Regulating for the "known unknowns" in Internet voting: quantum computing and long-term privacy

Adrià Rodríguez-Pérez[1], Núria Costa[1], Tamara Finogina[1]

Abstract: Quantum computing is yet another example of the shift towards governance and policy-making amidst uncertain risks. We know it is coming and we anticipate that it will have a huge impact on today's electronic communications: the underlaying mathematical problems that allow us to securely send an email, shop online or transfer money are at stake. Voting online will no longer be secure either. In this paper we address a more fundamental concern: how the technological developments in quantum computing tomorrow may affect the fundamental rights of people voting online today. Internet voting is being progressively adopted in many electoral processes, including governmental ones. Countries like Canada, Estonia, France and Switzerland often use it. Their systems satisfy the legal requirements for democratic elections today, but they will no longer be secure once quantum computers are used to break the underlying mathematical problems behind public key cryptography. Our claim in this paper is that this is not only a problem for future regulations, but today's secret ballots are already vulnerable to quantum cryptanalysis in the future (i.e., retrospective decryption). Despite governments and electoral administrations being aware of this risk, no specific measures are yet being adopted to mitigate it, as our analysis of the electoral regulations in the above-mentioned countries shows. Interestingly, there is already a set of alternatives that could be studied. In this paper we analyze several proposals that aim at providing long-term privacy in Internet voting, including secure data deletion, quantum-resistant cryptosystems, and anonymous voting. Whereas none of these alternatives is a silver bullet against quantum cryptanalysis, it is essential that their feasibility is studied so that technological developments do not harm citizen's fundamental rights.

Keywords: Internet voting; quantum computing; long-term privacy.

1 Introduction

"Imagine a cat in a box. There are two possible states for the cat, namely dead or alive. [...] Traditionally we would say that the cat is either dead or alive, we just do not know which. However, quantum theory says that the cat is in a superposition of two states—it is both dead and alive, it satisfies all possibilities. Superposition occurs only when we lose sight of an object, and it is a way of describing an object during a period of ambiguity. When we eventually open the box, we can see whether the cat is alive or dead. The act of looking at the cat forces it to be in one particular state, and at that very moment the superposition disappears" [Si99]. The Schrödinger's Cat experiment is frequently used to illustrate how quantum mechanics work and, more concretely, to give an intuition of the paradox of quantum superposition. Quantum computers are becoming more and more

[1] Scytl Election Technologies, S.L.U., Barcelona 08021, Spain

doi:10.18420/e-vote-id2023_08

a reality and the potential impact they might have on society is clear: they could bring considerable benefits to many industries, such as finance or chemicals, but they also pose an inevitable threat to secure communications in which public-key cryptography plays a crucial role. The security of this type of cryptography is based on the hardness of solving certain computational problems, such as the discrete logarithm or the factorization. Unfortunately, none of these problems is hard to solve for a quantum computer, so any system using public-key algorithms is at risk. But is this a risk we must address now? Or, on the contrary, can we wait until large practical quantum computers are built? The answer is that it depends on what we are protecting. Internet voting systems provide voters with the chance to cast their votes from anywhere and require a high level of security to protect voters' secrecy and the integrity of final results. Asymmetric encryption, digital signatures and Zero-Knowledge proofs are some of the cryptographic primitives used by these systems in order to meet the security needs. Although all of these are considered robust nowadays, they won't survive the quantum age. Special attention should be given to encryption and the political and personal implications that revealing the contents of an encrypted vote could have in the future. Thus, when talking about privacy[2] in the long-term, it is clear that we should transition to quantum-safe alternatives; but do we know how? Is there any regulation which provides guidance on how to be protected against quantum computers? The goal of the paper is to address how to regulate future technological challenges to ensure that the principle of secret suffrage is respected in Internet voting both during an election and once it is over.

Risks and uncertainty are central problems in governance and regulation. Acknowledging that it is already considerably complex to provide solutions to existing problems, how should we respond to future risks and challenges? One option is to ban the exploitation of technologies whose consequences are unforeseeable. Nowadays, bans and moratoria are being claimed for facial-recognition technologies [Cr19], spyware [Un21] and, more recently, Artificial Intelligence [Vo23]. Nevertheless, it is also possible to think of restrictions in lieu of bans. Another approach is to protect the legal assets that these technologies could jeopardize. This is the approach that was adopted, for example, in 1979 with the Moon Agreement: although space technology was not widely available at the time, it was decided to preserve the moon as a common heritage of humankind [Ch80]. A similar and more general approach can be found in International Climate Change Law, the so-called precautionary principle. Based on this principle, regulation "does not require 'full scientific certainty' where there are 'threats to serious or irreversible damage', and its lower evidentiary threshold could strengthen the protective potential of international environmental law" [BBR17]. Nowadays, the neurorights movement [GHY22] is based on similar foundations. All in all, and rephrasing Ulrich Beck [Le95], we have moved from a risk society to a society of uncertain risks, where governance and policymaking need to be revisited to cope with

[2] Throughout the paper, we will adhere to the most common terminology of "long-term privacy" to refer to compliance with the principle of secret suffrage after the end of an election. However, "long-term secrecy", which encompasses both privacy –or confidentiality- and anonymity as standards under this principle, would be more accurate. For a more detailed discussion about the principle of secret suffrage in remote electronic voting see section 2.2 below.

potential futures.The goal of this paper is, therefore, to provide guidance on how to regulate e-enabled elections in the face of uncertainty.

The case of quantum computing and long-term privacy in Internet voting is, in this regard, a good instance to illustrate the problems associated to the regulation of technologies that evolve quickly and to future threats, considering their impact on fundamental rights. As Keith Martin has put it, “[w]e know [quantum computing is] coming. We know it will impact contemporary cryptographic algorithms (to quite varying extents). We don’t know the time frames. We don’t know how realistically the theory can be converted into practice” [Ma20]. To analyse this precise scenario, section 2 starts by providing an overview of what is known so far about quantum computing and the state of the art of its developments, as well as by mapping the impacts that quantum computing could have on Internet voting in the medium and long-term. To do so, we resort to specific examples of systems being in use for governmental elections in Canada, Estonia, France, and Switzerland. These countries have been using Internet voting for several years now and there is a substantial body of evidence available about their electoral frameworks, technical requirements, and on how their systems work. Based on this overview, we identify three potential challenges of quantum computing to Internet voting: on secret suffrage, on election integrity, and on transparency and verifiability. Out of these three, we conclude, the challenges to secret suffrage (i.e., long-term privacy in Internet voting) require immediate action.

In section 3 we diagnose how ready these countries’ electoral regulations are to cope with the challenge of quantum computing for long-term privacy. We identify that even when authorities are aware of the threat posed by quantum computers, no specific measures are envisaged to mitigate or eliminate this risk. These findings are surprising because a great deal of theorizing already exists about the risks of quantum computing for Internet voting and there are also several technical alternatives to, at least, mitigate them. More specifically, we study data deletion, quantum-resistant cryptography, and anonymous voting (including blind signatures, anonymous channels, and oblivious transfers) as potential responses. While none of these is perfect, and we conduct a detailed evaluation of their advantages and limitations, the feasibility of pre-emptively legally requiring them today should be studied. Overall, in this paper we provide an interdisciplinary approach towards quantum computing and Internet voting, addressing the legal and cryptographic implications of emerging technologies for fundamental rights. For this reason, we conclude in section 4 by recommending that law- and policy-makers start discussing which alternative(s) should be adopted in their electoral frameworks for Internet voting today.

2 Quantum computing: what do we know so far, and what are the challenges for Internet voting?

2.1 Quantum computing: the state-of-the-art

Quantum computing is evolving quickly. The first significant contribution to the development of quantum computing came in 1982, when Richard Feynman [Fe82] postulated that to simulate the evolution of quantum systems in an efficient way, 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 [Sh94] developed a polynomial time quantum algorithm allowing quantum computers to efficiently factorize large integers exponentially quicker than the best classical algorithm on traditional machines, turning a problem which is computationally intractable into one that can be solved in just a few hours by a large enough quantum computer. Then, two years later, Lov Grover [Gr96] presented the second major quantum computing algorithm, which demonstrated the capability of quantum computers to speed up database search. These two are probably the most famous quantum algorithms but there are other examples such as the Deutsch-Jozsa Algorithm [DJ92] and its extension, the Bernstein-Vazirani [BV97] algorithm, or the Simon's algorithm [Si97] which inspired the quantum algorithms based on the quantum Fourier transform. The Quantum Algorithm Zoo [Jo11] provides an up-to-date catalog of quantum algorithms. Although there has been a lot of work on quantum algorithms throughout the years, physical implementation has been slow: "[q]uantum computing is still at an early stage: researchers are building the first working prototypes, and others are arguing about whether these machines will ever be more than research curiosities" [HG22]. Large technology companies [Da22] such as Google, Microsoft, Amazon or IBM have been working for years with the objective of building a large-scale quantum device. In 2016, IBM was the first one putting a quantum processor on the cloud so anyone could run experiments (the IBM Quantum Experience [IBb]). Then, in the subsequent years the company developed Falcon, a 27-qubit quantum computer (2018) and the 65-qubit Hummingbird (2020). In 2021, IBM built the first quantum processor with more than 100 qubits, the 127 qubit Eagle. More recently, in 2022, the 433-qubit Osprey, which shows that the predictions Bob Sutor (vice president of IBM Quantum Strategy and Ecosystem) shared with TechRepublic in 2020 were accurate, "[. . .] the company [. . .] released its quantum hardware roadmap [IBa], calling for a 127-qubit system in 2021, a 433-qubit system in 2022, and a 1,121-qubit system in 2023 [Gr20]." Nevertheless, Mike Loukides (vice president of emerging tech content at IT learning firm O'Reilly Media) "[. . .] estimates that it would take 1,000 logical qubits [. . .] to accomplish any real work [Pu22]".

On the other hand, Google presented in 2019 a 53-qubit quantum computer, Sycamore [Ae19], and claimed quantum supremacy[3] for the first time, which generated a lot of debate in the community [IB19]. Microsoft, on its side, is offering Azure Quantum

[3] Quantum supremacy describes the ability of a quantum computer for solving a problem that the most powerful conventional computer cannot process in a practical amount of time.

[Mi23], a cloud quantum computing service which provides an environment to develop quantum algorithms which can be run in simulators of quantum computers. Apart from well-established technology companies, there are also some emerging players which are working hard on quantum computing. An example is D-Wave Systems, which has quantum computers of thousands of qubits, although "[t]he numbers cannot be compared with other kinds of quantum computers because the D-Wave qubits are not universal: they can only be used to solve a limited range of quantum problems" [HG22]. The company was also the first to sell a quantum computer to the world.

Given these developments, some consider that "[c]hange may come as early as 2030, as several companies predict they will launch usable quantum systems by that time [Bi21]". In 2016 the NIST estimated that quantum computers would be available in 20 years, that is: by 2036 [Ch16a]. According to the EU Agency for Cybersecurity (ENISA), however, some threat agents could already have quantum computers in the next five to 10 years [Be21]. Nevertheless, as ENISA states in their report: "not all development in the area is public and it is fairly likely that the first fully functional large quantum computer will not be publicly announced".

Although the biggest problems that quantum computers can currently solve are still easily manageable for conventional computers, several potential applications are already being explored for quantum computing, such as machine learning, Artificial Intelligence, chemistry, finance or cryptography.

When it comes to cryptography, quantum computers will have a significant impact. Everyday tasks such as sending an e-mail, making an online purchase or authenticating your identity are protected by cryptography and, mostly, by public key algorithms[4]. The hardness of these algorithms is based either on the difficulty of finding prime factors (in the case of RSA or ElGamal) or working out the discrete logarithm (i.e., elliptic curves or finite fields). Both are computational problems already solved by Shor's quantum algorithm.

2.2 Should Internet voting systems be ready?

But how could quantum computing have an impact on Internet voting systems? Being used in the context of public political elections, Internet voting must also comply with the standards for democratic elections as enshrined in the main international law instruments. These include universal, equal, secret, and free suffrage (see e.g., art. 21 of the Universal Declaration of Human Rights, art. 25 of the International Covenant on Civil and Political Rights or, at the regional level, art. 3 of the Convention for the Protection of Human Rights and Fundamental Freedoms).

[4] In contrast to public-key cryptography, the impact of quantum algorithms on symmetric cryptography will not be as severe. A quantum computer could speed up computations required for symmetric encryption, but the speedup is not as significant enough to break the encryption in a feasible time. Doubling the secret key size of symmetric algorithms would be enough to preserve security.

Nowadays, Internet voting complies with these standards by means of cryptography: the votes are encrypted end-to-end to ensure the secrecy of the vote and the freedom of the voter; before counting, votes are mixed or tallied using homomorphic encryption to prevent the contents of a vote from being linked to the voter who has cast them, thus ensuring vote anonymity; and encrypted votes are also digitally signed with keys that are unique to each voter to ensure that all votes stored in the digital ballot box and tallied have been cast by eligible voters. The most advanced systems also offer end-to-end verifiability, so voters can check that their encrypted vote contains their choices (cast-as-intended verifiability), and that it has reached the digital ballot box unmodified (recorded-as-cast verifiability). Furthermore, third parties can also as-certain that the tally genuinely represents all votes cast and stored in the ballot box (counted-as-recorded verifiability) and that ballot boxes have not been stuffed with additional ballots (voter eligibility).

However, we have already explained that quantum computing could break some cryptographic algorithms, thus jeopardising Internet voting. In fact, during an expert dialogue about Internet voting that took place in Switzerland in 2020, some experts already pointed out that "[q]uantum computers or advances in cryptanalysis may at some point subvert the soundness of today's standard building blocks" [Sw20]. In this section, we provide a detailed account of the specific risks that quantum computing poses to Internet voting. To do so, we look at the specific election standards by international organizations, like the Council of Europe, and assess specific systems as they are currently being implemented in governmental elections in Canada, Estonia, France, and Switzerland.

Secret suffrage and long-term privacy. When it comes to secret suffrage, most Internet voting systems use a combination of end-to-end asymmetric encryption with some form of anonymous tallying, such as mix-nets or homomorphic tallying. This helps ensure, on the one hand, the confidentiality aspect of secret suffrage and, on the other, the anonymity of the votes [Ro22a; Vi15]. Therefore, the risks of quantum computing, even if not feasible yet, are especially acute when it comes to secret suffrage. In this regard, any data that is published today is vulnerable against quantum attacks in the future. According to Ward Beullens et al., "[w]hat makes matters worse is that any encrypted communication intercepted today can be decrypted by the attacker as soon as he [sic] has access to a large quantum computer, whether in 5, 10 or 20 years from now" [Be21]. Such a threat – referred to as retrospective decryption – was also acknowledged by the e-voting experts at the Swiss dialogue [Sw20]. Therefore, in the Internet voting context, an adversary could learn how a person voted some years ago, which may have political as well as personal implications (e.g., in case of family coercion). Voting data can be intercepted either because it has been published in a bulletin board, accessed by auditors, or because it has somehow been eavesdropped or leaked by internal attackers. In what follows, we explain the specific risks of quantum computing for secret suffrage by looking at two of its standards: confidentiality and anonymity.

Risks to confidentiality based on the vulnerabilities of conventional asymmetric encryption algorithms. The majority of the systems used nowadays in governmental elections use some

form of asymmetric or public-key encryption to protect the voting choices. Estonia [Es23], Switzerland [Sw23b] or France [DH22] are examples of countries which are currently offering Internet voting to their population. Their systems use the ElGamal public-key cryptosystem for encrypting the votes, whose security is based on the hardness of solving the discrete logarithm problem. This cryptosystem, as well as RSA, will be vulnerable against quantum-computing attacks. Thus, it will be possible to decrypt votes in the long-term using quantum computers and without the need of having the private key. Nevertheless, this would not be necessarily a problem as long as these votes are not related to voters' identity.

Risks to anonymity. Managing to decrypt a vote cast 10 to 20 years ago may not seem so relevant, at the end of the day the results of that election would have already been published. The problem with decrypting votes cast using current Internet voting systems is that it will be possible for the attacker to know what each voter has voted. This is because, in order to ensure the eligibility of all votes cast and stored in the ballot box, or to prevent that more than one vote per voter is included in the election tally, Internet votes are usually encrypted and digitally signed before they are cast. In fact, this is how the systems used in Estonia [Es23], Switzerland [Sw23b], and most of the municipalities in Canada [El20; GPD10] work: the voters make their choices, the vote is encrypted, and the encrypted vote is then signed and cast into the voting server. Nowadays, digitally signing an encrypted vote does not breach anonymity, because votes are usually anonymised before they are tallied, or they are counted without being decrypted (a method that is called homomorphic tallying). Furthermore, multi-party computations or key-sharing mechanisms prevent a malicious actor from decrypting the votes before they are anonymised, since decryption requires the cooperation of different parties who each guard a share of the private decryption key. However, having access to the votes encrypted with conventional cryptography and digitally signed in the future, when quantum computers are available, would allow an attacker to decrypt them at any time, even without meeting the threshold of shares of the private decryption key.

Equal and free suffrage (I): eligibility and election integrity (digital signatures). Based on what we said above, are digital signatures used to demonstrate voter eligibility and satisfy election integrity at stake as well? Whereas quantum computers will also be able to tamper digital signatures based on conventional cryptography, this is not such a considerable risk if compared to those posed to confidentiality and anonymity. At the end of the day, voter eligibility is information that must at least be accessed by the election administration and by auditors (meaning that it is not completely private); whereas election integrity, once satisfied, cannot be tampered with in the future. In short: voter eligibility and election integrity are checked while the election is taking place, and it is highly unlikely that modern quantum computing is at the point where it can break currently deployed cryptographic systems.

However, it cannot be ignored that actual quantum computers may already exist, or that they could exist anytime soon. It means that quantum computing is no longer a long-term

risk, but a medium-to-short one. For example, in the framework of the above-mentioned Swiss expert dialog, one expert noted that "[i]t is unclear whether quantum computers will exist in the near future or if they already exist. Therefore, it is not possible to determine when a post-quantum cryptographic redesign is necessary" [Sw20]. If we take into account that most developments in cryptography have been kept secret [Le01; Si99], this risk cannot be downplayed.

Free suffrage (II): end-to-end verifiability (zero-knowledge proofs). Internet voting systems are end-to-end verifiable if they can provide evidence that every step of the election was completed correctly and accurately. This stands for allowing voters to individually verify their votes, and any third-party to check that election results accurately reflect the voters' intention. The latter is possible due to cryptographic mechanisms, such as homomorphic tally or verifiable mixing, which can be verified by either repetition or mathematical proofs. In this regard, the proofs demonstrate the correctness of a certain process without giving information that might compromise the process itself.

Notwithstanding, and just as for voter eligibility and election integrity, quantum computers are not yet a problem for end-to-end verifiability. As previously mentioned, cryptographic proofs are generated for auditing the tallying. These proofs are zero-knowledge, which is crucial for anonymity, but they also satisfy another property which directly affects verifiability: soundness. Soundness means that if a statement is false (e.g., votes that are going to be decrypted are not those sent by the voters), the proof cannot convince the verifiers of the contrary. Since proofs are usually verified during or right after the election, the situation is not as critical. Nevertheless, if for any reason they have to be verified when practical quantum computers are available, we will not be sure anymore that what they are proving is indeed true.

3 Long-term privacy in Internet voting: desirable or compulsory?

3.1 Long-term privacy in Internet voting: an overview of existing regulations

In order to dispel whether countries where Internet voting is available have mitigation measures in place against future breaches of the secrecy of the vote, in what follows we detail the existing regulations for elections and Internet voting, with special attention to secret suffrage and long-term privacy, in Canada, Estonia, France and Switzerland.

Canada. Internet voting in Canada is extensively used at the local level. A few municipalities in the province of Ontario started using this voting channel back in 2003, and others in Nova Scotia followed as soon as 2006 [GPD10]. The number of municipalities has increased steadily ever since [GPD10], and in the last October 2022 municipal elections in Ontario

217 municipalities offered online voting, in some cases as the only voting channel. More recently, higher level administrations have also started considering Internet voting. For example, Northwest Territories first offered Internet voting in the 2019 territorial general election [El20]. In spite of this considerable uptake, the legal framework for Internet voting is not really detailed regarding the requirements that this technology should meet. For example, municipalities in Ontario base the lawfulness of Internet voting on section 42 of the Municipal Elections Act, which authorises them to "pass by-laws authorizing the use of an alternative voting method, such as voting by mail or by telephone, that does not require electors to attend at a voting place in order to vote" [CAE19]. Notwithstanding, this section does not detail any specific requirements that these remote voting methods should meet.

In an attempt to address this lack of legal standards, and following expert claims that additional regulations are needed [EG20; SD13], there is an on-going attempt by the Digital Governance Standards Institute (formerly known as CIO Strategy Council, CIOSC) to develop a "series of standards aim[ed] to specify minimum technical requirements for online electoral voting in Canada at the municipal, provincial and federal level" [CI20]. A technical committee on online electoral voting (Technical Committee 11) was set up in 2020[5]. At the time of writing, the technical committee is working on a third draft version of the standards. References to quantum-resistant cryptography were added to the second draft [CI22]. The current draft now mentions quantum-resistant cryptography twice: in section 4.1.1.4, "[a]ll data shall be encrypted with quantum-resistant encryption both in transit and at rest" [Di22]; and in section 8.1.1.2, "[t]he voting service shall ensure that the secrecy of the vote is guaranteed using quantum-resistant encryption during the casting, transfer, reception, collection, and tabulation of votes" [Di22]. However, the very same draft already comes with a warning that "[s]tandards have not yet been finalized for quantum-resistant encryption" [Di22]. Anyhow, these are voluntary standards that election administrators using Internet voting could decide whether to follow or not, which fall short of enshrining a requirement for long-term privacy and prescribing mitigation measures.

Estonia. Estonia remains to date the first and only European experience where online voting is offered to all the population, for all contests: national, local, and to the European parliament. Elections are regulated in three different acts: parliamentary elections are primarily regulated by the *Riigikogu* Election Act, while election for local government units are regulated by the Municipal Council Election Act and elections to the European Parliament by the European Parliament Election Act. Notwithstanding, the latter Acts refer to the *Riigikogu* Election Act on those aspects related to Internet voting. Likewise, the Referendum Act deals with referendums, which according to the provisions in Chapter 7 shall also provide the option to vote electronically. In addition to electoral regulations, "the Estonian e-government ecosystem is strongly regulated by legal instruments that provide a framework for security and protection of the personal data" [SV16]. This framework includes,

[5] All the details about this process can be found at: <https://dgc-cgn.org/standards/find-a-standard/standards-in-online-electoral-voting-2/can-ciosc-111-x202x-online-electoral-voting/> [last accessed 30 August 2023]

among others, Estonia's Personal Data Protection Act (1996), the Public Information Act (2000), the Population Register Act (2000), the Digital Signatures Act (2000), and the Electronic Communications Act (2004) [SV16].

The technical aspects of Internet voting are detailed in lower-level regulations. In these regulations, the risk of retrospective decryption is identified. In this regard, the General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia acknowledges that "a theoretical risk remains that someone is able to copy personalized i-votes from the system and attempts to guess the private key over time, by using remarkable computer resources over a long period of time" [EN23]. To mitigate this risk, the Framework advises taking account of this risk when "choosing the crypto algorithm for encryption of votes and the length of the key" as well as "rely[ing] on up-to-date studies on the security of crypto algorithms" [EN23]. The Framework has been recently updated, ahead of the *Riigikogu* elections of March 2023. Notwithstanding, almost identical provisions can be found in the previous version [El16]. Furthermore, the National Electoral Committee's Decision on the technical requirements to ensure the general principles of electronic voting also prescribes that unanonymous logs, electronic votes, personal data of voters included in the electronic voting system and the key for opening electronic votes are destroyed by the state election service together within the legally established deadlines [Na21]. The private key used for decryption must also be destroyed shortly after the election, thus rendering the non-anonymous and encrypted votes unusable, as is also required by the General Framework [EN23].

France. France can also be considered an Internet voting pioneer, even if the option to vote online is limited to French voters abroad. The French legal framework for Internet voting has remained more or less the same since a Constitutional amendment in 2008 introduced 11 members of the National Assembly to be elected by French voters abroad. Subsequently, the law num. 2013-659 of 22 July 2013 on the representation of French citizens abroad, set up a new institution representing the interests for French citizens abroad (the Consular Councils, for whose election voters could vote online) and amended the Electoral Code. As in the case of Estonia, there is a considerable amount of secondary regulation which completes the legal framework for Internet voting. Amongst them, specific requirements are to be found in the recommendations of the national data protection agency, the Commission Nationale de l'Informatique et des Libertés (CNIL). The CNIL first adopted a Recommendation on the security of e-voting systems in 2003 and then updated it in 2010 [CN10a]. The Recommendation provides general guidelines regarding minimal privacy, secrecy, and security requirements for Internet voting, including physical (e.g., access controls to the servers or rules for the clearance of authorized employees) and software measures (such as firewalls).

The CNIL has further updated their Recommendation in 2019 to take stock of the new requirements introduced by the European Union's General Data Protection Regulation (GDPR) after it entered into force [CN10b]. The goal of the update was to apply to future

developments in Internet voting, with a view to better respect the principles of personal data protection, and to inform data controllers on their choice for an online voting system [CN19]. In its new Recommendation, no specific references are made to the threat posed by retrospective decryption. Notwithstanding, the CNIL does prescribe the secure destruction of the data as soon as the deadline for complaints and appeals have been exhausted: "[a]ll support files (copies of the source and executable codes of the programs and of the underlying system, voting materials, tally files, results files, backups) must be kept under seal until the exhaustion of the channels and deadlines for appeal" [CN19]. The erasure of the data must be conducted, according to the CNIL, under the supervision of the electoral commission. Notwithstanding, the same measures were already prescribed in equivalent terms in 2010 [CN10a], which makes it unlikely that it is the result of specific awareness about the threat posed by quantum computers.

Switzerland. Even if the first tests with Internet voting in Switzerland took place back in 2003 [Sw04], the Swiss legal framework for Internet voting has recently undergone a major overhaul. Following the decision by the two main Internet voting providers not to continue offering their systems back in 2019 [Sw19], the legal framework has been updated, including with the already mentioned dialogue with expert communities and the amendment of two federal ordinances: the Federal Council's Ordinance on Political Rights and the Federal Chancellery's Ordinance on Electronic Voting [Sw22b]. Surprisingly, and in spite of the expert voices raising the issue of quantum computing during the dialogue, the updated regulations have not included specific requirements for long-term privacy. The need to protect secret suffrage in the long-term is therefore not specifically required in the new ordinances. Notwithstanding, the federal authorities seem to be aware of the concern, which has been identified in a recent risk assessment by the Swiss Federal Chancellery [Sw23a]. Interestingly, the risk is considered with a high impact score (with 35 points in a scale from 0 to 49), but of low probability [Sw23a] . According to the national authorities, in the absence of standardized post-quantum algorithms, it is still possible to prevent and mitigate the impact resulting from the evolution of quantum computing by increasing the key size of current encryption mechanisms [Sw23a]. In this case, it is considered that a key size of 3072 bits is enough.

At the same time, it is important to stress existing references to data deletion in the federal documents. For example, in their guide for risk assessment of *La Poste Suisse*'s Internet voting system, the Swiss Federal Chancellery now identifies four key post-election processes: file deletion; the destruction or secure deletion/formatting of the data supports; the destruction of the passwords; and the destruction of the smartcards [Sw22a]. However, none of these measures has been expressly linked to the actual threat posed by quantum computing. In fact, similar requirements can be found in previous regulations [Sw14; Sw18]. Therefore, these requirements could instead arouse from data protection regulations. Notwithstanding, identified monitoring measures associated to quantum computing do indeed include closer cooperation with the scientific community and the development of the

system and its documentation [Sw23a]. All in all, this approach can be summarized, using the very same words of the Swiss Federal Chancellery, as the fact that "no one can predict the future" [Sw23a].

3.2 Technical alternatives (their advantages and limitations)

Having now identified the specific risks posed by quantum computing to Internet voting systems and the existing *lacunae* in national electoral frameworks, it is now necessary to address which specific mechanisms could at least mitigate these risks. Since the main challenge is on preserving long-term privacy, this section will focus on technical alternatives to current implementations, so this standard is ensured.

The first technical alternative which comes to our minds is to leverage quantum computing/cryptography to protect long-term privacy in Internet voting systems, instead of just jeopardising them. The best-known example of a quantum algorithm is the Quantum Key Distribution (QKD) that allows two parties to exchange a secret using a special quantum channel and guarantees that an eavesdropper of the communication would be detected, and the process aborted [Wo21]. This is because it is not possible to measure the quantum state of the system without disturbing it. Nevertheless, we cannot rely only on the QKD for building a long-term private voting system compliant with electoral regulations. Even if all voters can securely transmit their choice directly to the electoral authority without the risk of being eavesdropped on, we would still have an issue with secret suffrage. The receiving entity (electoral authority) would know the individual choices of all voters and the intermediate tally at all moments. Hence, we would need to trust that entity for secrecy and tally fairness. Otherwise, we will need a voting solution similar to the existing ones but based on quantum cryptography. However, quantum cryptography needs special requirements such as its own infrastructure (which is not there yet) and does not cover all the needs of secure-communications and secure Internet voting systems (e.g., digital signatures, public-key encryption, zero-knowledge proofs, etc.). For this reason, we need to find other technical alternatives which allow for quantum-resistant Internet voting systems but without relying on quantum physics. Data deletion, quantum-resistant cryptography, and anonymous voting are some of the possible alternatives.

Data deletion. As we have seen above, requirements for data deletion following the end of an election are common. We have already identified these requirements in Estonia [Na21], France [CN19], and Switzerland [Sw22a]. Additionally, similar provisions can be found in the technical standards currently being developed in Canada [Di22].

Even if these measures seem to be related to data protection regulations rather than to the aim of protecting long-term privacy, they could seem at first sight an adequate mitigation mechanism. After all, if all election data is deleted once the election is over and after all the complaints and appeals deadlines have been exhausted, it will be no longer possible

to decrypt it in the future. Despite secure processes for data deletion already existing and being standardized, the problem with this alternative is that there are no guarantees that indeed all election data has been securely deleted. This risk cannot be downplayed if we consider that votes in Internet voting are cast from unsupervised environments and devices that fall outside the scope of the election administration, and through an insecure channel such as Internet voting. That means that potential attackers have a considerable surface to eavesdrop (un)encrypted votes before they reach the voting server, which they could keep despite the secure data deletion procedures. Likewise, an internal attacker from an election administration could easily generate a copy of all encrypted election data and prevent this copy from being deleted at the end of the election by safeguarding it outside the official election's voting infrastructure.

Therefore, this approach has important flaws. The main problems associated to this approach is that they are based on an analogy to paper-based voting channels, such as postal voting or voting in polling stations, that fails at apprehending the specific stakes in Internet voting (on the shortcomings of regulation by analogy see [Ro22a; Ro22b]). While deleting digital data is possible, it is virtually impossible to control the number of copies because copying digital data is far easier than doing so for hard, paper-based ballots, and does not require special tools. Quantum computing is a novel threat and, therefore, regulating by analogy does not work: no similar problems exist in paper-based voting channels, since physical voting supports (i.e., paper votes), cannot be as easily eavesdropped and/or copied as electronic ones.

Quantum-resistant cryptography. Another alternative, based on the draft standards currently being developed in Canada, is the use of quantum-resistant cryptography. Quantum-resistant or post-quantum cryptography are based on mathematical problems that quantum computers may not be able to solve easily. Some examples include lattice-based cryptography, supersingular elliptic curves, or codes [Ch16a]. Indeed, of all of these, lattice-based cryptography is the cryptosystem that has received more attention. Good evidence is the list of post-quantum candidates to be standardized by the NIST as a result of the process initiated in 2017. A clear majority (three cryptosystems out of the selected four) are based on hard problems over lattices.

When it comes to Internet voting, a first construction of a post-quantum Internet voting system was given in 2016 [Ch16b]. This system is inspired by Helios [Ad08] and is based on Learning With Errors (LWE) fully homomorphic encryption [DM15], unforgeable lattice-based signature and trapdoors for lattices. The authors do not propose any parameters neither an implementation of the system. One year later, the EVOLVE (Electronic Voting from Lattices with Verification) system was presented [Pi17], which is based on the voting protocol described in [Cr96]. Compared to the previous construction, EVOLVE makes use of zero-knowledge proofs and voters commit to their preferred voting options instead of encrypting them. Another proposal which uses fully homomorphic encryption is that presented in [AQA18]. The main contribution of these authors is the implementation of

an electronic voting system using the homomorphic encryption scheme (the BGV scheme [BGV12]) included in HElib, Homomorphic Encryption library). In [Rø20], the authors also make use of fully homomorphic encryption and propose to replace the classical proofs suggested in the coercion-resistant JCJ protocol [JCJ05] by quantum-resistant designated verifier proofs [STW14], thus making the protocol quantum-resistant. Another proposal from the same year [Gu20] designs an electronic voting scheme which supports ballots for multiple candidates. Each candidate is represented by a 0 or 1, the IBFHE scheme (Identity-Based Fully Homomorphic Encryption) is used for encryption and the ECDSA algorithm for signatures.

The last proposals we have found in the literature focus on verifiable mix-nets and build a post-quantum e-voting system using them as the main building block. The first proof of a shuffle based on lattices is presented in [CMM17] and is later significantly improved in [CMM20]. Also, based on this post-quantum proof of a shuffle, the authors construct a post-quantum Internet voting system which, in addition to providing long-term privacy, also meets the requirements of coercion-resistance and individual verifiability [Co21]. Similarly, in [Ar21] there are the following contributions: the first efficient verifiable shuffle of known values, the first post-quantum construction of a practical voting system that is suitable for more general ballots and that supports return codes and, finally, a concrete choice of parameters for the system and its implementation. The architecture of the voting protocol is very similar to previous voting systems such as the Norwegian internet voting protocol [Gj12]. Although the system does not provide universal verifiability, it provides privacy, cast-as-intended, and coercion-resistance by allowing re-voting and integrity if at least one auditor is honest. An extended version of the shuffle presented in the previous paper is given in [Ar22], as well as a compatible verifiable distributed decryption protocol. In addition, the authors give concrete parameters for their system, estimate the size of each component and provide an implementation of all sub-protocols, but not of the full system. They employ NFlib library for the polynomial arithmetic, the FLINT library for arithmetic routines not supported in NFlib, and for gaussian sampling they adapted COSAC.

Therefore, lattice-based cryptography seems to be a good alternative for the replacement of current asymmetric encryption algorithms such as RSA or discrete logarithm on prime fields or elliptic curves. It offers strong security guarantees and many cryptographic primitives which can be implemented using conventional computers. However, this is precisely one of the problems with these algorithms: they "need to be capable of running on conventional computers" [Ma20], and they may not be as efficient as the existing standards. For example, the proposal in [Co21] has been recently implemented in [FWK21]. The efficiency of their findings makes the actual implementation of this system not feasible for actual politically binding elections.

More important, the robustness of quantum-resistant crypto is theoretical, and "[a] new quantum algorithm may be discovered which breaks some of these schemes" [Ch16a]. A good example of this is the SIKE cryptographic algorithm, which was a NIST Post-Quantum Cryptography candidate that was cracked by experts using a conventional machine [CD23].

Moreover, when it comes to Internet voting, some of the key cryptographic building blocks (such as asymmetric encryption or key-sharing mechanisms) have not yet been standardized.

Anonymous voting. Most of the protocols presented above make use of traditional ways to build Internet voting protocols such as homomorphic primitives or mix-nets. Nevertheless, when trying to ensure voter's anonymity there is another well-known technique which consists of using blind signatures. This technique anonymizes the encrypted votes when they are cast, so theoretically the link between the encrypted vote and the voter who cast it is broken from the very beginning. In [Ka21] the authors propose a construction, based on the framework of Fujioka et al. [FOO92], which uses a blind signature scheme and a commitment scheme as the main building blocks. The first one allows for the preservation of the anonymity of each voter, while it forbids voters from voting twice. The second one prevents any partial result from being leaked before the end of the election. As the authors explicitly mention in their publication, this is the first online voting scheme that simultaneously provides post-quantum public verifiability and everlasting privacy (information-theoretic ballot anonymity).

Nevertheless, blind signatures or anonymous credentials are not enough to provide long-term privacy. Even though votes are not related to signatures, they are connected via other voter-identifiable information such as their IP address, cookies, etc. Even if we could entirely remove or hide all metadata, the nature of the election usually implies that voter registration (obtaining anonymous credentials) and vote-casting (using anonymous credentials) happens within a short time window. Therefore, it would be easy to link voters with their votes if they cast them at odd hours. Increasing the time between registration and voting would only result in problems with intermediate credentials safe-keeping and would prolong the opportunity for credential theft and coercion.

The alternative of casting votes via anonymous channels, as Univote voting system does, is also hardly a long-term private solution [Re13]. For example, The Onion Router (Tor) network provides anonymity (or rather pseudonymity) to millions of users accessing the internet daily. Communication over Tor is usually done via several relay nodes, which forward the traffic from the client's machine to the internet server and back. Yet, Tor is not perfectly anonymous. Many issues can result in personal data leakage ranging from misconfiguration and user mistakes to sophisticated attacks. It does not mean every user will be deanonymized every time, but a possibility remains. Unfortunately, even if we construct a perfectly anonymous Tor-like system, it would not be sufficient for long-term privacy. Imagine that the client entry point to the network - the guard relay in Tor's terms - is malicious. Such a relay knows when the voter connects and observes which ballot is posted soon after that (traveling through the network does not take long), which allows the linking of voters and votes. Also, the first node can always keep a copy of all data and wait until encryption becomes vulnerable. Finally, legal issues surrounding anonymous channels in general, and in Tor specifically, remain relatively unexplored. For example, some electoral legislation allows voters to use an alternative voting channel in case of a problem,

or the voter credentials are reissued, and the previously cast vote is canceled. However, with anonymous voting, it would be impossible to ensure a öne voter, one voteßtandard in case the voter has technical issues during voting.

The oblivious transfer could, in theory, allow the voter to get some information from a set of values that the election authority has without revealing requested elements. For example, in the BVOT voting system, voters can get encoding for the selected options from the list of all possible voting choices. However, if the protocol is not post-quantum secure, anyone observing the interaction can later break it and identify the requested values. Hence, the oblivious transfer would not work for long-term privacy protection.

4 Conclusions and recommendations

This paper has shown how developments in quantum computing are yet another example of the shift towards governance and policy-making amidst uncertain risks, and how this will impact Internet voting. We know it is coming and we anticipate that it will have a huge impact on today's electronic communications. More important, voting online will no longer be secure either. In this paper we have addressed a more fundamental concern: how the technological developments in quantum computing tomorrow may affect the fundamental rights of people voting online today. In spite of Internet voting systems used in governmental elections today satisfying the legal requirements for democratic elections, these will no longer be secure once quantum computers are used to break public key cryptography – and this may compromise voters' secrecy in the long term. Therefore, we have demonstrated that quantum computing is not only an issue that should be considered in future regulations for Internet voting, but that should be already addressed today. Whereas the impact of quantum computing on election integrity, voter eligibility and end-to-end verifiability is not an issue yet, today's secret ballots are already vulnerable. Our analysis of four governmental experiences (Canada, France, Estonia and Switzerland) shows that governments and electoral administrations are aware of this risk, but no sufficient measures are yet being adopted to mitigate it. Making this matter worse, the importance of long-term privacy in Internet voting has not sufficiently been considered and the principles for democratic elections have not been revisited in light of future challenges: it is important to rethink the principle of secret suffrage and enshrine a standard of long-term privacy in Internet voting.

Interestingly, there is also a set of alternatives that could already be studied to protect long-term privacy. In this paper, we have analysed several proposals, including secure data deletion, quantum-resistant cryptosystems, and anonymous voting. Amongst them, quantum-resistant or post-quantum cryptography seems the most suitable, even if its actual implementation still requires some effort. Therefore, and whereas none of these alternatives is a silver bullet against quantum computing, it is essential that their feasibility is studied so technological developments do not harm citizens' fundamental rights. Likewise, and even if none of the analysed experiences is satisfactory from the perspective of electoral standards and requirements, the Swiss example is the most promising. Authorities in

Switzerland conduct risk assessments ahead of each election, and they are already aware that technological developments in quantum computing may compromise long-term privacy. The conclusion they reach, however, is in our opinion unsatisfactory: increasing encryption keys' size and deleting data is not enough to guarantee long-term privacy. Destroying paper ballots may be enough to ensure that nobody links a voter to the voter who has cast it in the future, but when votes are cast electronically, they can easily be eavesdropped or copied, and copies could remain even when the main electoral infrastructure is destroyed.

The possibility of quantum-based retrospective decryption means that in the future it will be possible to know for whom each person has voted. Following its previous experiences in engaging experts in a wider dialogue on Internet voting, Switzerland – and any country using Internet voting – should already start involving them in making Internet voting quantum-proof as well. Otherwise, our rights are at stake.

References

[Ad08] Adida, B.: Helios: Web-Based Open-Audit Voting. In: Proceedings of the 17th Conference on Security Symposium. SS'08, USENIX Association, San Jose, CA, pp. 335–348, 2008.

[Ae19] Arute, F.; et al.: Quantum supremacy using a programmable superconducting processor. Nature 574/, pp. 505–510, 2019.

[AQA18] Aziz, A.; Qunoo, H.; Abusamra, A.: Using Homomorphic Cryptographic Solutions on E-voting Systems. International Journal of Computer Network and Information Security 10/, pp. 44–59, Jan. 2018.

[Ar21] Aranha, D. F.; Baum, C.; Gjøsteen, K.; Silde, T.; Tunge, T.: Lattice-Based Proof of Shuffle and Applications to Electronic Voting. In: Topics in Cryptology – CT-RSA 2021. Vol. 12704, Springer International Publishing, Cham, pp. 227–251, 2021.

[Ar22] Aranha, D. F.; Baum, C.; Gjøsteen, K.; Silde, T.: Verifiable Mix-Nets and Distributed Decryption for Voting from Lattice-Based Assumptions, Cryptology ePrint Archive, Paper 2022/422, 2022, URL: https://eprint.iacr.org/2022/422.

[BBR17] Bodansky, D.; Brunnée, J.; Rajamani, L.: International Climate Change Law. Oxford University Press, 2017.

[Be21] Beullens, W.; D'Anvers, J.; Hüsling, A.; Lange, T.; Panny, L.; de Saint Guilhem, C.; Smart, N.: Post-Quantum Cryptography: Current state and quantum mitigation, tech. rep., European Union Agency for Cybersecurity (ENISA), 2021, URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[BGV12] Brakerski, Z.; Gentry, C.; Vaikuntanathan, V.: (Leveled) Fully Homomorphic Encryption without Bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ITCS '12, Association for Computing Machinery, Cambridge, Massachusetts, pp. 309–325, 2012.

[Bi21] Biondi, M.; Heid, A.; Henke, N.; Mohr, N.; Pautasso, L.; Ostojic, I.; Wester, L.; Zemmel, R.: Quantum computing use cases - what you need to know, tech. rep., McKinsey Digital, 2021, URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know#/.

[BV97] Bernstein, E.; Vazirani, U.: Quantum Complexity Theory. SIAM Journal on Computing 26/5, pp. 1411–1473, 1997.

[CAE19] Cardillo, A.; Akinyokun, N.; Essex, A.: Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology? In (Krimmer, R.; et al., eds.): Electronic Voting, 4th International Joint Conference, E-Vote-ID. Vol. 11759, Springer International Publishing, Cham, pp. 67–82, 2019.

[CD23] Castryck, W.; Decru, T.: An Efficient Key Recovery Attack on SIDH. In (Hazay, C.; Stam, M., eds.): Advances in Cryptology – EUROCRYPT 2023. Vol. 14008, Springer Nature Switzerland, Cham, pp. 423–447, 2023.

[Ch16a] Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.; Smith-Tone, D.: Report on Post-Quantum Cryptography, tech. rep., National Institute of Standards and Technology (NIST), 2016, URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[Ch16b] Chillotti, I.; Gama, N.; Georgieva, M.; Izabachène, M.: A Homomorphic LWE Based E-voting Scheme. In (Takagi, T., ed.): Post-Quantum Cryptography. PQCrypto. Vol. 9606, Springer International Publishing, Cham, pp. 245–265, 2016.

[Ch80] Christol, C. Q.: The Common Heritage of Mankind Provision in the 1979 Agreement Governing the Activities of States on the Moon and Other Celestial Bodies. The International Lawyer 14/, pp. 429–483, 1980.

[CI20] CIO Strategy Council: National Standard of Canada - Standards Proposal, 2020, URL: https://dgc-cgn.org/wp-content/uploads/2020/06/CIOSC_Standards-Proposal-Health-Data-Capability_2020-05-26-1.pdf, visited on: 09/13/2023.

[CI22] CIO Strategy Council: Online Electoral Voting – Part X: Implementation of Online Voting in Canadian Municipal Elections (D2), 2022.

[CMM17] Costa, N.; Martínez, R.; Morillo, P.: Proof of a Shuffle for Lattice-Based Cryptography. In: Secure IT Systems. NordSec 2017. Vol. 10674, pp. 280–296, Nov. 2017, ISBN: 978-3-319-70289-6.

[CMM20] Costa, N.; Martínez, R.; Morillo, P.: Lattice-Based Proof of a Shuffle. In: Financial Cryptography and Data Security - FC 2019. Vol. 11599, Springer International Publishing, pp. 330–346, Mar. 2020.

[CN10a] CNIL: Délibération n° 2010-371 du 21 octobre 2010 portant adoption d’une recom-mandation relative à la sécurité des systèmes de vote électronique, JORF number 0272 of 24 November 2010, text number 29, 2010, URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000023124205, visited on: 08/23/2023.

[CN10b] CNIL: Sécurité des systèmes de vote par internet : la CNIL actualise sa recommanda-tion de 2010. Online press release, 2010, URL: https://www.cnil.fr/fr/securite-des-systemes-de-vote-par-internet-la-cnil-actualise-sa-recommandation-de-2010, visited on: 03/29/2023.

[CN19] CNIL: Délibération nº 2019-053 du 25 avril 2019 portant adoption d’une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notam-ment via Internet, JORF number 0142, of 21 June 2019, text number 95, 2019.

[Co21] Costa, N.: Long-term privacy in electronic voting systems, https://upcommons.upc.edu/han PhD thesis, Universitat Politècnica de Catalunya (UPC), 2021.

[Cr19] Crawford, K.: Halt the use of facial-recognition technology until it is regulated. Nature 572/, pp. 565–565, Aug. 2019.

[Cr96] Cramer, R.; Franklin, M.; Schoenmakers, B.; Yung, M.: Multi-Authority Secret-Ballot Elections with Linear Work. In (Maurer, U., ed.): Advances in Cryptology - EUROCRYPT. Vol. 1070, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 72–83, 1996.

[Da22] Dargan, J., 2022, URL: https://thequantuminsider.com/2022/09/05/quantum-computing-companies-ultimate-list-for-2022/, visited on: 03/20/2023.

[DH22] Debant, A.; Hirschi, L.: Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol, Cryptology ePrint Archive, Paper 2022/1653, https://eprint.iacr.org/2022/1653, 2022, URL: https://eprint.iacr.org/2022/1653.

[Di22] Digital Governance Standards Institute: Online Electoral Voting – Part X: Implementation of Online Voting in Canadian Municipal Elections (D3), 2022.

[DJ92] Deutsch, D.; Jozsa, R.: Rapid solutions of problems by quantum computation. In: Proceedings of the Royal Society of London A. Vol. 439, pp. 553–558, 1992.

[DM15] Ducas, L.; Micciancio, D.: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second. In: Advances in Cryptology - EUROCRYPT 2015. Vol. 9056, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 617–640, 2015.

[EG20] Essex, A.; Goodman, N.: Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada. Election Law Journal: Rules, Politics, and Policy 19/, pp. 1–18, May 2020.

[El16] Electronic Voting Committee: General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia, 2016, URL: https://www.venice.coe.int/files/13EMB/13EMB_Priit_Vinkel.pdf, visited on: 08/23/2023.

[El20] ElectionsNWT: CEO Report on the administration of the 2019 territorial general election, 2020, URL: https://www.electionsnwt.ca/sites/electionsnwt/files/report_of_the_chief_electoral_officer_on_the_administration_of_the_2019_general_election.pdf, visited on: 03/09/2023.

[EN23] Estonian National Electoral Committee: General description of the framework of the i-voting system IVXV, 2023.

[Es23] Requirements to IVXV framework, URL: https://www.valimised.ee/sites/default/files/uploads/eh/IVXV%20raamistiku%20n%C3%B5uded%20kr%C3%BCptos%C3%BCsteemile%20v02.pdf, visited on: 03/29/2023.

[Fe82] Feynman, R. P.: Simulating physics with computers. International Journal of Theoretical Physics 21/, pp. 467–488, 1982.

[FOO92] Fujioka, A.; Okamoto, T.; Ohta, K.: A Practical Secret Voting Scheme for Large Scale Elections. In: Advances in Cryptology - AUSCRYPT. 1992.

[FWK21] Farzaliyev, V.; Willemson, J.; Kaasik, J. K.: Improved Lattice-Based Mix-Nets for Electronic Voting, Cryptology ePrint Archive, Paper 2021/1499, 2021, URL: https://eprint.iacr.org/2021/1499.

[GHY22] Genser, J.; Herrmann, S.; Yuste, R.: International Human Rights Protection Gaps in the Age of Neurotechnology, NeuroRights Foundation, 2022.

[Gj12] Gjøsteen, K.: The Norwegian Internet Voting Protocol. In (Kiayias, A.; Lipmaa, H., eds.): E-Voting and Identity. Vote-ID 2011. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–18, 2012.

[GPD10] Goodmana, N.; Pammett, J. H.; DeBardeleben, J.: Internet Voting: The Canadian Municipal Experience, Canadian Parliamentary Review 33(3), 13-21, 2010.

[Gr20] Greig, J., 2020, URL: https://www.techrepublic.com/article/6-experts-share-quantum-computing-predictions-for-2021/, visited on: 08/23/2023.

[Gr96] Grover, L. K.: A Fast Quantum Mechanical Algorithm for Database Search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. STOC '96, Association for Computing Machinery, Philadelphia, Pennsylvania, USA, pp. 212–219, 1996, ISBN: 0897917855.

[Gu20] Guopeng, L.: Multi-Candidate Electronic Voting Scheme Based on Fully Homomorphic Encryption. Journal of Physics: Conference Series 1678/, p. 012064, Nov. 2020.

[HG22] Hoofnagle, C. J.; Garfinkel, S. L.: Law and Policy for the Quantum Age. Cambridge University Press, 2022.

[IBa] IBM, URL: https://www.ibm.com/quantum/roadmap, visited on: 03/20/2023.

[IBb] IBM Quantum Platform, URL: https://quantum-computing.ibm.com/, visited on: 03/20/2023.

[IB19] IBM Research Blog, 2019, URL: https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/, visited on: 03/20/2023.

[JCJ05] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-Resistant Electronic Elections. In: Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society. WPES ’05, Association for Computing Machinery, Alexandria, VA, USA, pp. 61–70, 2005, ISBN: 1595932283.

[Jo11] Jordan, S., 2011, URL: https://quantumalgorithmzoo.org/, visited on: 03/28/2023.

[Ka21] Kaim, G.; Canard, S.; Roux-Langlois, A.; Traoré, J.: Post-quantum Online Voting Scheme. In: FC 2021 - Financial Cryptography and Data Security. International Workshops. Vol. Lecture Notes in Computer Science. 12676, Virtual event, France, pp. 290–305, 2021, URL: https://hal.science/hal-03355875.

[Le01] Levy, S.: Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age. 2001.

[Le95] Leiss, W.; Beck, U.; Ritter, M.; Lash, S.; Wynne, B.: Risk Society, Towards a New Modernity. Canadian Journal of Sociology / Cahiers canadiens de sociologie 19/, p. 544, Nov. 1995.

[Ma20] Martin, K.: Cryptography. The Key to Digital Security, How It Works, and Why It Matters. W.W. Norton and Company, 2020.

[Mi23] Microsoft, 2023, URL: https://learn.microsoft.com/en-us/azure/quantum/overview-azure-quantum, visited on: 03/20/2023.

[Na21] National Electoral Committee: Tehnilised nõuded elektroonilise hääletamise üldpõhimõtete tagamiseks, 2021, URL: https://www.riigiteataja.ee/akt/327012021006, visited on: 08/23/2023.

[Pi17] del Pino, R.; Lyubashevsky, V.; Neven, G.; Seiler, G.: Practical Quantum-Safe Voting from Lattices. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. CCS ’17, Association for Computing Machinery, Dallas, Texas, USA, pp. 1565–1581, 2017, ISBN: 9781450349468.

[Pu22] Pure Storage, 2022, URL: https://blog.purestorage.com/purely-informational/are-quantum-computers-real/, visited on: 08/23/2023.

[Re13] Research Institute for Security in the Information Society - E-Voting Group: UniVote, 2013, URL: https://e-voting.bfh.ch/projects/univote/.

[Rø20] Rønne, P. B.; Atashpendar, A.; Gjøsteen, K.; Ryan, P. Y. A.: Short Paper: Coercion-Resistant Voting in Linear Time via Fully Homomorphic Encryption. In: Financial Cryptography and Data Security. Vol. 11599, Springer International Publishing, Cham, pp. 289–298, 2020.

[Ro22a] Rodríguez-Pérez, A.: Secret texts and cipherballots: secret suffrage and remote electronic voting, PhD thesis, Universitat Rovira i Virgili, 2022, URL: http://hdl.handle.net/10803/675606.

[Ro22b] Rodríguez-Pérez, A.: 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. Vol. 13553, Springer International Publishing, Cham, pp. 90–105, 2022.

[SD13] Schwartz, B.; Dan Grice, J.: Establishing a Legal Framework for E-Voting in Canada, 2013, URL: https://www.elections.ca/res/rec/tech/elfec/pdf/elfec_e.pdf, visited on: 09/13/2023.

[Sh94] Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science. Pp. 124–134, 1994.

[Si97] Simon, D. R.: On the Power of Quantum Computation. SIAM Journal on Computing 26/5, pp. 1474–1483, 1997.

[Si99] Singh, S.: The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books, 1999.

[STW14] Sun, X.; Tian, H.; Wang, Y.: Toward Quantum-Resistant Strong Designated Verifier Signature. 5/2, pp. 80–86, 2014.

[SV16] Solvak, M.; Vassil, K.: E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years (2005-2015). In cooperation with Estonian National Electoral Committee, Johan Skytte Institute of Political Studies, University of Tartu, Ülikooli 18, 51003 Tartu, Estonia, 2016.

[Sw04] Swiss Federal Chancellery: Le vote électronique dans sa phase pilote - Rapport inter-médiaire. 2004.

[Sw14] Swiss Federal Chancellery: Catalogue des exigences à remplir pour recou-rir au vote électronique lors de votations popu-laires fédérales, 2014.

[Sw18] Swiss Federal Chancellery: Annex to the FCh Ordinance of 13 December 2013 on Electronic Voting (OEV, SR 161.116). Technical and administrative requirements for electronic vote casting - version 2.0, 2018.

[Sw19] Swiss Federal Chancellery: Vote électronique – Public Intrusion Test 2019. Final report of the steering committee, 2019.

[Sw20] Swiss Federal Chancellery: Summary of the expert dialog - Redesign of Internet Voting Trials in Switzerland 2020, 2020, URL: https://www.newsd.admin.ch/newsd/message/attachments/63915.pdf, visited on: 09/12/2023.

[Sw22a] Swiss Federal Chancellery: Guide pour l’appréciation des risques. Système du vote électronique de La Poste Suisse. 2022.

[Sw22b] Swiss Federal Chancellery: Révision partielle de l’ordonnance sur les droits politiques et révision totale de l’ordonnance de la ChF sur le vote électronique (restructuration de la phase d’essai). Rapport explicatif en vue de l’entrée en vigueur au 1er juillet 2022, 2022.

[Sw23a] Swiss Federal Chancellery: Appréciation des risques Vote électronique de la Chancelle-rie fédérale 2023, 2023.

[Sw23b] Swiss Federal Chancellery: Swisspost e-voting documentation, 2023, URL: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/master/System/System_Specification.pdf, visited on: 03/09/2023.

[Un21] United Nations, 2021, URL: https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening, visited on: 09/08/2023.

[Vi15] Vinkel, P.: Remote Electronic Voting in Estonia: Legality, Impact and Confidence, PhD thesis, Tallin University of Technology, Aug. 2015.

[Vo23] Vox, 2023, URL: https://www.vox.com/future-perfect/2023/3/29/23660833/ai-pause-musk-artificial-intelligence-moratorium-chatgpt-gpt4, visited on: 09/08/2023.

[Wo21] Wolf, R.: Quantum Key Distribution - An Introduction with Exercises. Part of the book series: Lecture Notes in Physics, Springer, 2021.