and experts (who did not reject this option) and ICT experts, who considered it difficult to organize any election solely on paper-based methods, given the widespread use of technology throughout the electoral cycle (in this regard, see also van der Staak and Wolf, 2019: 12). More importantly, an interviewee pointed out, past mistakes in terms of data breaches, etc. could not be corrected on time. Therefore,

[29] In practice, however, voting periods for internet voting can be quite long. For example, and whereas in Estonia and France the voting period is of around five days, in Canada is usually offered for 10 days, and in Switzerland for up to four weeks, depending on the canton.

as one expert pointed out, it is worth discussing whether it should also be adequate to future-proof past elections.

The idea of future-proofing past and current elections can be linked to the concern about retrospective decryption, meaning the possibility for a malicious actor to reveal in the future the contents of votes cast today (or in the past) once quantum computers become available. In contrast to this view, most experts rated the risk of retrospective decryption of ballots as unlikely. First, they noted that retrospective decryption is not necessarily a risk in post-quantum discussion only. Any data encrypted with vulnerable algorithms or short keys might become vulnerable much sooner than a quantum computer arrives. Second, data collection is a cumbersome task. If the bulletin board is not public (as is now the case in the countries analyzed), the vote collection requires significant effort to intercept all ballots during their transmission or privileged access to the system, which limits attackers. Third, the main danger of retrospective decryption would come not from recovering votes from the ballots but from linking them to specific voters. However, electronic voting usually operates with pseudonyms and keeps voter details separate. Thus, many experts believe the link between pseudonyms and actual voters is well protected, and retrospective ballot decryption alone would not breach voters' privacy. Notwithstanding, most experts remarked that it is a risk we must accept if we continue e-voting; the risk is low, but it is there.

3.2.4. Data deletion as a mitigation measure

Most interviewees agreed that data deletion is helpful as a defense in-depth mechanism. In this regard, they stress that this is a typical requirement in electoral legal frameworks, which in some cases prescribe very short deadlines for the deletion of the votes (e.g., one month, although there is disagreement on whether the votes should be kept for a longer period in case the election is challenged). They speculated that this makes it more difficult for a potential attacker to gather sensitive information without privileged access or real-time monitoring. However, experts noted that data deletion does not guarantee that all the data will be erased, as no one can determine how many unauthorized digital copies exist. As an interviewee pointed out, in the current context where internet voting tends to be hosted in cloud environments with a lot of redundancy and end-to-end verifiability is also provided (as we have discussed above), it can become nearly impossible to ascertain that all the election data has been actually deleted.

Some experts even highlighted that deleting data is more helpful in increasing trust in the system than as actual mitigation (trust issues will be discussed later in section 3.5). In some cases, it is not only the data and all its backups but also the shares of the election private key that are destroyed during a public event. Moreover, the desire to keep all data indefinitely might be viewed by voters as a trust violation. Therefore, according to these views, data deletion procedures boil down to procedural guarantees and the ability of (some) stakeholders to ascertain that the procedures are being followed thoroughly.

To sum up, to a certain extent, all technologies used in elections will be at stake with the development of quantum computing. After all, not only internet voting, but technologies used

throughout the electoral cycle require at least some form of digital signature that could be tampered with by a quantum computer. The signature serves as proof of the origin of the data (e.g., to show that the list of eligible voters is coming from the authorities and not a third party). Notwithstanding, these challenges should only be considered when the development of quantum computing is more mature. In the meantime, there is no need to adopt quantum-resistant specific measures (even to ensure long-term privacy, for which there is no generalized consensus on it being an actual requirement), but mitigation measures are encouraged (such as data deletion procedures, limited access to election data, and refraining from deploying a public bulletin board). At the same time, research on quantum-resistant internet voting systems should be considered. In spite of the opinion of some interviewees, it is highly unlikely that an electoral process can go full paper. As we will argue in the next section, a transition toward post-quantum cryptography would be the best approach if a quantum computer is discovered to exist.

3.3. Transitioning towards post-quantum cryptography

Most interviewees agree that transitioning toward post-quantum security is a desirable goal. However, they noted that it is not a priority for now, and doing research should suffice. Most interviewees refer to guidelines from standardization agencies, such as those from NIST. However, they admit that NIST does not cover all cryptographic needs of internet voting and cannot be viewed as the ultimate guide. Therefore, some interviewees suggest keeping an open mind and researching beyond NIST's primary candidates by exploring more options, such as quantum cryptography, anonymous voting channels, etc.

There is an important disagreement between the interviewees regarding the hybrid approach as a solution to post-quantum security. The divide is especially evident among vendors and standardization agencies, which appear to have opposing views. Finally, the expectations are that the post-quantum transition will take at least ten years. However, experts admit that the speed of the transition will greatly depend on the investments and efforts of the big corporations.

3.3.1. Alternatives for quantum-resistant Internet votign systems

Among the most often mentioned alternatives were post-quantum cryptography, building an e-voting scheme with everlasting privacy, hybrid models, and designing a voting scheme using symmetric primitives only.

For example, standardization agencies and post-quantum cryptography experts universally agreed that a hybrid approach is the best, as it allows for diversification of the risks. They emphasize that it leaves room for upgrading post-quantum primitives in case an error is found without risking the privacy of the whole system. This fear might stem from the relative novelty of the research into lattice-based cryptography and other post-quantum primitives.

Other experts argued that a hybrid would make sense for protocols like TLS, but electronic voting would not be an ideal candidate due to its complexity. According to them, primitives like zero-knowledge proofs and mix-nets cannot easily support hybrid encryption, and any attempt at that would complicate the system far beyond a reasonable level. Moreover, for vendors, the only feasible

option is post-quantum cryptography. They highlight that building a hybrid solution would be far too expensive to implement and audit. Similarly, they would prefer to keep the current designs intact as major restructuring is costly and error-prone.

However, several experts believe it is not hard to develop solutions that do not require asymmetric cryptography unless homomorphic properties are mandatory. Another avenue they see is voting systems with everlasting privacy, which have already been proposed in the literature (see Haines et al., 2023) but have not been used in practice. At the same time, they suggested avoiding blind signature schemes because they cannot offer any good post-quantum implementation so far. Nevertheless, they urge stakeholders to keep an open mind and investigate multiple alternatives before choosing a particular construction.

Regarding trust in cryptographic standards, everyone agrees they are sound in principle. In particular, the NIST standards were mentioned by most interviewees. However, some participants were cautious that the NIST standard mainly relies on lattices and would like to explore more options, such as quantum cryptography, anonymous voting channels, etc. Partially, it can be explained by the uncertainty surrounding the publication by Chen, which was under review when those interviews took place (see a discussion in 2.3 above). Regardless, even if some interviewees doubt or consider themselves not experts in mathematics, they trust the people behind this process and note that the selection process of the candidates was transparent.

Upon further questioning, we discovered that NIST is universally regarded as the de facto industry standard and one of the main references for post-quantum cryptography. One interviewee suggested that NIST has more power than a democratic government in the matter of post-quantum transition. Nevertheless, most experts note that standardized algorithms do not cover the main primitives necessary for internet voting. For example, the NIST standard explicitly avoids homomorphic properties required for verifiable mixing, homomorphic tally, zero-knowledge proofs, etc.

3.3.2. Transition or not to transition? That is not the question!

In spite of agreeing that a transition is necessary, most interviewees confess it is still too early to implement post-quantum cryptography. They believe we are not at all ready to switch to quantum-resistant alternatives promptly. Among the different reasons, interviewees list post-quantum cryptography as being too slow for practical applications, the lack or complexity of secure code implementations, difficulties in selecting security parameters, and relative immaturity of the lattice-based cryptography field. Notwithstanding, and in contrast to most experts, interviewed cybersecurity and certification agencies are confident that standards and guidelines will be available soon, and the transition is simply a question of following the guidelines and investing resources. Moreover, they emphasize the importance of exploring hybrid solutions.

Nevertheless, the transition is universally seen as desirable by our interviewees, although not a priority (as discussed above, elections do not seem the most adequate nor the most concerning implementation). Many interviewees emphasized that Internet voting should solve more pressing se-

curity problems first: implementing more systems with end-to-end verifiability, utilizing redundancy, increasing transparency, etc. Additionally, some experts note that simply increasing the key sizes can be enough at this stage.

Half of the interviewees raised concerns about the lack of infrastructure around elections required for the post-quantum cryptography transition. This is especially acute for certain national implementations of internet voting, which rely on country-wide, hardware-based, digital infrastructures. For example, all Estonian stakeholders argued that starting with the digital ID ecosystem would be best. Furthermore, all interviewees agree that the hardware is not ready. One of the bottlenecks is chips and hardware capable of doing fast post-quantum cryptography. Moreover, many embedded devices will be unable to migrate and will have to be replaced, slowing the transition.

3.3.3. How would a transition look like?

When asked about concrete transition steps or roadmap, all experts agreed that raising awareness and continuing the research should be the main strategy. The post-quantum experts interviewed agree that an important first step would be to take a proper cryptographic inventory and then identify which algorithms would need to be upgraded and migrated. Some mentioned already existing roadmaps and guidelines and urged to follow them (see, for example, ANSSI's roadmaps mentioned in section 2.2.3 above).

A common sentiment among them is that quantum computers will be available long before the public learns about them, and we will not have time to react promptly. However, there was no certainty on how long the transition is expected to take, however, the majority estimated it would take at least 10 to 15 years. Generally, participants speculated that the transition speed would depend on how much money we are willing to invest in it. Some interviews noted that if major corporations (especially the cloud ones) shift to post-quantum or hybrid, it would speed up the transition significantly. However, no one expects upgrading old embedded devices to take less than ten years. Past efforts with TLS 1.0, SHA1, and md5 migrations taught us that transition would be a long process and that some would never do it.

To sum up, there seems to be a disagreement regarding hybrid models. The divide is especially evident among vendors and standardization agencies, which appear to have opposing views. Part of the issue is that Internet voting often requires specialized cryptographic primitives with homomorphic properties (e.g., mix-net, zero-knowledge proofs, homomorphic encryption, etc.), which are not covered by standards. Nevertheless, most experts agree that post-quantum cryptography is the best alternative, especially lattice-based one. As for the transition, everyone thinks that research must either start or continue. However, most interviewees believe it is too early for practical transition, especially considering that standards and guidelines are not yet finalized. They view this transition as highly desirable, yet not a priority. Finally, the expectations are that the post-quantum transition will take 10 to 15 years and will greatly depend on the investments and efforts done by the big corporations. The commonly mentioned blockers were hardware unprepared for handling new

cryptographic operations quickly, embedded devices that cannot be upgraded, and chip-based identification mechanisms that must be re-issued. Overall, experts recommended starting the transition with an inventory of the used cryptography to identify which parts should be replaced first.

3.4. Interagency cooperation (or dependency on third parties?)

A key finding observed throughout the interviews conducted for this study with the different stakeholders is the growing collaboration between Election Management Bodies (EMB)and cybersecurity agencies. Given the nature of election administrations, which tend to be staffed with legal professionals (spanning from judges to public servants) or made up of representatives from political parties, this cooperation should not come as a surprise (in this regard, see, for example also Loeber, 2020). Therefore, when it comes to quantum computing and post-quantum cryptography, this cooperation is desirable because of the expertise and responsibilities of EMB on the one hand and because of the broad impacts of this threat on the other. As pointed out by several interviewees, these are scientific issues that expert communities should address. Similarly, one expert considers that election organizers should neither decide the crypto nor write the standards (neither into law nor administrative decisions). Instead, their role should be to focus on the requirements (e.g., secrecy, integrity, verifiability), explaining how difficult it should be to break them. Second, it will not only affect elections. Therefore, a country-wide answer by cybersecurity agencies may be more appropriate. In this regard, most interviewees consider EMB should follow.

At the same time, however, interagency cooperation may have two shortcomings. First, some interlocutors were concerned about it turning into dependency from EMB to cybersecurity experts (either agencies or vendors). Second, interagency cooperation tends to be more reactive than proactive, thus not being a silver bullet when it comes to anticipating and preparing for future risks and threats.

On the one hand, from our interviews, we have found that, at least in the case of understanding the threat posed by quantum computers as well as the potential alternatives to mitigate it, interagency cooperation turns into dependency from the election administrations towards cybersecurity expert bodies. Interestingly, some interviewees see this dependency as a trend rather than an exception. For example, one cybersecurity expert pointed out that one of the key issues is that EMB do not consider themselves owners of the e-enabled electoral process, which would explain their dependence on third parties (mainly cybersecurity agencies, but also vendors and academia). On the other side of the issue, one electoral expert also pointed out that cybersecurity agencies are normally eager to assume roles that traditionally have not pertained to them, and this further hampers the capacities of election management bodies to take ownership of these processes. As another expert argued, it seems that EMB tends to delegate as much as possible, whereas cybersecurity Agencies tend to take and retain control over these issues. In the long term, this trend leaves most of the key technological decisions in the hands of the latter when there are underlying policy and regulatory decisions that

should be made by the former. The above-mentioned discussion about key lengths in Estonia is a good example of this dependency[30].

Despite acknowledging this dependency, most interviewees also argue that these are not always the rule or exist to the same degree. Most experts argue that collaboration between election administrations and cybersecurity agencies depends on the country, the history, their degree of digitalization, etc. Therefore, most experts distinguished between countries and administrations that could be more prepared to deal with the quantum threat (due to their digital soundness and literacy, as well as because of their resources) against those where they already struggle to support the existing digital infrastructures (and in which discussions about future challenges such as quantum computing are unlikely to take place). In any case, however, interviewees agreed that not even the most prepared EMB would be ready to deal with the quantum threat at the moment. Either because of a lack of staff for this purpose, such as in-house research and cryptography teams, or funds to support independent researchers, all sorts of public administrations tend to become dependent on private parties. These span from academia to vendors, but in any case, this dependence is not ideal when it comes to foresight. Likewise, and as we have argued above, when cooperation with cybersecurity agencies takes place, it is more focused on addressing current challenges (reactive) rather than on preventing and mitigating potential risks in the future.

3.5. Quantum computing, understandability, and trust in election technology

Most of our findings on the previous issues seem to boil down to a matter of trust. Several examples have already been mentioned, spanning from the general assumption that conventional asymmetric cryptography cannot be currently broken to seeing lattices as the best alternative to mitigate the potential of quantum computing, as well as when it comes to the work of standardization agencies like NIST. In fact, some interviewees already stressed that the current use of cryptography, as well as the conduct of key steps in internet voting, is aimed at building trust rather than at ensuring the security of the process. For example, one interviewee mentioned that many of the cryptographic processes now being implemented may not be silver bullets in terms of risk mitigation, but they help to build trust with electoral stakeholders; the case of destroying data supports or election keys after an election is over is an example of this.

Therefore, the question arises: how can this trust be maintained when stakeholders so diverse and with different backgrounds should be involved in foreseeing the quantum threat and the transition towards post-quantum solutions? Most interviewees argued that continuous dialogue and advances in research were necessary, whereas others were concerned with the fact that electoral and technology stakeholders speak different languages may trump such exchanges. When asked about the potential of mis- and dis-information to erode this trust, few experts considered that quantum computing instrumentalized as disinformation can erode trust in internet voting. In fact, if anything, one interviewee argued that the media are exaggerating the threat of quantum computing.

[30] Another interesting aspect that was pointed out, and which merits further discussion, is how cybersecurity agencies turn on academia and, to a lesser extent, on vendors to make their decisions and advance their systems.

4. Conclusions

In spite of the absent steps being taken to make internet voting quantum-proof, there is no electoral exception when it comes to preparedness against quantum computing. Our research has shown that most stakeholders, including those from electoral administrations as well as those who are not, are well aware of the threat posed by developments in this field. Likewise, most interviewees argue that it is both too early to start a transition, and that elections are not the best first application of quantum-resistant cryptography. In fact, it is not only internet voting that could be compromised but any technology used throughout the electoral cycle.

To sum up, to a certain extent, all technologies used in elections will be at stake with the development of quantum computing. After all, not only internet voting, but technologies used throughout the electoral cycle require at least some form of digital signature that could be tampered with by a quantum computer. The signature serves as proof of the origin of the data (e.g., to show that the list of eligible voters is coming from the authorities and not a third party). Notwithstanding, these challenges should only be considered when the development of quantum computing is more mature. In the meantime, it seems that currently, there is no need to adopt specific measures to ensure quantum-readiness (even to ensure long-term privacy, for which there is no generalized consensus on it being an actual requirement), although mitigation measures are generally encouraged (such as data deletion procedures, limited access to election data, and refraining from deploying a public bulletin board). At the same time, research on quantum-resistant internet voting systems should be considered. In spite of the opinion of some interviewees, it is highly unlikely that an electoral process can go full paper. If a quantum computer is discovered to exist, transitioning toward post-quantum cryptography would be the best medium and long-term approach.

How should this transition take place? Most experts agree that post-quantum cryptography is the best alternative, especially lattice-based ones. However, most interviewees believe it is too early for practical transition, especially considering that standards and guidelines are not yet finalized. They view this transition as highly desirable, yet not a priority. Nevertheless, there seems to be a disagreement regarding hybrid models. The divide is especially evident among vendors and standardization agencies, which appear to have opposing views. Part of the issue is that internet voting often requires specialized cryptographic primitives with homomorphic properties (e.g., mix-net, zero-knowledge proofs, homomorphic encryption, etc.), which are not covered by standards.

Having said that, most interviewees agree that the post-quantum transition could take between 10 and 15 years and that this period will greatly depend on the investments and efforts of the big corporations. For this reason, and in line with many of the insights shared in this paper, we conclude that it is still time to take some preparatory steps, from research to inventories of cryptographic algorithms. The sooner these steps are taken, the better for the transition.

References

ANSSI. (2022). ANSSI views on the Post-Quantum Cryptography transition. In https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition

ANSSI. (2023). ANSSI views on the Post-Quantum Cryptography transition (2023 follow up). In https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography

Basin, David (2021) Review of Symbolic Proofs for Swiss Post's Voting System. https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Scope%201%20Final%20Report%20David%20Basin%2030.11.2021.pdf.download.pdf/Scope%201%20Final%20Report%20David%20Basin%2030.11.2021.pdf

Beullens, Ward et al. (2021) Post-quantum cryptography. Current state and quantum mitigation. European Union Agency for Cybersecurity (ENISA).

Canadian Centre for Cyber Security (2021) Preparing your organization for the quantum threat to cryptography - ITSAP.00.017. https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

Canadian Quantum-Readiness Working Group (2021) Canadian National Quantum-Readiness. Best Practices and Guidelines. https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf

Castryck, Wouter & Decru, Thomas (2023, May 15). An efficient key recovery attack on SIDH. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2022/975

Chen, L., Jordan, S. , Liu, Y. , Moody, D. , Peralta, R. , Perlner, R. and Smith-Tone, D. (2016), Report on Post-Quantum Cryptography, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8105

Essex, Aleksander (2021) Analysis of the Swiss Post e-Voting System. Audit Scope 1: ryptographic Protocol. https://www.bk.admin.ch/dam/bk/de/dokumente/pore/Scope%201%20Final%20Report%20Aleksander%20Essex%2029.11.2021.pdf.download.pdf/Scope%201%20Final%20Report%20Aleksander%20Essex%2029.11.2021.pdf

Essex, Aleksander (2022) 2022 Re-evaluation of the Swiss Post e-Voting System. Audit Scope 1: Cryptographic Protocol. https://www.bk.admin.ch/dam/bk/en/dokumente/pore/E_Voting/Examination_Reports_March2023/Scope%201%20Final%20Report%20Aleksander%20Essex%2030.09.2022.pdf.download.pdf/Scope%201%20Final%20Report%20Aleksander%20Essex%2030.09.2022.pdf

Estonian Information System Authority (2019) Annual Cyber Security Assessment 2019. https://www.ria.ee/media/1502/download

European Commission (2024, April 11), Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. Available at: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

Feynman, Richard P. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21, 467-488. https://doi.org/10.1007/BF02650179

German Federal Office for Information Security. (2020). Migration to post quantum cryptography. Recommendations for action by the BSI. In https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2

Hackett, Robert (2020). IBM plans a huge leap in superfast quantum computing by 2023. Fortune. Retrieved May 21, 2024, from https://fortune.com/2020/09/15/ibm-quantum-computer-1-million-qubits-by-2030/

Haines, Thomas, Mueller, Johannes, & Mosaheb, Rafieh & Pryvalov, Ivan (2023). Sok: Secure e-voting with everlasting privacy. Proceedings on Privacy Enhancing Technologies (PoPETs).

Loeber, Leontine (2020) Use of Technology in the Election Process: Who Governs? Election Law Journal: Rules, Politics, and Policy 2020 19:2, 149-161. https://doi.org/10.1089/elj.2019.0559

Moody, Dustin (2016, February 24-26), Post-Quantum Cryptography Standardization: Announcement and outline of NIST's Call for Submissions, PQCrypto 2016, Fukuoka, Japan. https://csrc.nist.gov/presentations/2016/announcement-and-outline-of-nist-s-call-for-submis

Moody, Dustin (2020, December 2). The Future Is Now: Spreading the Word About Post-Quantum Cryptography. NIST. Retrieved May 21, 2024, from https://www.nist.gov/blogs/taking-measure/future-now-spreading-word-about-post-quantum-cryptography

Mosca, Michele & Piani, Marco (2023). Quantum Threat Timeline Report 2023. In https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/. Global Risk Institute. Retrieved May 21, 2024, from https://globalriskinstitute.org/mp-files/quantum-threat-timeline-report-2023.pdf/

National Academies of Sciences, Engineering, and Medicine. 2019. Quantum Computing: Progress and Prospects. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196

NIST (2016, December 20), Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, 81 Federal Register 92787, 92787-92788. https://federalregister.gov/a/2016-30615

NIST. (2023a, August 24). FIPS 203 (Draft), Module-lattice-based key-encapsulation mechanism standard. CSRC. https://csrc.nist.gov/pubs/fips/203/ipd

NIST. (2023b, August 24). FIPS 204 (Draft), Module-lattice-based digital signature standard. CSRC. https://csrc.nist.gov/pubs/fips/204/ipd

NIST. (202c, August 24). FIPS 205 (Draft), Stateless Hash-Based Digital Signature Standard. CSRC. https://csrc.nist.gov/pubs/fips/205/ipd

OECD (2024), Framework for Anticipatory Governance of Emerging Technologies, OECD Science, Technology and Industry Policy Papers, OECD Publishing, Paris, https://doi.org/10.1787/0248ead5-en

Riley, Duncan (2022). Half of organizations worry about quantum 'harvest now, decrypt later' attacks. Silicon Angle. Retrieved May 21, 2024, from https://siliconangle.com/2022/09/20/half-organizations-concerned-quantum-harvest-now-decrypt-later-attacks/

Rodríguez-Pérez, Adrià (2022a) Secret texts and cipherballots: secret suffrage and remote electronic voting. PhD Dissertation in the framework of the Programme in Law, Universitat Rovira I Virgili (Tarragona, Spain). http://hdl.handle.net/10803/675606

Rodríguez-Pérez, Adrià (2022b) The Council of Europe's CM/Rec(2017)5 on e-voting and Secret Suffrage: Time for yet Another Update?. In: Krimmer, R., Volkamer, M., Duenas-Cid, D., Rønne, P., Germann, M. (eds) Electronic Voting. E-Vote-ID 2022. Lecture Notes in Computer Science, vol 13553. Springer, Cham. https://doi.org/10.1007/978-3-031-15911-4_6

Rodríguez-Pérez, Adrià, Costa, Núria, & Finogina, Tamara (forthcoming) Regulating for the "known unknowns" in internet voting: quantum computing and long-term privacy. E-Vote-ID 2023 Eight International Joint Conference on Electronic Voting 3 – 6 October 2023 · Luxembourg City, Luxembourg.

Shor, Peter Williston (1994). Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124-134.

Swiss National Cyber Security Centre (2023) National Cyberstrategy. https://www.ncsc.admin.ch/dam/ncsc/en/dokumente/strategie/cyberstrategie-ncs/Nationale-Cyberstrategie-NCS-2023-04-13-EN.pdf.download.pdf/Nationale-Cyberstrategie-NCS-2023-04-13-EN.pdf

Van der Staak, Sam & Wolf, Peter (2019) Cybersecurity in Elections. Models of interagency collaboration. https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

Wang, Brian (2020). PsiQuantum Targets Million Silicon Photonic Qubits by 2025. Next Big Future. Retrieved April 21, 2024, from https://www.nextbigfuture.com/2020/04/psiquantum-targets-million-silicon-photonic-qubits-by-2025.html

Wang, Brian (2021). Google Promises 'Useful, Error-Corrected' Quantum Computer By End Of Decade, Unveils New Quantum Campus. The Quantum Insider. Retrieved May 21, 2024, from https://thequantuminsider.com/2021/05/19/google-promises-useful-error-corrected-quantum-computer-by-end-of-decade-unveils-new-quantum-campus/

White House (2019), Exec. Order No. 13885, Vol. 84, No. 172. https://www.govinfo.gov/content/pkg/FR-2019-09-05/pdf/2019-19367.pdf

While House (2022), Exec. Order No. 14073, Vol. 87, No. 89. https://www.govinfo.gov/content/pkg/FR-2022-05-09/pdf/2022-10076.pdf

Young, Shalanda D. (2022, November 18). Memorandum for the heads of executive departments and agencies. Migrating to Post-Quantum Cryptography. Executive Office of the President. Office of Management and Budget. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

Appendix

Table 1: Questions asked during the interviews

	EMB and election experts	E-voting experts	Cryptographers	Cybersecurity and standardization agencies	Election technology vendors
Have you ever heard about quantum computers?	✓	✓	✓	✓	✓
If so: How familiar are you with quantum computing	✓	✓	✓	✓	✓

If so: How would you describe what is quantum computing in simple terms?	✓	✓	✓	✓	✓
If so: What will be the main danger of a quantum computer? What are your main concerns about quantum computers?	✓	✓	✓	✓	✓
If so: When do think quantum computers will be an actual threat?		✓	✓	✓	✓
If not: Explain what computing is and why is it a challenge (maybe mention a couple examples)		✓	✓	✓	✓
Is quantum computing a hoax?	✓	✓	✓	✓	✓
If not: What types of applications will quantum computing enable? Are there any upsides to the quantum computers?		✓	✓	✓	✓
If not, What impact will quantum computing have on the internet, banking, e-voting, etc.?		✓	✓	✓	✓
If not: What do we need to be doing now to future-proof our elections?		✓	✓	✓	✓
If not: Is quantum threat something e-voting should be concerned about now?		✓	✓	✓	✓

	EMB and election experts	E-voting experts	Cryptographers	Cybersecurity and standardization agencies	Election technology vendors
Is breaking vote secrecy after 10, 20, or 50 years dangerous? If so, why?	✓	✓			✓
Are you concerned that someone is collecting data now to decrypt it when a quantum computer will be capable of it?					
Which are the main challenges preventing quantum computing from being already a stable technology?			✓	✓	
How far are we from solving the scalability problem of quantum computers?			✓		
Will the changeover be gradual or abrupt? (Will discoveries in quantum computing be step-by-step or sudden)			✓		
Who is most likely will have the first quantum computer capable of breaking standard cryptography?			✓		

In addition to large tech companies (IBM, Google, AWS...) which other companies do you think are achieving promising results in the field of quantum computing?			✓		
Should there be regulations regarding quantum computer development?			✓		
How well are we prepared to deal with quantum computer threats now	✓	✓	✓	✓	✓
Are you aware of any initiatives to prepare for the quantum computer era? Do you know what your country is doing to prepare for this threat?	✓	✓	✓	✓	✓
Which do you think is the best approach to address the quantum threat?		✓	✓	✓	✓
What steps do you believe are necessary to mitigate the potential consequences of quantum computers?		✓	✓	✓	✓
Should we demand data to be deleted after X years?	✓	✓	✓	✓	✓
What would it take to demonstrate convincingly to most people that quantum computers are real enough to address practical real-world problems?	✓	✓	✓	✓	✓
What is your shot-term to-do list for preparing for quantum computer arrival?		✓	✓	✓	✓

	EMB and election experts	E-voting experts	Cryptographers	Cybersecurity and standardization agencies	Election technology vendors
What steps can an enterprise take today to prepare for quantum computing?		✓	✓	✓	✓
Do you think post-quantum cryptography is a feasible alternative? Is lattice-based cryptography the future?		✓	✓	✓	✓
How do we know we can trust the quantum-safe solutions that are available now?		✓	✓	✓	✓
Are you considering a transition towards post-quantum? If so, when?	✓	✓	✓	✓	✓
Are you considering hybrid cryptographic solutions as an alternative in the short- to medium-term?		✓	✓	✓	✓
What do you think of the new NIST algorithms and their security? If you have concerns, which alternatives do you think would be better?	✓	✓	✓	✓	✓

Do you think investment in post-quantum migration should start now or wait until quantum computers become fully practical?	✓	✓	✓	✓	✓
How long will the quantum-safe “transformation” take?		✓	✓	✓	✓
When do we need to complete the transition?		✓	✓	✓	✓
How would you “discover” which data and systems to migrate to new post-quantum algorithms first?	✓	✓	✓	✓	✓

About the Authors

Adrià Rodríguez-Pérez

Political scientist and jurist, with a PhD cum laude in Electoral Law and Information and Communication Technologies from Universitat Rovira i Virgili. His research focuses on the intersection of digital technologies, fundamental rights, and their (global) governance. He currently holds the position of Legal Advisor specialised in Electoral Law at the European Commission for Democracy through Law (Venice Commission) and is an External Associate Researcher at the Communication Networks & Social Change (CNSC) Research Group of the Universitat Oberta de Catalunya.

Núria Costa

Dr. Núria Costa received her Telecommunication Engineering Degree (2012) and her PhD cum laude in post-quantum cryptography (2021) from the Universitat Politècnica de Catalunya. She currently works at Universitat Pompeu Fabra as a postdoctoral research fellow in the project Artemisa, which aims to promote the creation and use of techniques and tools necessary to understand and face the challenges of digital security, as well as to promote the active participation of women and their empowerment in the field of cybersecurity.

Tamara Finogina

Cryptographer with a PhD cum laude in Applied Mathematics from Universitat Politècnica de Catalunya. Her research focuses on long-term privacy and verifiability. She has experience in both electronic voting and post-quantum cryptography. She currently works at Internxt, the open-source cloud storage provider.

