Information and Computation 295 (2023) 105112

Contents lists available at ScienceDirect

Information and Computation

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

Roadmap of post-quantum cryptography standardization: Side-channel attacks and countermeasures

Ari Shaller, Linir Zamir, Mehrdad Nojoumian *

Florida Atlantic University, Department of Computer & Electrical Engineering and Computer Science, 777 Glades Road, Boca Raton, FL 33431, United States of America

ARTICLE INFO

Article history:
Received 16 April 2022
Received in revised form 4 August 2023
Accepted 15 October 2023
Available online 20 October 2023

Keywords:
Post-quantum cryptography
PQC standardization
Quantum-resistant algorithms
Side-channel attacks
Attacks on PQC

ABSTRACT

Quantum computing utilizes properties of quantum physics to build a fast-computing machine that can perform quantum computations. This will eventually lead to faster and more efficient calculations especially when we deal with complex problems. However, there is a downside related to this hardware revolution since the security of widely used cryptographic schemes, e.g., RSA encryption scheme, relies on the hardness of certain mathematical problems that are known to be solved efficiently by quantum computers, i.e., making these protocols insecure. As such, while quantum computers most likely will not be available any time in the near future, it's necessary to create alternative solutions before quantum computers become a reality. This paper therefore provides a comprehensive review of attacks and countermeasures in Post-Quantum Cryptography (PQC) to portray a roadmap of PQC standardization, currently led by National Institute of Standards and Technology (NIST). More specifically, there has been a rise in the side-channel attacks against PQC schemes while the NIST standardization process is moving forward. We therefore focus on the side-channel attacks and countermeasures in major post-quantum cryptographic schemes, i.e., the final NIST candidates.

1. Introduction

It is known that quantum computing is an incoming threat towards many of the current major Public-Key Cryptosystems (PKC), such as Rivest–Shamir–Adleman (RSA), Diffie-Hellman (DH), and Elliptic Curve (EC) cryptosystems. These cryptographic schemes rely on the hardness of Integer Factoring (IF) problem or Discrete Logarithm (DL) problem, which can be broken in polynomial time using Shor's algorithm [1,2]. There are many predictions towards the realization of large-scale quantum computers, ranging from as early as 2026 [3,4] to somewhere between thirty to forty years to come [5]. Despite that, the issue of quantum computing is deemed concerning enough that the National Institute of Standards and Technology (NIST) announced their plan on standardizing and transitioning from conventional cryptography to Post-Quantum Cryptography (PQC), followed by a similar announcement from the National Security Agency (NSA).

Post-quantum cryptography refers to cryptographic algorithms that are based on hard mathematical problems, which can withstand the attacks of both conventional and quantum computers. There are major families of the PQC cryptosystems that are as follows: *Code-based, hash-based, isogeny-based, lattice-based*, and *multivariate-based*. There are many cryptosystems being studied throughout the years, including some of the earlier ones, McEliece [6] and Niederreiter [7]. Although these

* Corresponding author.
E-mail addresses: ashaller2017@fau.edu (A. Shaller), lzamir2016@fau.edu (L. Zamir), mnojoumian@fau.edu (M. Nojoumian).

https://doi.org/10.1016/j.ic.2023.105112
0890-5401/

cryptosystems are quantum-resistant, they are still vulnerable to side-channel attacks. This type of attack, first demonstrated in the research by Paul Kocher et al. [8,9], is able to recover secret information by exploitation of physical leakages. More specifically, the authors studied the exploitation of timing variation on DH, RSA, and other cryptosystems and continued on the topic of side-channel attacks with simple and differential power analysis.

Although extensive research has been conducted regarding other kinds of information leakage., the literature is still lacking compared to the number of algorithms available to be tested, the kind of side-channels and attacks to be observed, and the hardware or software to be employed. Besides, there are an overwhelming number of open problems to be scrutinized in this landscape. We therefore assess attacks and countermeasures in PQC by focusing on latest advancements in this field.

1.1. Our motivation and contribution

Side-Channel Attack (SCA) is comparatively inexpensive and easy to perform since comprehensive understanding of the system is sometimes not needed. This type of attack does not affect only particular algorithms, but all implementation-specific algorithms. With the threat of quantum computers, and therefore, the increase in effort to create quantum-resistant algorithms, there are emerging algorithms that are required to be assessed and evaluated from various security perspectives.

Security against SCA is unknown in many of these algorithms. This can become a source of leakage in a wide range of information systems. Indeed, even without considering new post-quantum hardware and software technologies, if security against side-channel attacks is ignored, the new algorithms will still be insecure in their real-world implementations despite being resilient against quantum attacks. That is why, in addition to quantum-safe algorithms, it is imperative that researchers also pay as much attention to the study of PQC algorithms with side-channel resistance.

As stated earlier, the literature on post-quantum cryptography, especially on side-channel attacks and its countermeasures, is still lacking. In other words, with the number of newly-developed algorithms, attacks, software, or hardware, there is a significant gap in the literature that needs to be filled. This paper therefore provides a roadmap for researchers in academia and industries who are conducting research on quantum-safe software and hardware platforms.

1.2. Organization of the paper

Section 2 provides preliminary materials regarding PQC. Section 3 reviews side-channel attacks and countermeasures regarding post-quantum cryptography in the order of code-based, hash-based, isogeny-based, lattice-based, and multivariate-based families. Finally, Section 4 provides concluding remarks.

2. Preliminary materials

This section provides a basic introduction to post-quantum cryptography and its major families, including the mathematical methods used for each cryptography family. Additionally, it will introduce the methods for evaluating side-channel leakage.

2.1. Post-quantum cryptography

PQC is a cryptographic paradigm that is secured by definition against attacks of both conventional and quantum computers. Quantum computers provide adversaries with the ability to solve computationally expensive mathematical problems faster than any classical computer. This can then break some of the most commonly used cryptographic encryption systems, which rely on the hardness of some mathematical problem. Note that there is no PQC setting such that the underlying mathematical problem can not be solved. In the worst case scenario, it can be solved by exhaustive search. All of these mathematical problems are based on computationally hard problems, which have appropriate algorithms to solve them, but are computationally too expensive even for quantum computers. Many PQC solutions have been made to meet the requirements and criteria of post-quantum cryptography, and depending on its mathematical foundation, each of those proposed algorithms belongs to one of the families of post-quantum cryptography. These major families are code-based, hash-based, isogeny-based, lattice-based, and multivariate.

1. *Code-Based*: Cryptosystems from this family utilizes error-correcting codes that operate on bits. These codes receive its name for its ability to detect and correct a limited number of errors in a sequence of bits. The first cryptosystem of this family was proposed in 1978 by Robert J. McEliece [6]. The McEliece cryptosystem utilizes a generator matrix for its public-key and a Goppa code for its private-key. In 1986, Niederreiter [7] developed a cryptosystem with a parity check matrix. Later, there were some modifications and improvements on the McEliece cryptosystem, for example using systematic generator matrix and quasi-cyclic moderate parity check.
2. *Hash-Based*: The idea of hash-based cryptography is that multiple instances of One-Time Signature Scheme (OTS) are combined with a secure hash function so that they can be used more than once. Merkle [10] proposed this and created Merkle Signature Scheme (MSS) that now has many variants including the eXtended Merkle Signature Scheme (XMSS) and the multi-tree version XMSS^{MT}. There are two kinds of hash-based signature algorithms: Stateful and stateless. Stateful hash-based signatures are more difficult to manage because each signature key has a state that must be changed

Table 1
PQC candidates in the NIST 4th-round of standardization. Those in bold are finalists and the rest are selected algorithms.

Family	Public-key Enc/Key-establishment Algorithms	Digital Signatures
Code-based	**BIKE, Classic McEliece, HQC**	-
Hash-based	-	SPHINCS+
Isogeny-based	SIKE: Initially selected but not secure anymore [14]	-
Lattice-based	Crystal-Kyber	Crystal-Dilithium, Falcon
Multivariate	-	-

after the key has been used. On the other hand, stateless signatures do not need to change the state of the signature key, resulting in an easier implementation.

3. *Isogeny-Based*: This cryptography is based on the hard problem of finding an isogeny between two supersingular elliptic curves. This idea was first introduced by Rostovtsev and Stolbunov in 2006 [11] as isogenies between ordinary elliptic curves. In 2012, the algorithm was broken using a 'subexponential-time quantum algorithm' attack by Childs, Jao and Soukharev in [12]. That same original idea was then further developed by Jao and De Feo as a key exchange mechanism over supersingular elliptic curves. The new algorithm, named Supersingular Isogeny Diffie-Hellman (SIDH) [13], utilizes the idea of walking through a sequence of supersingular elliptic curves. Compared to the code-based and lattice-based cryptography, the isogeny-based cryptosystem has a much smaller key size; however, a recent work by Castryck and Decru [14] showed an efficient key-recovery attack on SIKE that exploits the auxiliary points. This attack made SIKE insecure.
4. *Lattice-Based*: First introduced by Ajtai in 1996 [15], lattice-based cryptography is based on the hardness of solving lattice problems. One of these problems is called the Short Vector Problem (SVP). In 1997, Ajtai and Dwork [16] presented a public-key cryptosystem using the modification of this problem called u-SVP, which tries to find a unique nonzero shortest vector v in an n dimensional lattice L. The first scheme of this family is NTRU, proposed in 1998 by Hoffstein et al. [17].
5. *Multivariate*: This family of cryptography is constructed based on multivariate polynomials over a finite field. Matsumoto and Imai created an asymmetric cryptosystem based on multivariate polynomials, called C* in 1988 [18]. A decade later, in 1999, Kipnis et al. [19] proposed a new scheme, named Unbalanced Oil-and-Vinegar (UOV), that is a modification of the previously Oil and Vinegar scheme by Patarin [20].

Table 1 illustrates the cryptographic schemes from five PQC families based on the National Institute of Standards and Technology (NIST) fourth-round standardization results. NIST recognized the potential threats quantum computing can bring to current security algorithms such as RSA, so they initiated a standardization process with a competition to find the best overall post-quantum cryptography algorithms.

2.2. Side-channel attacks

In a side-channel attack, an adversary gains information from power output traces, electromagnetic radiations, execution times or any other leaked residual data by relating this information with operations made by the attacked unit. This relationship can create a pattern that the adversary can then use to recover secret information of the cryptographic system. There are different possible categories for side-channel attacks, which are:

1. **Power Attack**: In this method, adversaries can measure the power consumption of some cryptographic device. By analyzing the different power surge outputs, the adversary can gain some information on the encrypted secret. These types of SCA can be divided into several subtypes such as Simple Power Analysis (SPA), where the adversary collects power traces from the same input, or Differential Power Analysis (DPA), where the adversary collects input power traces and analyzes the power consumption as an instance of a function of the processed data. An effective power attack is usually a combination of several SCA methods.
2. **Timing Attack:** Cryptographic devices' running time can give useful information to an adversary who listens and measures the changes in time for a set of different messages.
3. **Fault Attack:** This is a type of active SCA where the adversary attempts to induce errors in an algorithm to expose information. Faults may be induced through various means such as electromagnetic injection, voltage, etc. There are various fault attacks such as *randomization, bit-flipping*, and *zeroing*.
4. **Electromagnetic Attack:** Electronic charges moving through the system can have unique characteristics that the adversary can measure and analyze. Similar to power attack, the electromagnetic attack only requires observations.
5. **Optical Attack:** This is a less common attack that utilizes emitted visual information, usually in the form of photons that are being transmitted, when a logic state changes. Special sensors can detect such sensitive information and correlate it to the transmitted data. A variation of the optical attack is the Thermal Imagery attack, where the sensors can detect thermal changes in the operation.

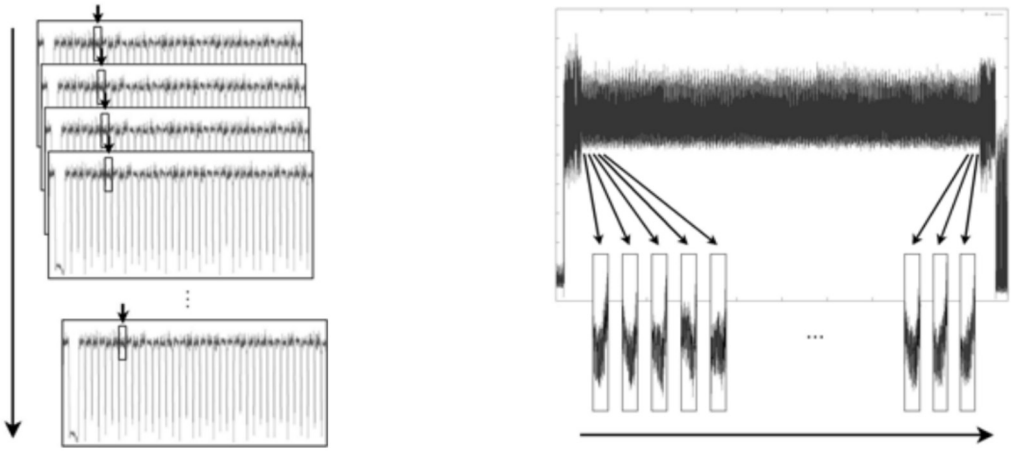

Fig. 1. Vertical (left) and Horizontal (right) attack. [21].

6. **Acoustic Attack:** Keystrokes, CPU operations and other devices produce special sound that can be detected, analyzed and deciphered to extract valuable information regarding a cryptosystem.

Side-channel attacks can be the basis for more advanced cryptographic attacks. As an example, among others, we can refer to *collision attack*. In this attack, the adversary can attack some cryptographic functions by reading its intermediate values looking for collisions. Since a collision can only occur for a subset of keys, observing a few collisions can help the adversary to identify a unique key. Detection of these collisions is possible by reading the intermediate values with some SCA, e.g., power channels.

2.2.1. Shapes of attacks

Ref. [21] presents a distinction between *horizontal* and *vertical* attacks. In vertical attacks, the adversary can obtain sensitive information by analyzing the same output data of several side-channel traces, whereas in horizontal attacks, the adversary can extract sensitive information by analyzing several parts from a single trace, as shown in Fig. 1.

Attacks are usually either vertical or horizontal, however, it is possible for an attacker to combine both attacks into what is called *Rectangle* attack [22].

2.3. SCA countermeasures

Side-channel attacks have been proven to be effective against many cryptographic algorithms. This has raised the need for countermeasure methods that can provide the needed security against these special types of attacks. Countermeasures techniques to side-channel attacks mask, hide or shuffle the residual leakages of an algorithm, e.g., its power consumption, by either making them independent from the output value or by reducing the release of leaked data.

With the increase of the effectiveness of side-channel attacks, more state-of-the-art countermeasures have been introduced. Most of them fall into two main types: Hardware-based and software-based. Hardware-based countermeasures usually include modifications to the hardware layer such as internal clock randomization, power consumption modifications, and/or usage randomization. Software-based countermeasures include sharding, bit splitting, and other algorithmic changes to prevent adversaries from gaining information. Countermeasures are usually deployed in both software and hardware to achieve a high level of security. This paper covers some of the commonly used countermeasures for side-channel attacks. Most of them fall within the following methods: Masking, hiding, or randomizing. Each one of these methods can be implemented in hardware, software, or a combination of both.

2.3.1. Masking

Masking is a common countermeasure method that usually involves splitting the sensitive cryptographic data into random shares. The side-channel leakage from an individual share is not enough to reveal the sensitive data. The value of the mask must be known in order to reconstruct the sensitive data. This method, however, can be vulnerable to methods that measure and combine side-channel leakage from multiple shares, e.g., DPA style attack.

2.3.2. Hiding

Hiding is a methodology that aims to hide the leaked data in a time constant process across the cryptographic scheme such that the output power consumption is kept constant. This countermeasure method has two categories: *Time altering*, e.g., adding dummy operations throughout the run or shuffling the operations for each time constant, and *amplitude change*, e.g., increasing the level of noise in the system or reducing the output signal [23].

Table 2
NIST Code-Based PQC: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
Classic McEliece	Timing Attack [39]	Timing attack against an existing McEliece implementation using Patterson Algorithm during decoding step of decryption phase. The attack finds a connection between the error vector wright and the number of iterations made by the Extended Euclidean algorithm [58,59].	To raise degrees of the error locator polynomial. A secured modified algorithm is proposed in [39] with a constant run time that performs no jumps related to the secret input, and only accesses memory addresses depending on public input.
	Simple Power Analysis [38]	Attack targets information leakage from power traces on operations, different instructions such as save and load. It then learns sensitive data including possibly the secret error vector [60]. Another possibility is by targeting the secret permutation matrix in the cryptosystem. A microcontroller implementation can execute this attack [40].	Software level design to prevent power spikes with branch statement and data dependent running time.
	Differential Power Analysis [42]	The first successful DPA on quasi-cyclic MDPC McEliece implementation. This attack targeted the syndrome computation and the key rotation exposing weaknesses to power attacks in both. Another successful DPA attack is by targeting the bit permutation, as described in [39].	Shuffling the syndrome computation would prevent the leakage with low overhead. Another proposed countermeasure is a masking technique which adds Goppa codewords to ciphertexts during the permutation algorithm.
	Fault Attack [30]	This paper looked at the McEliece scheme to see if m can be corrupted and not corrected, if the output of $m \times G$ is faulty, and if there is a fault on the vector e. McEliece was found to be resistant to fault injections due to the error correcting code. It is noted that in QC and QD matrices, the scheme is more susceptible.	Dedicated hardware which computed the encryption twice for comparison would help stop a fault injection attack.
	Reaction Attack [51]	An adversary can gain sensitive information by observing the reaction of someone decrypting a ciphertext with its private key.	Countermeasures include a modification to the original protocol that is resistant to reaction attacks exploiting decoding failures [33], using stochastically generated negative acknowledgments sent in the feedback channel to mask some of the operations and using an outer fountain code that makes feedback channels redundant.
QC-MDPC	Timing Attack	Using an iterative bit-flipping algorithm to attack the decryption procedure is shown to be effective for the key recovery attack [61].	Repeated encryption can help the security of the scheme against timing attacks [62].
	Differential Power Analysis	A constant-time implementation for QC-MDPC code-based cryptography for mitigating timing attacks was found to be vulnerable to differential power attacks [32]. This was a base for other single and multiple-trace attacks [63].	Applying a randomization of countermeasures such as intermediate data masking before the syndrome computation.
	Reaction Attack	A key recovery reaction attack has been proven to be useful against BIKE's decoder, as a correlation between the distances of 1's in the decryption key and its secret [64].	Reworking the decoder to have it more powerful and reduce the decoding error probability.

2.3.3. Randomizing

A simple yet effective method to handle SCA is to randomize the data that may leak through. This includes randomizing the execution time, power consumption, or any other data that adversaries can use to gain information. This method requires an understanding of the possible side-channel attacks that adversaries can utilize in order to know what variables should be randomized. Given its random nature, it is impossible to guarantee that the adversary will not gain useful information.

3. PQC attacks and countermeasures

In this section, the current research on attacks and corresponding countermeasures for PQC is thoroughly reviewed. Also, side-channel attacks and countermeasures for alternate candidates will be briefly discussed. This section is organized based on the PQC families. Note that we will just review the proposed attacks and countermeasures, however, this does not mean all attacks are well-countered. Coming up with stronger attack strategies as well as secure countermeasures is an ongoing effort in the PQC community.

3.1. Code-based PQC

Code-based cryptography relies on error correcting codes that are used to deal with errors in data over noisy channels. We now discuss some well-known attacks against code-based PQC. At the end of this section, Table 2 summarizes attacks and countermeasures for code-based PQC.

The classic McEliece is a candidate algorithm for post quantum public-key cryptosystems that is based on the general decoding problem, which is NP-hard and thus can withstand attacks by quantum computers [24]. The private-key for McEliece is a random binary irreducible algebraic geometric code, also known as Goppa code, and the public-key is a random generator matrix of randomly permuted variants of that code. The ciphertext is a codeword with added errors such that only the one in possession of the private-key can remove the errors. Since McEliece relies on an NP-hard decoding problem, there are no effective quantum algorithms for breaking it, which makes it one of the few known algorithms that is safe against PQC attacks.

Similar to other schemes, McEliece has some security drawbacks. One of which is its susceptibility to side-channel attacks [25]. A commonly used SCA is called a reaction attack, proposed by Hall et al. [26], where the adversary can gain sensitive information by observing the reaction of someone decrypting a ciphertext with its private-key. Another drawback is the long public-key sizes that are disguising generator matrices for Goppa codes. There have been many proposed solutions and different McEliece modifications to handle these security problems and shorten the public-key size, however, many of these solutions failed. Some of the commonly used McEliece modifications and their known attacks are presented as follows.

A Low Density Parity Check (LDPC) code correction, instead of Goppa solution, was proposed by Monico et al. [27]. LDPC is a code-correction code that uses a parity check matrix where each of its columns and rows contains a fixed number of nonzero entries. Quasi-Cyclic LDPC, proposed by Baldi et al. [28], is an improved version of the LDPC McEliece proposal where a low-complexity encoding with a high-performance decoding is achieved. QC-LDPC solution provides a much smaller public-key size and is considered a secure and efficient solution. Another improvement to the LDPC McEliece Cryptosystem was proposed by Misoczki et al. in [29], named Moderate Density Parity-Check (MDPC). The security of this new version has the benefit of relying on a single coding-theory problem. Quasi-Cyclic Moderate Density Parity-Check (QC-MDPC) is similar to the QC-LDPC, however, it provides extremely compact-keys. Cayrel and Dusart present an effective fault injection attack in [30]. McEliece cryptosystem is considered secure against this type of attack due to its ability to correct faults that may occur. Quasi-cyclic, however, shows a greater sensitivity to fault injection attacks because of its compact matrices; since faulty rows are used several times.

QcBits [31] is a public-key algorithm, another variant of the McEliece, that utilizes a constant time key-pair generation for QC-MDPC encryption scheme while maintaining quantum attack resistance. However, Rossi [32] showed that using a DPA attack, partial information of the private-key can be recovered, and then using a system of noisy binary linear equations, the entire key can be revealed. To defend against side-channel attacks during syndrome calculations in QcBits, a simple masking procedure is proposed by XOR-ing the corrupted codeword with a random word prior to syndrome calculation, which effectively masks the DPA leak. Since this is only effective during syndrome calculations, additional side-channel countermeasures should be considered to fully protect the private-key during other calculations. Santini [33] proposed using monomial codes to form private-keys in place of using Quasi-Cyclic Low Density Parity-Check (QC-LDPC) or QC-MDPC, which are vulnerable to exploitation of decoding failures. This is the first McEliece cryptosystem variant that admits non-negligible decoding failure rate and hinders reaction attacks. Although public-keys are larger than QC-LDPC and QC-MDPC code-based variants, they are significantly smaller than Goppa variants that are not subject to reaction attacks.

Bit-flipping Key Encapsulation (BIKE) [34] is a code-based PQC that corrects errors in a QC-MDPC linearcode. This design uses an ephemeral key-pair in order to prevent possible reaction attacks. Reinders [35] proposes a hardware setting implementing a block-based design that takes advantage of side-channel resilience of wide word multiplier blocks. Hamming Quasi-Cyclic (HQC) cryptosystem is a candidate algorithm for the NIST post-quantum standardization project. Liu et al. [36] show that the hardness assumption for previous versions of HQC, i.e., s-DQCSD, does not hold, claiming HQC cannot attain Indistinguishability under Chosen-Plaintext Attack (IND-CPA) security with the proposed parameters. A proposed modified scheme of HQC that can attain IND-CPA security with the hardness assumption of s-DQCSD with a variable weight was then proposed. It relies on Bose–Chaudhuri–Hocquenghem (BCH) codes with repetition codes [37]. The attack exploits a correlation between the weight of error and running time of decoding BCH codes using Berlekamp's simplified algorithm. This attack takes less than one minute with a success probability of finding the key at 93%. By using a constant running time for the algorithm, the adversary will not be able to perform timing side-channel attacks, included are two variants for constant time algorithm for BCH codes.

There have been several successful simple power analysis attacks on McEliece public-key cryptosystem. [38–40] has extensively reviewed simple power analysis attacks that exploit information leakage due to the relation between the error of vector weight and the iteration number of the extended Euclidean algorithm used in Patterson's Algorithm. The attack relies on flipping one bit of the ciphertext and measuring the output power trace. If the bit flipping causes an increase to the weight of the error vector, then the bit flipped is not correct. Similarly if the bit flipping is correct, then there is a removal of the bit in the error vector. Flipping two correct bits causes a reduction to the iteration number thus exposing a leak. The power trace samples were easily identified by the iterative nature of the algorithm, due to the Extended Euclidean Algorithm (EEA), and the iteration number can be determined by counting the power peaks in those positions. This relation revealed the secret error vector, allowing for an adversary to decrypt the message. Petrvalsky [41] used an SPA attack targeting the computation of the private permutation matrix to recover the whole bit permutation matrix. In this attack, observing traces of the syndrome computation can lead to the detection of modulo 2 additions. If the adversary locates every modulo 2 addition for every cipher input with only one bit equal to one, the permutation matrix is recoverable.

Differential power analysis attacks have had successful implementations on hardware McEliece cryptosystems. Chen et al. [42] was the first to use a differential power analysis to exploit two leakages that occur during the syndrome computation

step of the decryption. The analysis was not affected by padding, commonly used to achieve Chosen-Ciphertext Attack (CCA) security. The leakage of the syndrome register gives information on the two secret key halves and succeeds with tens of power traces. The key recovery stems from the relation between private and public-key such that only half of the bits of the secret key are needed to recover the full key. [43] continued this research by completing a DPA on a hardware Field Programmable Gate Arrays (FGPA) implementation with a horizontal attack. During this attack, the syndrome computation followed by an algebraic step, that relates the public and private-key, was exploited on a QC-MDPC McEliece implementation. A counter to this attack utilizes a parallelized implementation, as proposed in [44]. Another DPA attack was found successful by Petrvalsky [45] who was able to recover the whole 64×64 permutation matrix during McEliece PKC decryption. Positions of permuted bits are obtained by searching for correlation peaks of the power traces. By knowing the position of bits in the input cipher and the position of the same bits in permuted ciphers, the permutation matrix is recoverable.

Some interesting insight into the security of McEliece, from Couvreur [46], shows that families of Goppa code can be distinguished from random codes by square considerations and attacks. High rate Goppa code and Goppa code with degree of extensions equal to 2 can be distinguished from random codes. Even though it was only shown to exploit a particular class of Goppa code, further research should be considered if similar attacks can exploit other Goppa families.

A masking countermeasure for McEliece [38] is to detect the untimely termination of the extended Euclidean algorithm, and if this is the case, to continue the EEA until proper degrees of the error locator polynomial are achieved such that the weight of the error vector is equal to the degree of the error locator polynomial. Doing so masks the power traces for the EEA implementation, closing the information leak on the simple power analysis. Other countermeasures for securing McEliece cryptosystem, proposed by Bernstein [47], include increasing n, the length of code used, using a list-decoding algorithm for classical irreducible binary Goppa code [48], and utilizing concrete parameters for CCA2- secure variants. More recent masking techniques [45] suggest adding Goppa codewords to ciphertexts during the permutation algorithm to protect from a DPA. Performing identical steps to the addition operations during encryption can remove patterns during power traces for a simple power analysis [41]. There is further research to be conducted on the amount of information leakage that occurs during each of these masking techniques.

Most countermeasures that have been applied to MDPC McEliece to prevent information leaking come at the cost of large overhead performance, usually requiring upwards of double the storage and computational time needed. Chen [42] suggests an approach to hiding, called shuffling [49], that processes the ciphertext bits and key bits in a random order rather than a predictable one. Shuffling the syndrome computation may not be so simple as Veyrat [50] discusses shuffling the syndrome computation in such a way that no information leaked is quite difficult and not always sufficient. Shuffling the syndrome calculation successfully is incentivizing because of the low overhead cost to implement. Adversaries using a DPA or SPA rely on understanding the timing, or predictability, of when a specific key bit is processed during encryption, therefore having a random order for these processes would make the analysis harder. Combining masking with shuffling is frequently used to import security of small embedded devices [50].

Two countermeasures against reaction attacks on McEliece cryptosystems are QC-LDPC and QC-MDPC, which have shown to help bring McEliece closer to practical applications with greater security. Due to the nature of timed attacks against QC-MDPC systems, Farkas [51] proposed two countermeasures to help McEliece cryptosystems that are using QC-LDPC or QC-MDPC. The first one is to "send more NACKs [Negative Acknowledgement] in the feedback channel than dictated by decryption failure to make the feedback channel as stochastic as possible" [51]. The other is to use fountain code as an outer code for McEliece, transforming the Automatic Repeat ReQuest (ARQ) scheme into an Forward Error Correction (FEC) scheme. There have been several hardware implementations of McEliece [52–55,44,56,57]. For instance, [57] implemented a hardware design of the 128-bit CCA2 secure McEliece cryptosystem by incorporating a BLAKE-512 module, a cryptographic hash function, into the architecture and a complete binary-EEA algorithm for the Goppa field on a Virtex-6 FGPA showing a resistance to timed attacks. This architecture will help to develop similar cryptoprocessors for other cryptosystems in the future.

3.2. Hash-based PQC

A hash function is an efficient mapping of binary strings of arbitrary length to binary strings of a fixed length, called hash value. Hash-Based Signatures (HBS) use the security property of a one-way function, pre-image resistance, second pre-image resistance, and collision resistance such that an adversary cannot change the information without changing the hash value. There are two types of HBS schemes: *stateful* and *stateless*. A hash function resistant to an attack is mostly correlated to the number of bits, n, of the hash value. Table 3 summarizes attacks and countermeasures for hash-based PQC.

3.2.1. Stateful

The stateful HBS scheme private-key is a set of one-time signature private-keys such that no unique one-time signature (OTS) key is ever used to sign more than one message. A message is signed when a randomly generated private-key x is applied to a hash function H creating a public-key. This process is repeated where the input becomes $H(x_k)$, creating a hash chain. McGrew et al. [65] explain the importance of the signing process to be executed in a controlled environment such that the aforementioned condition is met. An example of OTS is the Winternitz scheme, a.k.a. WOTS [10], that was first introduced in 1989 by Merkle as an optimization of the one-time signature scheme, first described by Lamport [66], a.k.a., Lamport-Diffie OTS. WOTS OTS scheme can sign many bits on a single run, determined by the Winternitz parameter, and

Table 3
NIST Hash-Based PQC: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
SPHINCS+	Differential Power Analysis	The differential power attack has been proven to be useful against SPHINCS and XMSS variants. Multi-target platforms are used to collect power traces from both hardware and software implementations. SCAUL [77] is a secret key recovery attack that does not require any prior knowledge of the system and it has been proven to be useful and effective.	Simple countermeasures such as addition of random clock jitters have been proven to be helpful in preventing DPA attacks.
	Fault Attack	[78] presents the first practical fault attack against hash-based cryptography. The attack allows the creation of signature forgery.	Countering a fault injection attack for hash-based crypto has been proven to be challenging. The only currently known countermeasure is the work of Kermani et al. [76], where they found a way to detect such an attack by recomputing subtrees with swapped nodes. However, this countermeasure does not guarantee safety against all forms of fault attacks.

it is considered resistant to attacks by quantum computers. There have been many proposed improvements for the WOTS scheme. The WOTS+ [67], proposed by Hülsing, offers a shorter signature without compromising the security and it has been included as a standard in the IETF. Buchmann et al. proposed the WOTS PRF [68], which is another variation of the WOTS that uses pseudorandom function (PRF) instead of the original hash function. Since OTS schemes are single-use, their applicability for general use is improbable.

To conquer the obstacle of limited use of OTS, Multi-Time Signature Schemes (MTS) were introduced. These schemes create many-time signatures using OTS as a foundation. Merkle Signature Schemes [10] (MSS) create multiple public and private-key by concatenating a set of OTS key pairs into a single binary hash tree structure. As Cooper [69] explains, a hash tree is created by an OTS public-key hashing once to form the leaves, which are then hashed together in pairs to form the next set leaves and so forth until all the public-keys have been used to generate a single hash value, a.k.a. the root of the tree. This will then be used as a long-term public-key. Examples of this are extended Merkle signature schemes and Leighton-Micali Scheme (LMS). Hierarchical Signature Schemes (HSS) are MTS schemes that use hash-based signatures to form a hyper tree by chaining trees of multiple layer MSS trees [70]. Examples of this are XMSS^{MT}, XMSS with tightened security (XMSS-T) and LMS.

3.2.2. Stateless

The major drawback of the stateful scheme is the necessity to cache the last used OTS key pair. The Stateless Signature Schemes (SSS) accomplish this by using few signature schemes. Some examples of this are Hash-to-Obtain-a-Random-Subset (HORS), PRNG-to-Obtain-a-Random-Subset (PORS), and HORS with Tree (HORS-T). SPHINCS [71], a stateless HBS, uses a hyper tree with the upper layers using XMSS and Winternitz type One-Time Signature Scheme (WOTS+) to sign roots of their ancestors and the lowest layer using a Merkle tree construction with HORS-T for signing messages. SPHINCS uses multiple HORS-T key pairs and randomly selects one per signature generation, resulting in no need for path-state tracking. The third round of the NIST PQC standardization considered SPHINCS+ and Gravity-SPHINCS as alternate candidates resilient to PQC attacks. Both are two different improvements of the original SPHINCS algorithm by using the HORST, which was introduced in the original SPHINCS in a slightly different way.

3.2.3. Attacks and countermeasures

Attacks on hash algorithms look for a message with the same message digest as a message that has already been signed (a second pre-image), or look for any two messages that have the same message digest (collision) and try to get the private-key holder to sign one of them [72], also called a two message attack. It is much more likely that an adversary would find a generic collision than finding the second pre-image. A large weakness of hash-based signature schemes is that they are susceptible to fault attacks and to a lesser extent side-channel attacks. Genet [73] describes the first practical fault attack against hash based PQC. The attack is performed on the original stateless scheme SPHINCS. A fault attack requires signing a message M to obtain a valid signature. Then by resigning the same M, the scheme will produce the same signature, passing through the same path of the hyper tree. Once a sub-tree is successfully forged, it can be used to sign an arbitrary message $M\prime$. There are few countermeasures to a fault attack on hash-based schemes and this could be an area for further investigation. Some related advancements [74] made use of Grover's algorithm to reduce a quantum pre-image attack's time complexity from $O(2^{n/2})$ to $O(2^{n/3})$. There has not been significant research conducted into hash pre-image attacks. Most quantum attack algorithms focus on hash collision resistance. MJ Kannwischer et al. [75] analyze the differential power analysis attack on XMSS and SPHINCS. They found that the new version of XMSS can withstand the proposed attack, however, SPHINCS is still susceptible to it.

In order to avoid reuse of an OTS key, the state of the private-key must be updated after each signature generation. One method uses a counter to act as a pointer to the current value of the OTS key for use, which can help avoid unintentional reuse of the same key. There are cryptographic hardware implementations which guarantee to increment each time the

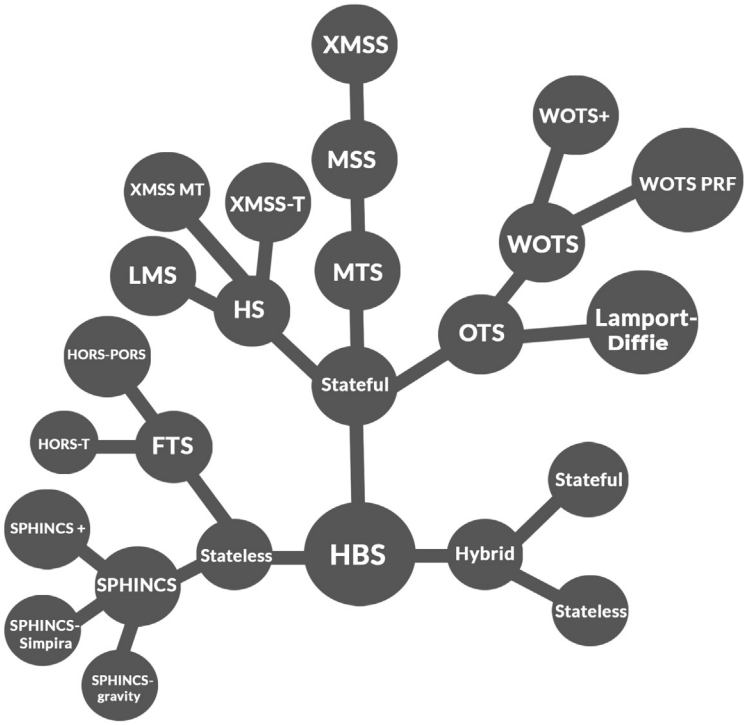

Fig. 2. Roadmap of the Hash-Based Cryptography.

counter's value is read [69]. Mozaffari et al. [76] suggest one of the only current methods to protect against fault attacks by detecting the fault through recomputing the sub-trees with swapped nodes and to implement an enhanced hash function designed to be resistant. The only known method to be completely resistant to fault attacks is to only use each OTS once and store them. Caching systems are widely used in XMSS^{MT} and LMS as an efficient way of storing one OTS per sub-tree layer and refreshing upon each new sub-tree. If corruption occurs on a sub-tree while the signature is being cached, an adversary can not discover the secret key [73]. Future research is needed on the implementation of new countermeasures for fault attacks on hash-based signature schemes. Fig. 2 shows a roadmap of the current hash-based cryptography including some of the alternate candidates of NIST PQC standardization.

3.3. Isogeny-based PQC

Isogeny-based cryptography is the method of establishing a secret key through an invertible algebraic map between elliptic curves. There are two main computations for isogeny-based cryptography: generating a secret kernel and computing a large-degree isogeny over the kernel. This field is relatively new and requires extensive research and testing. Isogeny cryptosystems are based on supersingular elliptic curves and error-correcting code that are considered to be resilient to quantum computers in the future. Quantum attacks against supersingular elliptic curves remain exponential due to the non-commutativity of the endomorphism ring. The benefits of PQC isogeny schemes are the small key and signature sizes. The security of isogeny-based algorithms relies on the difficulty of solving Elliptic Curve Discrete Logarithm (ECDL). Table 4 summarizes attacks and countermeasures for code-based PQC.

Koziel et al. [79] show the first hardware implementation of the Supersingular Isogeny Diffie-Hellman (SIDH) protocol. This design is a fast and scalable architecture for isogeny-based cryptosystems that presents an efficient finite-field arithmetic and scheduling methods. SIKE [80] is a Supersingular Isogeny Key Encapsulation based on pseudo-random walks in supersingular isogeny graphs that was a candidate for the NIST round 2 standardization process. Since the secret kernel generator uses a double-point multiplication over a torsion basis, which share many similarities with traditional elliptic curve cryptography, an adversary may use existing side-channel attacks for elliptic curves [81]. The other approach is to perform various walks of small degrees on an isogeny graph using the hidden kernel point, and if the adversary can identify these walks, they then discover a subset of the isogeny computation between two distant isomorphism classes [81]. This weakens the SIKE security. Zhang et al. [82] successfully executed the first side-channel attack on SIKE, implemented on a real ARM-based device. The differential electromagnetic attack only needed a few hundred traces for successful recovery of the key. A window based countermeasure was proposed to eliminate vertical leakage and prevent side-channel attacks with little cost.

Table 4
NIST Isogeny-Based PQC: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
SIKE	Refined Power Analysis [89]	Three attacks proposed: Partial-zero attack on Three Point Ladder (TPL) [13]. A zero point attack on the three-point differential ladder. A power analysis on large-degree isogenies.	A countermeasure method [93] utilizes a combination of randomized projective coordinates. This countermeasure defense can be efficient against most known forms of DPA with isogeny-based implementations.
	Fault Attack [90]	This is the first fault attack on super-singular isogeny cryptosystems. The attack works against signature schemes but not key-exchange protocols. Even though the fault will stop the validity of the signature, since a signer will not change the long-term secret, an adversary can gain information on the secret.	To check the order before publication of the auxiliary points or to compress the points R and $\phi(R)$ if the challenge bit is 0.
	Fault Attack (Loop-abort faults) [92]	This is the first attack on supersingular isogeny-based schemes that doesn't use the validation method of [91].	
	Key-Recovery Attack [14]	This attack exploits the auxiliary points. This attack made SIKE insecure.	

Castryck et al. [83] propose an adaptation of the Couveignes–Rostovtsev–Stolbunov scheme to the Supersingular Elliptic Curve, called Commutative Supersingular Isogeny Diffie-Hellman (CSIDH), which is considered to be efficient compared to SIDH, while still providing a non-interactive key exchange and validation. Banegas et al. [84] proposed a Constant Time Isogeny Diffie-Hellman algorithm (CTIDH) as a new and faster constant-time algorithm to evaluate the CSIDH group. This is achieved mainly by the organization of primes and isogenies in batches that improves its speed and security.

Jaques and Schanck [81] introduce a model of quantum computation to compare between classical and quantum algorithms. The comparison of claw-finding attacks, between Grover's and Tani's algorithm, on SIDH and SIKE provides a model for cryptanalysis that should be relevant to other cryptanalytic algorithms that use quantum walks on Johnson graphs. These include subset sums, information set decoding, and quantum Merkle puzzles. This research only looked at quantum access to quantum memory stating that there may be inexpensive quantum access to classical memory. The comparison showed that Tani's algorithm is capable of breaking SIKE compared to the classic van Oorschot-Wiener algorithm. The golden collision problem finds a unique collision among the outputs of pseudo random functions generalizing the meets-in-the-middle problem. It has been used to analyze NIST PQC candidate SIKE. This quantum circuit has a linear cost for random access, defeating Grover or classical van Oorschot-Wienercollision finding algorithms that are exponential. Jaques et al. [85] demonstrate new algorithms for golden collision in quantum circuit models. Although showing a security degradation in SIKE, more importantly was the demonstration of achieving the same trade off between gate count T and quantum memory R. This also showed that quantum RAM is not necessary when using less than $N^{(2/7)}$ memory.

Peng [86] constructed the first identity-based signature scheme on isogenies, named CsiiBS, with proof for Unforgeability against chosen-message attacks (UF-CMA) security in a random oracle model. This was created by optimizing the group action evaluation method and parameter selection constraints. Further research is needed to construct higher performance schemes or increased security properties. Galbraith et al. [87] proposes two signature schemes based on supersingular isogeny problems. Both identification schemes are built using the Fiat-Shamir transform. The first scheme is built from the De Feo-Jao-Plut identification protocol with proposed optimization parameters and the second introduces a new randomization method for isogeny path, coming from the quaternion isogeny algorithm of Kohel et al. [88].

Jao et al. [89] proposed three zero-value power analysis attacks on SIDH that threaten the security of these schemes. The security weakness is due to forcing zero conditions of large-degree isogenies, which allows an adversary to determine all nearby curves. This adversary can then create a set of isogenies the sender is using, and then test them. The countermeasure proposed here is to randomize the resulting isogenous curves. The first fault attack on supersingular isogenies signature schemes was proposed by Ti [90]. The attack changes base points into a random point during the auxiliary point computation, which reveals the secret isogeny with one successful perturbation. This attack utilizes the Kirkwood et al. [91] validation method. It was noted that the scheme would not work well against key-exchange protocols.

Fault injection attacks present a vulnerability to SIDH key exchanges [92]. By injecting a fault, a sender will compute a partial isogeny that leaks information about the secret key. This is the first attack on isogeny-based schemes that bypasses the Kirkwood et al. validation method. Some countermeasures were proposed to check after each loop if the value counter is equal to the number of iterations. The countermeasure can be strengthened by adding additional parallel counters and routinely validating their values. This would protect against single faults. Isogeny based cryptography is still a new field, although there have been few successfully implemented secure algorithms, this should still be considered as a research opportunity. Fig. 3 shows a roadmap of the current isogeny-based cryptography including the alternate candidate SIKE of NIST PQC standardization.

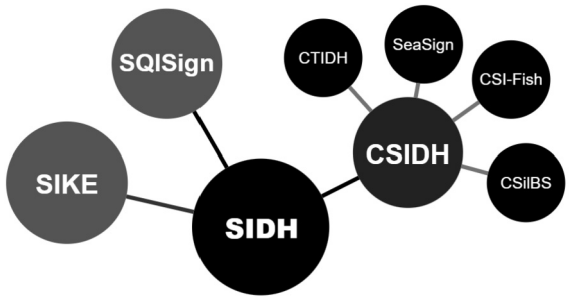

Fig. 3. Roadmap of the Isogeny-Based Cryptography.

3.4. Lattice-based PQC

Lattices are defined as all possible weighted sums of a set of base vectors when scaled by integers in the n-dimensional Euclidean space. More precisely, a lattice in $\mathbb{R}^n$, generated by the base vector set $B = b_1, b_2, ..., b_n$, is defined as $L(B) = \{\sum x_i b_i | x_i \in \mathbb{Z}^n\}$. Lattices can be constructed using a number of lattice-based schemes most common of which are Learning With Error (LWE) and Learning With Rounding (LWR). LWR involves finding a vector, a.k.a., secret vector s, given a matrix A and vector $b = As + e$. Other construction methods are the NTRU assumption and the Short Integer Solution (SIS).

The standard lattice scheme is mostly used for encryption and it requires computations with large matrices, which needs a significant amount of memory. A subgroup of lattices, named **ideal lattice**, was first introduced by Lyubashevsky and Micciancio in [94] as a generalization of cyclic lattices. This subgroup is considered to be more efficient than the standard lattices by its special matrix generation with a cyclic shift of the first matrix row, which is a representation of a full standard lattice matrix.

NTRU, one of the first lattice-based cryptosystems, was first introduced in 1998 by Hoffstein et al. [17]. Even though this design is now considered broken, there have been many variations that have been proven to be secure and quantum safe. NTRU Prime, the round three finalists for the NIST PQC standardization, is one of the variants. It is an ideal lattice and it is based on the algebraic structures of polynomial rings. Its hardness relies on the shortest vector problem in a lattice using the Ring-LWE problem. Easttom et al. [95] overview three different security features of NTRU. They suggest that by using a larger N size, NTRU was deemed secure against Lower Dimension Lattice (LDL) attacks and a substantial level of randomness in the cipher text. Zheng [96] used a first order collision attack on NTRU exposed its vulnerability to side-channel attacks even with proposed countermeasures from previous research [23]. It is then proposed that more secure countermeasures, resilient to collision attack, would be to introduce a combination of dummy operations and mathematical randomization, which was shown to be effective. FrodoKEN [97] is an alternate candidate that has made it to the third round of the NIST PQC standardization. FrodoKEN is a lattice-based key encapsulation mechanism that is defined as a tuple of algorithms (KeyGen, Encaps, Decaps). FrodoKEN's security relies on the hardness of LWE.

Primas et al. [98] performed the first single-trace attack on lattice-based encryption that can be used to attack masked implementations. The attack targets the Number Theoretic Transform (NTT), commonly used in lattice-based cryptosystems. The attack is described in three steps. First is to obtain a profiling of power traces during the inverse computation of NTT during decryption and match the recorded templates at each modular operation. This forms a probability vector for each operation. The second step is to combine all of step one's information over the entire NTT using a Belief Propagation (BP) to create a factor-graph representation of the NTT and continuously run BP until convergence. Finally, the step three is to combine recovered intermediate with the public-key. This is done by creating linear equations in the intermediates and the decryption key and using them to decrease the rank of the lattice spanned by the public-key. Lattice-basis reduction and decoding discovers the decryption key. If all 192 intermediates recovered are correct, the probability for success is one hundred percent. This research exposes the vulnerability of lattice-based schemes to SPA. It is stated that masking is helpful against a DPA.

Some additional countermeasures are proposed by [98] guaranteeing a constant run-time and control flow. The key recovery can be prevented by shuffling and random insertion of dummy operations. The research also considers Oder et al. [99] proposing countermeasures to briefly discuss their flaws with this SPA attack while adding additional methods to those countermeasures. Ravi et al. [100] demonstrate a chosen ciphertext attack (CCA) over lattice-based Public-Key Encryption (PKE) and Key Encapsulation Mechanism (KEM) in the chosen ciphertext model, i.e., IND-CCA security. Targeting the side-channel vulnerability in the error correcting codes allows an adversary to differentiate the value/validity of decrypted codewords. The study performs experimental validation of the attack on an ARM Cortext-M4F micro controller. This attack performed key-recovery in minutes, marking it a very quick attack. Further research into side-channel resistant error correcting codes is urged. Table 5 summarizes attacks and countermeasures for NTRU.

Ravi et al. [103] show a vulnerability in the message decoding of lattice-based PKE and KEM. The message decoding function leaks information of single bits of decrypted message $m\prime$ when error correcting code is used and decrypted code word $c\prime$ when error correcting code is not used. The vulnerability has the potential to be exploited through side-channel attacks and fault attacks. Sim et al. [101] expand upon single-trace attacks against lattice-based encryption. They evaluate

Table 5
NTRU: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
NTRU	First-order power analysis [96]	Power traces were gathered during decryption operations using five thousand different ciphertexts and a fixed unknown secret key. Correlation coefficients related to the key can be found.	Use of dummy operations, timing noise, and mathematical randomization.
	Single-trace attack (SPA) [98]	Masking is not sufficient enough against SPA. Exposes the vulnerability of NTT leakage. This attack can be applied to any lattice based scheme that uses NTT.	Ensure a constant run time and control flow. Shuffling can be used to protect against SPA. Dummy operations can increase resistance to SPA.
	Simple side-channel analysis [99]	Here a new implementation of CPA-secured ring-LWE encryption is proposed. A CCA2-transform was applied to ring-LWE. Optimization parameters were proposed to increase performance.	This new implementation used masked decoding to create a side-channel resistant ring-LWE encryption scheme.
	Side-channel assisted chosen ciphertext attack [100]	A generic EM side-channel chosen cipher text attack exposed vulnerabilities with error correcting procedure and in FO transformations that leak information about the output.	An efficient masking scheme that has yet to be invented would be desirable. Masking FO transformations that doesn't become too costly should be an area of research to be done.
	Single-trace side-channel attack [101]	The attack targets the message encoding operation in the encapsulation phase. The attack was able to recover the entire secret message for CRYSTALS-KYBER and SABER one hundred percent of the time. It is noted that this attack is applicable to NTRU.	Shuffling and masking should help to increase the complexity of the attack.
	Fault analysis [102]	A successful fault attack against NTRU public key digital signature algorithm. This attack assumes an adversary is able to inject a transient fault in a small number of coefficients in the polynomials in the signing algorithm.The attacker can calculate the difference between the faulty signature and correct one thus obtaining the secret key.	To detect temporal permanent faults and disable the device output. A redundancy based fault detection technique which detects transient and permanent faults is discussed. Another technique is proposed to defend against second order fault analysis.

three types of single-trace attacks on CRYSTALS-KYBER, SABER, and FrodoKEM: a clustering-based attack utilizing a determiner, an attack that targets algorithms that are used to scan one sensitive bit at a time during encoding, and lastly an attack that targets algorithms that scan multiple sensitive bits during encoding. Regardless of optimization level, the attacks were completely successful experimentally for CRYSTALS-KYBER and SABER. This paper suggests these attacks could extend to NTRU, Streamlined NTRU Prime, NTRU Prime. As previously stated, the proposed countermeasures here are a combination of shuffling and masking.

CRYSTAL-KYBER is considered to be one of the most promising encryption schemes in round three of NIST PQC standardization. This scheme is based on the hardness of Module Learning With Errors (MLWE). The MLWE is a new problem with little known attacks successful against it. It was shown to be of level CCA security in Quantum Random Oracle Model (QROM) [104]. Recently Ravi et al. [105] weakened CRYSTAL-KYBER security by using a fault attack that removed the hardness of the LWE problem and showed that with enough observed signatures with the same public-private key pair, a successful key recovery on Dilithium can take place. Pessl and Primas [106] expand upon [98] demonstrating an improved single-trace attack on an optimized constant-time CRYSTALS-KYBER by making improvements to the belief propagation. Although when masking is used, the advantage is lost. The paper briefly discusses the need for further investigation into better masking and binding techniques to protect lattice-based schemes such as KYBER against single-trace SPA. Table 6 summarizes attacks and countermeasures for CRYSTALS-KYBER.

SABER is a key encapsulation mechanism based on the hardness of module learning with rounding (MLWR), a variant of MLWE where error terms are substituted for rounding from one modulus to a second smaller modulus. Reductions to MLWR from MLWE exist, which the NIST has noted as a concern [108]. The rounding operation in SABER gives increased efficiency for modular reduction and polynomial multiplication steps. An advantage to SABER is, its readiness for general purpose applications. The NIST has no active suggestions for change to SABER but recommends further research into side-channel analysis and optimization of SABER. Van et al. [109] masked SABER to make it side-channel resistant. The masking only uses a 2.5x overhead factor. The SABER allows for simple masking conversion algorithms due to its power of two moduli and LWR as the hard problem. This masking technique utilizes constant-time implementation so a SPA technique would be difficult to implement. Van [109] suggests randomizing the order of execution of vulnerable routines in conjunction with masking could be resilient to DPA attacks. Table 7 summarizes attacks and countermeasures for SABER.

Bindel [110] tested lattice-based signature schemes, such as Bimodal Lattice Signature Scheme (BLISS), Ring-TESLA based on the Tightly-secure Efficient Signatures from standard LAttices (TESLA) and Guneysu-Lyubashevsky-Poppelmann (GLP), against fault attacks and proposed some countermeasures against them. One countermeasure against randomization fault attack is to check the correctness of the secret key. For skipping faults attacks, a new variable for saving the result-sum

Table 6
CRYSTALS-KYBER: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
CRYSTALS-KYBER	Single Trace Attack [106]	Builds upon [98] to successfully attack the Kyber scheme targeting the NTT for side-channel leakage.	Masking, Blinding, and Shuffling are recommended.
	Fault Analysis [105]	This fault attacks targets the nonce byte used in the Sample function. By inducing a fault to reuse the same seed the error component can be recovered. The fault attack was not successful in a direct key recovery but were able to reduce the hardness of LWR problems. Security of Kyber is weakened.	Use of separate seed for S and E. Synchronization of faults that are vulnerable to leaks. Further research on weakened Kyber.
	Fault Countermeasures [107]	Lattice based cryptography relies on hardness of LWE which utilizes error samplers making it an easy target for side-channel analysis on those computations.	Three countermeasures: Low cost counts the number of repetitions in the observation and alerts if the repetition exceeds an improbable value. Standard calculates the sample mean and sample variance simultaneously checking for repetitions. The expensive test includes the previous two while also performing a chi-squared test for comparing observed and expected values.
	Side-Channel, Fault Injection [103]	Vulnerabilities in message decoding procedures in lattice based KEM were explored. Side-channel and fault injection attacks were deployed on Kyber and SABER with a ninety nine percent success rate.	Random shuffling, less frequent updates and use of vectorized instructions were recommended.
	Single-trace side-channel attack [101]	The attack targets the message encoding operation in the encapsulation phase. The attack was able to recover the entire secret message for CRYSTALS-KYBER and SABER one hundred percent of the time. It is noted that this attack is applicable to NTRU.	Shuffling and masking should help to increase the complexity of the attack.

Table 7
SABER: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
SABER	Side-Channel Resistant to DPA [109]	A masked implementation of SABER is built with 2.5x overhead.	A new efficient masked primitive for SABER is proposed that allows masked logical shifting directly on arithmetic shares. This could replace the masked noise sampling which is more costly.
	Side-Channel, Fault Injection [103]	Vulnerabilities in message decoding procedures in lattice based KEM were explored. Side-channel and fault injection attacks were deployed on Kyber and SABER with a ninety nine percent success rate.	Random shuffling, less frequent updates and use of vectorized instructions were recommended.

was a successful countermeasure. A different approach is to add secret information to random information [110]. Zeroing is prevented by checking if the values of the secret, error polynomial, the randomness during signing, the hash value, or the encoding polynomial are zero. Espitau et al. [111] show the vulnerability to faults attacks of round two of the NIST lattice-based digital signature schemes. The proposed countermeasure here is similar to Bindel [110] by checking if the value of the random commitment element y_1 is not zero.

CRYptographic SuiTe for Algebraic Lattices (CRYSTAL)-Dilithium is a lattice-based signature scheme that relies on the hardness of MLWE and Module Short Integer Solution (MSIS) and follows the Fiat-Shamir with aborts technique [111]. The advantage to Dilithium is the compressed key size, which is the rounded LWE. Dilithium uses the same modulus and ring for all parameter sets via the uniform distribution that is a simpler implementation of FALCON. Kim et al. [112] is the first to propose a side-channel attack on Dilithium. A single-trace attack in NTT encryption during Dilithium signature generation process exposed a vulnerability in the NTT operation because the full key can be derived regardless of optimization level for each stage of NTT. Regardless of masking, the success rate on the NTT operation was 100%. Fournaris et al. [113] described how to efficiently mask Dilithium signature scheme based on a modification of the reference implementation of Dilithium by setting a power of two moduli instead of prime. This research also found leakages on decomposition functions and the rejection operation for a non-masked Dilithium implementation. Ravi et al. [114] was able to use a side-channel assisted forgery attack on Dilithium. This was done in two stages, where the partial secret-key s_i is recovered through a power analysis attack on the polynomial multiplier. A forgery signature scheme is then applied by only using s_i. It is only shown that Dilithium breaks with knowledge of the partial-secret key. Table 8 summarizes attacks and countermeasures for CRYSTALS-Dilithium.

Fast Fourier Lattice-based Compact Signatures over NTRU (FALCON) is the last lattice-based signature scheme that uses the hash-and-sign paradigm. The hardness is based on the Short Integer Solution (SIS) problem over NTRU lattices. FALCON

Table 8
CRYSTALS-Dilithium: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
CRYSTALS-Dilithium	Side-Channel Assisted Forgery Attack [114]	The attack takes two steps: 1) Recover the partial secret key $\bar{s}_1$ through power analysis attack on polynomial multiplier. 2) Forge signatures with only knowing $\bar{s}_1$.	This reduction in Dilithium signature calls for better methods of protecting the secret key from SCA.
	Single-trace attack [112]	This targeted the NTT encryption during Dilithium signature generation. This attack is applicable to schemes that use NTT. Masking was not sufficient enough to stop this attack.	New countermeasures need to be researched on implementing Dilithium with side-channel resistance.
	Correlational Power Attack [113]	This attack targets the polynomial multiplication operation during digital signature generation. Experimental validation of power trace capturing and profiling was successful.	
	Fault Countermeasures [107]	Lattice based cryptography relies on hardness of LWE which utilizes error samplers making it an easy target for side-channel analysis on those computations.	Three countermeasures: Low cost counts the number of repetitions in the observation and alerts if the repetition exceeds an improbable value. Standard calculates the sample mean and sample variance simultaneously checking for repetitions. The expensive test includes the previous two while also performing a chi-squared test for comparing observed and expected values.
	Fault Analysis [105]	This fault attacks targets the nonce byte used in the Sample function. By inducing a fault to reuse the same seed the error component can be recovered. If The rounding error on LWE instance t can be derived through observation of lots of signatures then an adversary can make a full key recovery. This shows the reduced hardness of the LWE problem due to the induced fault.	Use of separate seed for S and E. Synchronization of faults that are vulnerable to leaks. Further research on weakened Dilithium.

Table 9
FALCON: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
FALCON	Side-Channel Analysis [115]	The Gram-Schmidt norms of the secrete basis leaks information to SCA. Recovering the Gram-Schmidt norms leads to a full secret key recovery.	The countermeasures to prevent this leak are already implemented in [116], which includes masking FALCON.

requires tree data structures, extensive floating-point operations, and random sampling from several discrete Gaussian distributions [108]. The advantage to FALCON is the small bandwidth, and efficiency of signing and verifying. The disadvantage is the long key generation. Fouque et al. [115] discuss side-channel leakage of FALCON. The leakage only provides an estimate of the Gram-Schmidt norms. In order for a fully key recovery there needs to be a sufficient recovery algorithm. FALCON leakage arises from the approximate values but no efficient method in the full key recovery exists which calls for further research. Table 9 summarizes attacks and countermeasures for FALCON. The NIST has suggested for the Dilithium team to add a category 5 parameter set. It is expected that either Dilithium or FALCON will be standardized as a PQC signature scheme.

It is worth mentioning that the lattice-based encryption is still a new area of research and there should be further investigation into the proposed countermeasures against SPA and DPA attacks. Fig. 4 shows a roadmap of the current lattice-based cryptography. It is differentiated by the different hard problems such as SVP, LWE, and LWR). The dark circles are candidates that have been dropped, the gray is for alternate candidates, and the lightened circles are for finalists.

3.5. Multivariate-based PQC

Security of the multivariate quadratic public-key cryptosystems relies on the hardness of solving a large system of multivariate quadratic equations. This problem is also referred to as the MQ-problem. The public-key function is a set of polynomial functions. The MQ problem has been proven to be NP-hard even for quadratic polynomials over the finite field GF(2). The general security requirement for this scheme is that the private-key is difficult to be obtained from the public-key. The advantage of the multivariate cryptosystems is the generation of short signatures and fast verification.

A Great Multivariate Signature Scheme (GeMSS) [117] is one of the alternate candidates that made it to the third round of the NIST PQC standardization. GeMSS is a signature scheme algorithm with a fast verification process with the expense of having a large public-key. GeMSS was developed using the QUARTZ algorithm.

Hashimoto et al. [118] describes a fault attack on Multivariate Public-Key Cryptosystems (MPKC). The paper discusses the security of MPKC against fault attacks and shows the reduction in complexity of finding the secret key S and T by inducing faults on the central map G, or faults on the random values r. Although [119] shows that no known attacks can

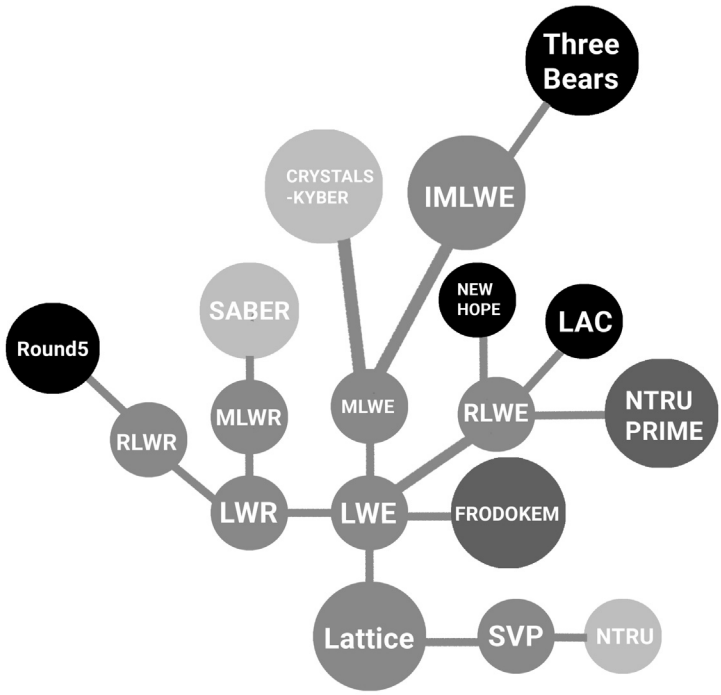

Fig. 4. Roadmap of the Lattice-Based Cryptography.

Table 10
Rainbow: Summary of Attacks and Countermeasures.

	Attack	Description	Countermeasures
Rainbow	Correlation Power Analysis [121]	Recovered the full secret key using a CPA on a 8-bit AVR micro controller. Then used a hybrid attack to recover S and used an Algebraic Key Recovery (AKR) to find T. UOV multivariate schemes are susceptible to this attack when using equivalent key $\tilde{T}\prime$.	To use random affine maps T instead of equivalent key. A combination of masking, hiding, shuffling, and dummy operations are suggested to help prevent SCA.
	Fault Attack [119]	Targets signature schemes based on [118].	Multivariate signature schemes are resistant to fault attacks.

lead to complete key recovery. It has been shown that distinguishing a key from multivariate leakage samples and multiple models can be done in a single step [120]. This paper derives closed-form expression of optimal distinguishers in terms of matrix operations in models that can either be profiled offline or regressed online. Park et al. [121] experimentally validate a correlation power analysis on RAINBOW that recovers the full secret key. This is done by identifying the secret leakage of the secret affine maps S and T during matrix-vector products in signing when RAINBOW is implemented with equivalent keys. The equivalent keys led to the entire secret affine map T. To recover the full secret key, S is discovered during the SPA, then T is recovered by a mounting algebraic key recovery attacks [121]. This team demonstrated the leakage experimentally on an 8-bit AVR microcontroller. This attack can be applied to multivariate signature schemes that are multi-layered. Recently, a power attack using the Least-SQuare (LSQ) technique was performed by observing power traces of the registers that hold the monomials and polynomials of the multivariate system with which an adversary can predict the secret keys. The least-square power analysis is described in full here targeting QUAD, which relies on the iteration of a randomly chosen multivariate quadratic system [122]. Table 10 summarizes attacks and countermeasures for Rainbow. Fig. 5 shows a roadmap of the multivariate PQC of round three of NIST.

4. Concluding remarks

Recent advancements in hardware technology related to quantum computers have raised serious concerns in the security and cryptography communities. While quantum computers most likely will not be available any time in the near future, it's necessary to create an alternative cryptographic landscape, known as post-quantum cryptography, before this hardware revolution becomes a reality. In response to this urgency, National Institute of Standards and Technology is currently leading the PQC standardization and has so far defined third round candidate algorithms.

We therefore provided a comprehensive review of attacks and countermeasures in PQC to portray a roadmap of this standardization efforts. Since there has been a rise in the side-channel attacks against PQC schemes, we mainly focused

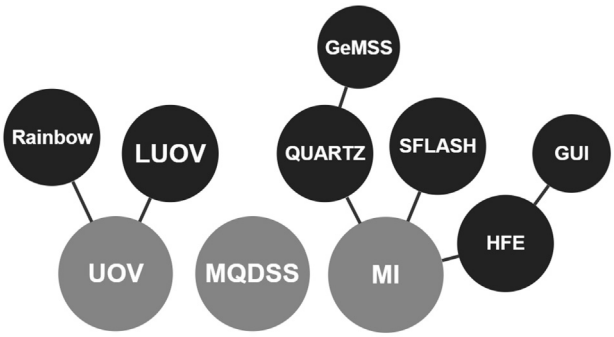

Fig. 5. Roadmap of the Multivariate Cryptography.

on the side-channel attacks and countermeasures in the final NIST candidates. We also explored some key concepts of the attacks and their countermeasures with the aim of assisting researchers who are conducting research in this emerging field.

The latest developments in various areas of PQC illustrate that it's necessary to further scrutinize the security of PQC protocols against all kinds of attacks including the side-channel attack in order to come up with guaranteed countermeasure solutions. It may take several years, if not one or two decades, until the PQC community accomplishes this challenging mission. Solutions such as SIKE was assumed to be secure for years and it could get to the NIST 4th-round of standardization, but surprisingly, it was recently compromised by a very strong and novel attack [14]. This development is a great example that highlights how difficult it is to finalize the whole process of the PQC standardization. Being open to all critiques and novel ideas in addition to collective efforts in the PQC community are the best strategies to pursue in order to successfully accomplish this standardization mission.

Declaration of competing interest

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

Data availability

No data was used for the research described in the article.

Acknowledgment

We thank the anonymous reviewers for their constructive feedback. This research was sponsored by the National Science Foundation and was accomplished under Grant Number CNS-1801341.

References

[1] P.W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE, 1994, pp. 124–134.
[2] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) (1999) 303–332.
[3] M. Mosca, Cybersecurity in an era with quantum computers: will we be ready?, Cryptology ePrint Archive, Report 2015/1075 https://eprint.iacr.org/2015/1075, 2015.
[4] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone, Report on post-quantum cryptography, National Institute of Standards and Technology, US Department of Commerce.
[5] B. Schneier, NSA plans for a post-quantum world, Schneier on Security.
[6] R.J. McEliece, A public-key cryptosystem based on algebraic, Coding Theory 4244 (1978) 114–116.
[7] H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory, Probl. Control Inf. Theory 15 (2) (1986) 159–166.
[8] P.C. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, in: Annual International Cryptology Conference, Springer, 1996, pp. 104–113.
[9] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Annual International Cryptology Conference, Springer, 1999, pp. 388–397.
[10] R.C. Merkle, A certified digital signature, in: Conference on the Theory and Application of Cryptology, Springer, 1989, pp. 218–238.
[11] A. Rostovtsev, A. Stolbunov, Public-key cryptosystem based on isogenies, IACR Cryptol. ePrint Arch. 2006 (2006) 145.
[12] A. Childs, D. Jao, V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, J. Math. Cryptol. 8 (1) (2014) 1–29.
[13] D. Jao, L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, in: International Workshop on Post-Quantum Cryptography, Springer, 2011, pp. 19–34.
[14] W. Castryck, T. Decru, An efficient key recovery attack on SIDH, Cryptology ePrint Archive, Paper 2022/975, https://eprint.iacr.org/2022/975, 2022.
[15] M. Ajtai, Generating hard instances of lattice problems, in: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 1996, pp. 99–108.
[16] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/average-case equivalence, in: Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, 1997, pp. 284–293.

[17] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: a ring-based public key cryptosystem, in: International Algorithmic Number Theory Symposium, Springer, 1998, pp. 267–288.
[18] T. Matsumoto, H. Imai, Public quadratic polynomial-tuples for efficient signature-verification and message-encryption, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1988, pp. 419–453.
[19] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1999, pp. 206–222.
[20] J. Patarin, The oil and vinegar signature scheme, in: Dagstuhl Workshop on Cryptography, September, 1997, 1997.
[21] C. Clavier, B. Feix, G. Gagnerot, M. Roussellet, V. Verneuil, Horizontal correlation analysis on exponentiation, in: International Conference on Information and Communications Security, Springer, 2010, pp. 46–61.
[22] A. Bauer, É. Jaulmes, E. Prouff, J. Wild, Horizontal and vertical side-channel attacks against secure RSA implementations, in: Cryptographers' Track at the RSA Conference, Springer, 2013, pp. 1–17.
[23] M.-K. Lee, J.E. Song, D. Choi, D.-G. Han, Countermeasures against power analysis attacks for the NTRU public key cryptosystem, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 93 (1) (2010) 153–163.
[24] E. Berlekamp, R. McEliece, H. Van Tilborg, On the inherent intractability of certain coding problems (corresp.), IEEE Trans. Inf. Theory 24 (3) (1978) 384–386.
[25] R. Avanzi, S. Hoerder, D. Page, M. Tunstall, Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems, J. Cryptogr. Eng. 1 (4) (2011) 271–281.
[26] C. Hall, I. Goldberg, B. Schneier, Reaction attacks against several public-key cryptosystem, in: International Conference on Information and Communications Security, Springer, 1999, pp. 2–12.
[27] C. Monico, J. Rosenthal, A. Shokrollahi, Using low density parity check codes in the McEliece cryptosystem, in: 2000 IEEE International Symposium on Information Theory (Cat. No. 00CH37060), IEEE, 2000, p. 215.
[28] M. Baldi, M. Bodrato, F. Chiaraluce, A new analysis of the McEliece cryptosystem based on QC-LDPC codes, in: International Conference on Security and Cryptography for Networks, Springer, 2008, pp. 246–262.
[29] R. Misoczki, J.-P. Tillich, N. Sendrier, P.S. Barreto, MDPC-McEliece: new McEliece variants from moderate density parity-check codes, in: 2013 IEEE International Symposium on Information Theory, IEEE, 2013, pp. 2069–2073.
[30] P.-L. Cayrel, P. Dusart, McEliece/Niederreiter PKC: sensitivity to fault injection, in: 2010 5th International Conference on Future Information Technology, IEEE, 2010, pp. 1–6.
[31] T. Chou, QcBits: constant-time small-key code-based cryptography, in: International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2016, pp. 280–300.
[32] M. Rossi, M. Hamburg, M. Hutter, M.E. Marson, A side-channel assisted cryptanalytic attack against QcBits, in: International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2017, pp. 3–23.
[33] P. Santini, M. Baldi, G. Cancellieri, F. Chiaraluce, Hindering reaction attacks by using monomial codes in the McEliece cryptosystem, in: 2018 IEEE International Symposium on Information Theory (ISIT), IEEE, 2018, pp. 951–955.
[34] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C.A. Melchor, et al., BIKE: Bit Flipping Key Encapsulation, 2017.
[35] A.H. Reinders, R. Misoczki, S. Ghosh, M.R. Sastry, Efficient BIKE hardware design with constant-time decoder, IACR Cryptol. ePrint Arch. 2020 (2020) 117.
[36] Z. Liu, Y. Pan, T. Xie, Breaking the hardness assumption and IND-CPA security of HQC submitted to NIST PQC project, IET Inf. Secur. 14 (3) (2019) 313–320.
[37] G. Wafo-Tapa, S. Bettaieb, L. Bidoux, P. Gaborit, E. Marcatel, A practicable timing attack against HQC and its countermeasure, IACR Cryptol. ePrint Arch. 2019 (2019) 909.
[38] H.G. Molter, M. Stöttinger, A. Shoufan, F. Strenzke, A simple power analysis attack on a McEliece cryptoprocessor, J. Cryptogr. Eng. 1 (1) (2011) 29–36.
[39] F. Strenzke, E. Tews, H.G. Molter, R. Overbeck, A. Shoufan, Side channels in the McEliece PKC, in: International Workshop on Post-Quantum Cryptography, Springer, 2008, pp. 216–229.
[40] T. Richmond, M. Petrvalsky, M. Drutarovsky, A side-channel attack against the secret permutation on an embedded McEliece cryptosystem, in: 3rd Workshop on Trustworthy Manufacturing and Utilization of Secure Devices-TRUDEVICE, 2015.
[41] M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel, V. Fischer, Countermeasure against the SPA attack on an embedded McEliece cryptosystem, in: 2015 25th International Conference Radioelektronika (RADIOELEKTRONIKA), IEEE, 2015, pp. 462–466.
[42] C. Chen, T. Eisenbarth, I. Von Maurich, R. Steinwandt, Differential power analysis of a McEliece cryptosystem, in: International Conference on Applied Cryptography and Network Security, Springer, 2015, pp. 538–556.
[43] C. Chen, T. Eisenbarth, I. von Maurich, R. Steinwandt, Horizontal and vertical side channel analysis of a McEliece cryptosystem, IEEE Trans. Inf. Forensics Secur. 11 (6) (2015) 1093–1105.
[44] S. Heyse, I. Von Maurich, T. Güneysu, Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices, in: Cryptographic Hardware and Embedded Systems-CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings 15, Springer, 2013, pp. 273–292.
[45] M. Petrvalsky, T. Richmond, M. Drutarovsky, P.-L. Cayrel, V. Fischer, Differential power analysis attack on the secure bit permutation in the McEliece cryptosystem, in: 2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA), IEEE, 2016, pp. 132–137.
[46] A. Couvreur, A. Otmani, J.-P. Tillich, Polynomial time attack on wild McEliece over quadratic extensions, IEEE Trans. Inf. Theory 63 (1) (2016) 404–427.
[47] D.J. Bernstein, T. Lange, C. Peters, Attacking and defending the McEliece cryptosystem, in: International Workshop on Post-Quantum Cryptography, Springer, 2008, pp. 31–46.
[48] D.J. Bernstein, List decoding for binary Goppa codes, in: International Conference on Coding and Cryptology, Springer, 2011, pp. 62–80.
[49] S. Tillich, C. Herbst, Attacking state-of-the-art software countermeasures—a case study for AES, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2008, pp. 228–243.
[50] N. Veyrat-Charvillon, M. Medwed, S. Kerckhof, F.-X. Standaert, Shuffling against side-channel attacks: a comprehensive study with cautionary note, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2012, pp. 740–757.
[51] P. Farkaš, Two countermeasures against reaction attacks on LEDApkc and other QC-MDPC and QC-LDPC based McEliece cryptosystems in ARQ setting heuristic discussion, in: 2018 26th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE, 2018, pp. 1–5.
[52] P.-J. Chen, T. Chou, S. Deshpande, N. Lahr, R. Niederhagen, J. Szefer, W. Wang, Complete and improved FPGA implementation of classic McEliece, Cryptology ePrint Archive.
[53] J. Richter-Brockmann, J. Mono, T. Güneysu, Folding BIKE: scalable hardware implementation for reconfigurable devices, IEEE Trans. Comput. 71 (5) (2021) 1204–1215.
[54] W. Wang, J. Szefer, R. Niederhagen, FPGA-based Niederreiter cryptosystem using binary Goppa codes, in: Post-Quantum Cryptography: 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings 9, Springer, 2018, pp. 77–98.
[55] J. Hu, R.C. Cheung, Area-time efficient computation of Niederreiter encryption on QC-MDPC codes for embedded hardware, IEEE Trans. Comput. 66 (8) (2017) 1313–1325.

[56] S. Heyse, T. Güneysu, Towards one cycle per bit asymmetric encryption: code-based cryptography on reconfigurable hardware, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2012, pp. 340–355.
[57] S. Ghosh, I. Verbauwhede, Blake-512-based 128-bit CCA2 secure timing attack resistant McEliece cryptoprocessor, IEEE Trans. Comput. 63 (5) (2012) 1124–1133.
[58] A. Shoufan, F. Strenzke, H.G. Molter, M. Stöttinger, A timing attack against Patterson algorithm in the McEliece PKC, in: International Conference on Information Security and Cryptology, Springer, 2009, pp. 161–175.
[59] F. Strenzke, A timing attack against the secret permutation in the McEliece PKC, in: International Workshop on Post-Quantum Cryptography, Springer, 2010, pp. 95–107.
[60] S. Heyse, A. Moradi, C. Paar, Practical power analysis attacks on software implementations of McEliece, in: International Workshop on Post-Quantum Cryptography, Springer, 2010, pp. 108–125.
[61] Q. Guo, T. Johansson, P. Stankovski, A key recovery attack on MDPC with CCA security using decoding errors, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2016, pp. 789–815.
[62] E. Eaton, M. Lequesne, A. Parent, N. Sendrier, QC-MDPC: a timing attack and a CCA2 KEM, in: International Conference on Post-Quantum Cryptography, Springer, 2018, pp. 47–76.
[63] B.-Y. Sim, J. Kwon, K.Y. Choi, J. Cho, A. Park, D.-G. Han, Novel side-channel attacks on quasi-cyclic code-based cryptography, IACR Trans. Cryptogr. Hardw. Embed. Syst. (2019) 180–212.
[64] Q. Guo, T. Johansson, P.S. Wagner, A key recovery reaction attack on QC-MDPC, IEEE Trans. Inf. Theory 65 (3) (2018) 1845–1861.
[65] D. McGrew, P. Kampanakis, S. Fluhrer, S.-L. Gazdag, D. Butin, J. Buchmann, State management for hash-based signatures, in: International Conference on Research in Security Standardisation, Springer, 2016, pp. 244–260.
[66] L. Lamport, Constructing digital signatures from a one-way function, Tech. Rep., Citeseer, 1979.
[67] A. Hülsing, W-OTS+–shorter signatures for hash-based signature schemes, in: International Conference on Cryptology in Africa, Springer, 2013, pp. 173–188.
[68] J. Buchmann, E. Dahmen, S. Ereth, A. Hülsing, M. Rückert, On the security of the Winternitz one-time signature scheme, in: International Conference on Cryptology in Africa, Springer, 2011, pp. 363–378.
[69] D.A. Cooper, D.C. Apon, Q.H. Dang, M.S. Davidson, M.J. Dworkin, C.A. Miller, Recommendation for stateful hash-based signature schemes, NASA Spec. Publ. 800 (2020) 208.
[70] S. Suhail, R. Hussain, A. Khan, C.S. Hong, On the role of hash-based signatures in quantum-safe Internet of things: current solutions and future directions, arXiv preprint, arXiv:2004.10435.
[71] D.J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, Z. Wilcox-O'Hearn, SPHINCS: practical stateless hash-based signatures, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2015, pp. 368–397.
[72] A. Sotirov, M. Stevens, J. Appelbaum, A.K. Lenstra, D. Molnar, D.A. Osvik, B. de Weger, MD5 considered harmful today, creating a rogue CA certificate, Tech. Rep., EPFL, 2008.
[73] A. Genêt, M.J. Kannwischer, H. Pelletier, A. McLauchlan, Practical fault injection attacks on SPHINCS, IACR Cryptol. ePrint Arch. 2018 (2018) 674.
[74] P. Wang, S. Tian, Z. Sun, N. Xie, Quantum algorithms for hash preimage attacks, Quantum Eng. 2 (2) (2020) e36.
[75] M.J. Kannwischer, A. Genêt, D. Butin, J. Krämer, J. Buchmann, Differential power analysis of XMSS and SPHINCS, in: International Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, 2018, pp. 168–188.
[76] M. Mozaffari-Kermani, R. Azarderakhsh, A. Aghaie, Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC, ACM Trans. Embed. Comput. Syst. 16 (2) (2016) 1–19.
[77] K. Ramezanpour, P. Ampadu, W. Diehl, SCAUL: power side-channel analysis with unsupervised learning, IEEE Trans. Comput. 69 (11) (2020) 1626–1638.
[78] L. Castelnovi, A. Martinelli, T. Prest, Grafting trees: a fault attack against the SPHINCS framework, in: International Conference on Post-Quantum Cryptography, Springer, 2018, pp. 165–184.
[79] B. Koziel, R. Azarderakhsh, M.M. Kermani, D. Jao, Post-quantum cryptography on FPGA based on isogenies on elliptic curves, IEEE Trans. Circuits Syst. I, Regul. Pap. 64 (1) (2016) 86–99.
[80] R. Azarderakhsh, M. Campagna, C. Costello, L. Feo, B. Hess, A. Jalali, D. Jao, B. Koziel, B. LaMacchia, P. Longa, et al., Supersingular isogeny key encapsulation. Submission to the NIST Post-Quantum Standardization project 152 (2017) 154–155.
[81] S. Jaques, J.M. Schanck, Quantum cryptanalysis in the RAM model: claw-finding attacks on SIKE, Cryptology ePrint Archive, Report 2019/103 https://eprint.iacr.org/2019/103, 2019.
[82] F. Zhang, B. Yang, X. Dong, S. Guilley, Z. Liu, W. He, F. Zhang, K. Ren, Side-channel analysis and countermeasure design on ARM-based quantum-resistant sike, IEEE Trans. Comput. 69 (11) (2020) 1681–1693.
[83] W. Castryck, T. Lange, C. Martindale, L. Panny, J. Renes, CSIDH: an efficient post-quantum commutative group action, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2018, pp. 395–427.
[84] G. Banegas, D.J. Bernstein, F. Campos, T. Chou, T. Lange, M. Meyer, B. Smith, J. Sotáková, CTIDH: Faster constant-time CSIDH, 2021.
[85] S. Jaques, A. Schrottenloher, Low-gate quantum golden collision finding, IACR Cryptol. ePrint Arch. 2020 (2020) 424.
[86] C. Peng, J. Chen, L. Zhou, K.-K.R. Choo, D. He, CsiIBS: a post-quantum identity-based signature scheme based on isogenies, J. Inf. Secur. Appl. 54 (2020) 102504.
[87] S.D. Galbraith, C. Petit, J. Silva, Identification protocols and signature schemes based on supersingular isogeny problems, J. Cryptol. 33 (1) (2020) 130–175.
[88] D. Kohel, K. Lauter, C. Petit, J.-P. Tignol, On the quaternion ℓ-isogeny path problem, LMS J. Comput. Math. 17 (A) (2014) 418–432.
[89] B. Koziel, R. Azarderakhsh, D. Jao, Side-channel attacks on quantum-resistant supersingular isogeny Diffie-Hellman, in: International Conference on Selected Areas in Cryptography, Springer, 2017, pp. 64–81.
[90] Y.B. Ti, Fault attack on supersingular isogeny cryptosystems, in: International Workshop on Post-Quantum Cryptography, Springer, 2017, pp. 107–122.
[91] D. Kirkwood, B.C. Lackey, J. McVey, M. Motley, J.A. Solinas, D. Tuller, Failure is not an option: standardization issues for post-quantum key agreement, in: Workshop on Cybersecurity in a Post-Quantum World, 2015, p. 21.
[92] A. Gélin, B. Wesolowski, Loop-abort faults on supersingular isogeny cryptosystems, in: International Workshop on Post-Quantum Cryptography, Springer, 2017, pp. 93–106.
[93] N.P. Smart, An analysis of Goubin's refined power analysis attack, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2003, pp. 281–290.
[94] V. Lyubashevsky, D. Micciancio, Generalized compact knapsacks are collision resistant, in: International Colloquium on Automata, Languages, and Programming, Springer, 2006, pp. 144–155.
[95] C. Easttom, A. Ibrahim, C. Chefronov, I. Alsmadi, R. Hanson, Towards a deeper NTRU analysis: a multi modal analysis, Int. J. Cryptogr. Inf. Secur. 10 (2) (2020) 11–22.
[96] X. Zheng, A. Wang, W. Wei, First-order collision attack on protected NTRU cryptosystem, Microprocess. Microsyst. 37 (6–7) (2013) 601–609.

[97] E. Alkim, J.W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, v. Nikolaenko, C. Peikert, a. Raghunathan, D. Stebila, et al. FrodoKEM learning with errors key encapsulation, Retrieved October 6 (2019) 2020.
[98] R. Primas, P. Pessl, S. Mangard, Single-trace side-channel attacks on masked lattice-based encryption, in: International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2017, pp. 513–533.
[99] T. Oder, T. Schneider, T. Pöppelmann, T. Güneysu, Practical CCA2-secure and masked ring-LWE implementation, IACR Trans. Cryptogr. Hardw. Embed. Syst. (2018) 142–174.
[100] P. Ravi, S.S. Roy, A. Chattopadhyay, S. Bhasin, Generic side-channel attacks on CCA-secure lattice-based PKE and KEM schemes, IACR Cryptol. ePrint Arch. 2019 (2019) 948.
[101] B.-Y. Sim, J. Kwon, J. Lee, I.-J. Kim, T.-H. Lee, J. Han, H. Yoon, J. Cho, D.-G. Han, Single-trace attacks on message encoding in lattice-based KEMs, IEEE Access 8 (2020) 183175–183191.
[102] A.A. Kamal, A.M. Youssef, Fault analysis of the NTRUSign digital signature scheme, Cryptogr. Commun. 4 (2) (2012) 131–144.
[103] P. Ravi, S. Bhasin, S.S. Roy, A. Chattopadhyay, Drop by drop you break the rock-exploiting generic vulnerabilities in lattice-based PKE/KEMs using EM-based physical attacks, IACR Cryptol. ePrint Arch. 2020 (2020) 549.
[104] D. Hofheinz, K. Hövelmanns, E. Kiltz, A modular analysis of the Fujisaki-Okamoto transformation, in: Theory of Cryptography Conference, Springer, 2017, pp. 341–371.
[105] P. Ravi, D.B. Roy, S. Bhasin, A. Chattopadhyay, D. Mukhopadhyay, Number “not used” once-practical fault attack on pqm4 implementations of NIST candidates, in: International Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, 2019, pp. 232–250.
[106] P. Pessl, R. Primas, More practical single-trace attacks on the number theoretic transform, in: International Conference on Cryptology and Information Security in Latin America, Springer, 2019, pp. 130–149.
[107] J. Howe, A. Khalid, M. Martinoli, F. Regazzoni, E. Oswald, Fault attack countermeasures for error samplers in lattice-based cryptography, in: 2019 IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, 2019, pp. 1–5.
[108] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, et al., Status report on the second round of the NIST post-quantum cryptography standardization process, US Department of Commerce, National Institute of Standards and Technology.
[109] M. Van Beirendonck, J.-P. D'Anvers, A. Karmakar, J. Balasch, I. Verbauwhede, A side-channel resistant implementation of SABER, IACR Cryptol. ePrint Arch. 733 (2020) 2020.
[110] N. Bindel, J. Buchmann, J. Krämer, Lattice-based signature schemes and their sensitivity to fault attacks, in: 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), IEEE, 2016, pp. 63–77.
[111] T. Espitau, P.-A. Fouque, B. Gérard, M. Tibouchi, Loop-abort faults on lattice-based [F]iat-[S]hamir and hash-and-sign signatures, in: International Conference on Selected Areas in Cryptography, Springer, 2016, pp. 140–158.
[112] I.-J. Kim, T.-H. Lee, J. Han, B.-Y. Sim, D.-G. Han, Novel single-trace ML profiling attacks on NIST 3 round candidate Dilithium, IACR Cryptol. ePrint Arch.
[113] A.P. Fournaris, C. Dimopoulos, O. Koufopavlou, Profiling Dilithium digital signature traces for correlation differential side channel attacks, in: International Conference on Embedded Computer Systems, Springer, 2020, pp. 281–294.
[114] P. Ravi, M.P. Jhanwar, J. Howe, A. Chattopadhyay, S. Bhasin, Side-channel assisted existential forgery attack on Dilithium-a NIST PQC candidate, IACR Cryptol. ePrint Arch. 2018 (2018) 821.
[115] P.-A. Fouque, P. Kirchner, M. Tibouchi, A. Wallet, Y. Yu, Uprooting the Falcon tree?, IACR Cryptol. ePrint Arch. 2019 (2019) 1180.
[116] T. Prest, T. Ricosset, M. Rossi, Simple, fast and constant-time Gaussian sampling over the integers for Falcon, 2019.
[117] A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, J. Ryckeghem, GeMSS: a great multivariate short signature, Ph.D. thesis, UPMC-Paris 6 Sorbonne Universités; INRIA Paris Research Centre, MAMBA Team …, 2017.
[118] Y. Hashimoto, T. Takagi, K. Sakurai, General fault attacks on multivariate public key cryptosystems, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 96 (1) (2013) 196–205.
[119] J. Krämer, M. Loiero, Fault attacks on UOV and rainbow, in: International Workshop on Constructive Side-Channel Analysis and Secure Design, Springer, 2019, pp. 193–214.
[120] N. Bruneau, S. Guilley, A. Heuser, D. Marion, O. Rioul, Optimal side-channel attacks for multivariate leakages and multiple models, J. Cryptogr. Eng. 7 (4) (2017) 331–341.
[121] A. Park, K.-A. Shim, N. Koo, D.-G. Han, Side-channel attacks on post-quantum signature schemes based on multivariate quadratic equations, IACR Trans. Cryptogr. Hardw. Embed. Syst. (2018) 500–523.
[122] W. Li, X. Huang, H. Zhao, G. Xie, F. Lu, Fuzzy matching template attacks on multivariate cryptography: a case study, Discrete Dyn. Nat. Soc. (2020).