A Survey on Post-Quantum Public-Key Signature Schemes for Secure Vehicular Communications

Kyung-Ah Shim, *Member, IEEE*

***Abstract*— Basic security requirements such as confidentiality, user authentication and data integrity, are assured by using public-key cryptography (PKC). In particular, public-key signature schemes provide non-repudiation, integrity of transmitted messages and authentication. The presence of a large scale quantum computer would be a real threat to break the most widely used public-key cryptographic algorithms in practice, RSA, DSA, ECDSA signature schemes and Diffie-Hellman key exchange. Thus, all security protocols and applications where these public-key cryptographic algorithms are used are vulnerable to quantum-computer attacks. There are five directions of cryptographic primitives secure against a quantum computer: multivariate quadratic equation-based, hash-based, lattice-based, code-based and supersingular isogeny-based cryptography. These primitives could serve as replacements for current public-key cryptographic algorithms to prepare for post-quantum era. It is important to prioritize the fields to be replaced by post-quantum cryptography (PQC) since it is hard to replace the currently deployed PKC with PQC at the same time. The fields directly connected to human life such as vehicular communications should be the primary targets of PQC applications. This survey is dedicated to providing guidelines for adapting the most suitable post-quantum candidates to the requirements of various devices and suggesting efficient and physically secure implementations that can be built into existing embedded applications as easily as traditional PKC. It focuses on the five types of post-quantum signature schemes and investigates their theoretical backgrounds, structures, state-of-the-art constructions and implementation aspects on various platforms raging from resource constrained IoT devices to powerful servers connected to the devices for secure communications in post-quantum era. It offers appropriate solutions to find tradeoffs between key sizes, signature lengths, performance, and security for practical applications.**

***Index Terms*— Implementation attack, post-quantum cryptography, public-key signature scheme, quantum algorithm, Shor algorithm, side-channel attack.**

I. Introduction

INTERNET of things (IoT) is an emerging technological paradigm connecting millions of smart objects for advanced services. This innovative paradigm makes the smart objects capable of hearing, seeing, thinking and performing jobs by sharing information and coordinating decisions. Enabling of IoT is accomplished through efforts by network and hardware industry and the enormous amount of data generated through IoT big data and data mining fields. With its wide ranging applications in home automation, healthcare, industrial control and environmental and social domains, IoT can have wide ranging expectations. IoT leads to the evolution of Vehicle Ad hoc Networks (VANET) into Internet of Vehicles (IoV). According to Gartner [1], 20.4 billion of things will be connected to Internet by 2020 among which vehicles will account for a significant portion and the business IoT endpoint spending will reach almost $3 trillion. VANET and IoV have different the concept of vehicles. While a vehicle is considered as a node to disseminate messages among vehicles in VANET, each vehicle is a smart object equipped with a powerful multi-sensor platform, computation units, communications technologies, IP-based connectivity to Internet and to other vehicles either directly or indirectly. A vehicle in IoV enables the interactions between intra-vehicle components, vehicles and road, vehicles and vehicles, and vehicles and people and the acquisition and processing of large amount of data from various geographical areas through intelligent vehicles computing platforms to offer various categories of services for road safety and other services to drivers and passengers. One of major obstacles to the deployment and prevalent use of IoT and IoV is privacy-security vulnerabilities. Security and privacy issues for IoT are targets of great importance.

A. Public-Key Cryptography

Since its invention in the late 1970s, public-key cryptography (PKC) is fundamental buildingblock for secure communications in cyber security. E-commerce, online banking, cloud computing and mobile communication depend on the security of the underlying cryptographic algorithms. Basic security requirements, confidentiality, user authentication, data integrity and non-repudiation are assured by using appropriate public-key and symmetric-key cryptographic algorithms. PKC such as digital signatures and key exchange plays a crucial role in establishing secure communications without requiring pre-key distribution unlike symmetric-key cryptography in many practical applications. In particular, public-key signature schemes provide non-repudiation, integrity of transmitted messages and authentication. Millions of web servers use public-key certificates and digital signatures as part of the Transport Layer Security (TLS) to allow users to verify the identity of the server. Millions of merchant payment terminals verify the digital signatures from EMV (Europay, Mastercard, and Visa) payment cards to ascertain that the cards were not cloned. Phone manufacturers rely on digital signatures to protect the integrity of the operating system software and

Manuscript received 27 July 2020; revised 4 July 2021 and 7 October 2021; accepted 17 November 2021. Date of publication 10 December 2021; date of current version 12 September 2022. This work was supported by the National Institute for Mathematical Sciences funded by the Ministry of Science and Information and Communication Technologies (ICT), South Korea, under Grant B21720000. The Associate Editor for this article was S. Olariu.

The author is with the Division of Basic Researches for Industrial Mathematics, National Institute for Mathematical Sciences, Daejeon 34047, Republic of Korea (e-mail: kashim@nims.re.kr).

Digital Object Identifier 10.1109/TITS.2021.3131668

applications running on the millions of mobile phones. The integrity of billion apps that had been downloaded from its App Store is guaranteed by digital signatures. This survey focuses on public-key signature schemes secure against a quantum computer.

B. Impact of a Quantum Computer on PKC

In 1996, Shor [2] presented a polynomial-time quantum algorithm for solving the (elliptic curve) discrete logarithm problem ((EC)DLP) in finite fields or on elliptic curves and the integer factorization problem (IFP). Security of the public-key cryptographic algorithm, RSA, DSA or ECDSA, currently in use depends on the hardness of integer factorization problem, the discrete-logarithm problem in finite fields or on elliptic curves. All these public-key cryptographic algorithms are expected to be broken easily by an adequate quantum computer. Thus, there is a growing demand for investigating their alternatives, so-called post-quantum cryptography (PQC). The definition of PQC is public-key cryptography that resists attacks using classical and quantum computers. Currently deployed international standard PKC (RSA, DSA, ECDSA, Diffie-Hellman key exchange) should be replaced with PQC in all applications where the traditional PKC are used before a quantum computer is developed.

The impact of a quantum computer on PKC will be dramatic: most public-key cryptographic algorithms currently in use are expected to be broken easily by a quantum computer. Thus, all applications where public-key cryptographic algorithms are used are vulnerable to quantum-computer attacks: communication protocols, authentication protocols verifying the authenticity via digital certificate provided through a public-key infrastructure (PKI), various internet standards (TLS, S/MIME, PGP, and GPG). Embedded systems in vehicles require connected technologies that rely on PKC to secure data and authenticate communications. The increasing connectivity of cars via mobile networks enables a lot of new services and interactivity between car and end-user. Due to the comparable long lifetime of cars in the field, in the automotive industry, the impact of quantum computers could be greater. In fact, long-term security is an important issue in PQC. There are applications, for instance, energy infrastructure, where products' lifetime of 15-30 years is common. Security systems in these application that are not merely secure for today but that should be remained secure long-term against attacks by quantum computers.

C. Related Works for PQC

NSA [3] updated their Suite B cryptographic algorithms emphasizing the need and importance of a transition to post-quantum algorithms. NIST [4] announced the standardization plan targeted for post-quantum public-key encryption, digital signature and key exchange. Other standardization bodies, NIST, ETSI and IETF have followed by developing cryptographic standards resistant to quantum computers. In particular, post-quantum cryptographic algorithms have also received increased attention from industry. A line of work starting with initial adaptations by Google with collaborations, has involved Internet companies running experiments to measure the performance of real connections using post-quantum key exchange (combined with the traditional elliptic curve Diffie–Hellman, so-called "hybrid" key exchange), by modifying client browsers and edge servers to support select the hybrid key exchange schemes in TLS 1.3. Google has integrated a post-quantum key exchange scheme, New Hope, into the development version of its web browser (Chrome Canary) and into some of its web servers (e.g. https://play.google.com/store) [5]. Also, Microsoft has presented a Supersingular Isogeny Diffie-Hellman key exchange (SIDH) scheme with a software library implementing its suite [6]. These initiatives show the feasibility of integration for post-quantum schemes into existing standards. There are works for post-quantum security for IoTs, Cyber-Physical Systems, 5G and vehicular communications (V2X) [7]–[10]. There have been investigated the suitability of post-quantum signature schemes on IoT constrained devices and networks: hash-based signature schemes [11]–[14] and lattice-based signature schemes and multivariate quadratic-based signature schemes [15], [16].

D. Transition From PKC to PQC and Transition Priority

System designers must already think about migration from traditional PKC to PQC. To migrate to PQC and information security systems secure against a quantum computer, a staged hybrid approach should be considered. The reasons are the need to address different use-case constraints, such as communicating among varying IoT devices, increasing security levels and ensuring backward compatibility. In the first phase, the classical PKC and PQC will be used in conjunction. These will include the classical PKC and most likely a few PQC. In the middle phase, PQC will be upgraded as needed and continue to work alongside the classical PKC. In the end phase, PKC will be superseded completely. Some experts estimate the necessary transition time for PQC standards to be 10 years [17], [18].

It is also important to prioritize the fields to be replaced by PQC since it is hard to replace the currently deployed PKC with PQC at the same time. It is expected that the transition will happen too quickly for some categories of product IT that are in the early phases of long life cycles, as is the case in the automotive and aerospace industries. Higher-value systems are usually transitioned first while less critical systems remain in place until the end of their life cycle. The fields directly connected to human life such as vehicular communications should be the primary targets of PQC applications. In fact, the traditional signature schemes and post-quantum signature schemes have the same functionalities, security services and applicability except for their resistance to a quantum computer. Thus, for the security of all security systems based on signature schemes in post-quantum era, post-quantum signature schemes can be replaced by the traditional signature schemes in all applications where they are used utilizing the same practical scenarios and methodologies. This paper can be used for guiding new security protocol designers and developers when selecting appropriate signature algorithms while

respecting requirements and design constraints to prepare for the post-quantum era.

E. Scope of This Survey and Contributions

Public-key cryptographic algorithms secure against both classical and quantum computers could serve as replacements for current public-key cryptographic algorithms to prepare for the post-quantum era when a general quantum computer is realized. Motivated by further advances in classical cryptanalysis and a quantum computer, it is important to investigate these potential alternatives to apply secure constructions and efficient implementations at hand when they are finally needed. There are five main directions of post-quantum cryptographic primitives secure against a quantum computer: multivariate quadratic equation-based, hash-based, lattice-based, code-based and supersingular isogeny-based cryptography. These cryptographic primitives believed to protect both classical and quantum attacks have considered as post-quantum replacements.

- This survey focuses on public-key signature schemes belong to the five types of PQ-cryptographic primitives and investigates their theoretic backgrounds, structures, implementation aspects and security results against implementation attacks, regarding the alternative public-key signature schemes for secure communication and protection in the post-quantum era.
- It is important to consider suitability of post-quantum schemes on embedded processors and devices, including low-cost microcontrollers and hardware devices (FPGA/ASIC). This survey evaluates the availability and suitability of five-types PQ-signature schemes on various platforms raging from resource constrained IoT constrained devices with 8-bit ATmega microcontrollers to powerful servers connected to the devices as well as their hardware implementations.
- It is a survey on the PQ-signature schemes for a broad spectrum of real-world applications. It offers appropriate solutions to find tradeoffs between performance, key sizes, signature lengths, and security for practical applications in the upcoming post-quantum era. This survey provides a guideline on the selection of the PQ-signature schemes adapting to the different requirements and challenges of components connected to IoT.

The paper is organized as follow. We summarize pre-quantum security level and post-quantum security level of widely deployed cryptographic systems affected by well-known quantum algorithms, Grover algorithm and Shor algorithm in Section II. Section III provides the state-of-the-art results of the five types PQ-signature schemes in terms of theoretical backgrounds, basic structures and implementation results on various platforms ranging from 8-bit resource constraint devices to powerful server as well as their hardware implementations. In Section IV, we investigate the latest results of implementation attacks such as side-channel attacks, fault attacks and cold boot attack for the PQ-signature schemes. In Section V, we provide comparisons between the PQ-signature schemes in terms of key sizes, signature sizes and performance, and discussions on future research issues. Section VI provides concluding remarks.

II. Quantum Algorithms and Quantum Attacks

Here, we describe well known quantum algorithms and quantum attacks. The most well-known quantum algorithms are Grover's algorithm [19] for searching in data and Shor's algorithm [2] for solving the integer factorization problem and the discrete logarithm problem. Post-quantum cryptography means public-key cryptographic algorithms which are believed to be secure against attacks by a quantum computer. Security of practically used public-key cryptographic algorithms relies on one of three mathematical hard problems: the DLP, the ECDLP or the IFP. A sufficiently large quantum computer capable of implementing Shor's algorithm can easily solve these problems in polynomial time. In contrast to the public-key cryptographic algorithms, symmetric cryptographic algorithms and hash functions can protect attacks by a quantum computer due to Grover's algorithm. Grover [19] proposed a quantum searching algorithm for an unordered database of size N using $\sqrt{N}$ quantum queries, i.e. it is quadratically faster than the best known classical searching algorithm for the same work. Thus, doubling the key size of the symmetric cryptographic algorithms including block ciphers and stream ciphers and hash functions can prevent the quantum attacks. We summarize classical security level (pre-quantum security level) and post-quantum security level of widely deployed cryptographic algorithms affected by two quantum algorithms, Grover's algorithm and Shor's algorithm from [20] in Table I.

Shor [2] proposed a polynomial-time quantum algorithm for solving the IFP and (EC)DLP. Hallgran [21] proposed a quantum algorithm for solving Pell's equation in polynomial time. The other polynomial-time quantum algorithms are related to the ideal class group and the principal ideal problem (PIP). These fundamental problems in number theory are related to many open conjectures in both analytic and algebraic number theory. Hallgren [22] presented a quantum algorithm for solving these problems for number fields of constant degree in polynomial time. Eisentrager *et al.* [23] proposed a quantum algorithm that computes the unit group in classes of number fields with arbitrary degree in polynomial time remaining the way to compute the ideal class group and principal ideal problem (PIP) in the general case. Recently, Biasse and Song [24] proposed polynomial-time quantum algorithms for solving the PIP and computing the ideal class group in classes of number fields with arbitrary degree under the Generalized Riemann Hypothesis. Their algorithms are also useful for the cryptanalysis of post-quantum cryptographic schemes based on ideal lattices [25], [26].

An efficient quantum attack on a public-key cryptosystem, Soliloquy, designed by Campbell-Groves-Shepherd in GCHQ was proposed [25]. This may be the first quantum attack on a lattice-based scheme. It also turned out that the attack can be applied to Smart-Vercauteren's fully homomorphic encryption scheme presented at PKC'10 [27], and Garg-Gentry-Halevi's multilinear map presented at Eurocrypt'13 [28]. However, this does not mean that current lattice-based cryptography in general is vulnerable to this type quantum attack. The attack used

TABLE I
CURRENT CRYPTOGRAPHIC ALGORITHM WIDELY USED IN PRACTICE

Cryptographic Algorithm	Scheme	Type	Pre-quantum Security Level	Post-quantum Security Level
Symmetric-Key Cryptographic Algorithm	AES-128	Block cipher	128	64 (Grover)
	AES-256	Block cipher	256	128 (Grover)
	Salsa20	Stream cipher	256	128 (Grover)
	GMAC	MAC	128	128 (No impact)
	Poly 1305	MAC	128	128 (No impact)
Hash Function	SHA-256	Hash function	256	128 (Grover)
	SHA-3	Hash function	256	128 (Grover)
Public-Key Cryptographic Algorithm	RSA-3072 [29]	Encryption	128	Broken (Shor)
	RSA-3072 [29]	Signature	128	Broken (Shor)
	DSA-3072 [29]	Signature	128	Broken (Shor)
	ECDSA-256	Signature	128	Broken (Shor)
	DH-3072 [29]	Key exchange	128	Broken (Shor)
	ECDH-256 [29]	Key exchange	128	Broken (Shor)

that Soliloquy is based on a special type of ideals that turned out to be weaker than general ideals. It is believed that it is hard to generalize to current ideal/lattice-based cryptography. Particularly, it does not work on the schemes that have the worst-case security proofs using the Ring-LWE or Ring-SIS problems The result on Soliloquy highlights the importance of worst-case hardness proofs introducing vulnerabilities on easy special cases of the hard problem and the use of structured lattices using cyclotomic polynomials for practical feasibility. Some construct lattice-based schemes using weaker ideals with more useful structures such as ring, module and NTRU ideals for key size reduction and efficiency than general standard ideals. Although the quantum attack is not easy to generalize, it may a warning about the use of such structured ideals for the construction of the lattice-based schemes.

III. POST-QUANTUM SIGNATURE SCHEMES

In this section, we investigate the security and practicality of the five types of PQ-signature schemes in terms of their theoretical backgrounds, structures and the state-of-the-art implementation results: multivariate quadratic equation (MQ)-based schemes, lattice-based schemes, hash-based schemes, code-based schemes and supersingular isogeny-based schemes.

A. Definition and Formal Security Models

We first escribe a definition and their formal security models of public-key signature schemes [31].

1) Public-Key Signature Schemes: A PKS scheme $\mathcal{PKS} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vfy})$ consists of the following three polynomial-time algorithms:

- KeyGen: Given a security parameter λ, a key generation algorithm outputs a secret/public key pair $(sk, pk) \leftarrow \mathsf{KeyGen}(1^{\lambda})$.
- Sign: Given a secret key sk and a message m, a signing algorithm outputs a signature $\sigma \leftarrow \mathsf{Sign}(sk, m)$.
- Vfy: Given a public key pk, a message m and a signature σ, a verification algorithm outputs 1 if the signature is valid, or 0 otherwise, where $\{0, 1\} \leftarrow \mathsf{Vfy}(pk, m, \sigma)$.

We describe the processes of general public-key signature schemes in Fig. 1.

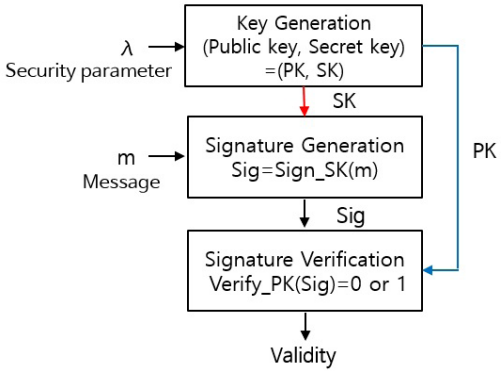

Fig. 1. The processes in public-key signature schemes.

2) Formal Security Model: Security of PKS schemes is defined by existential unforgeability against an adaptive chosen-message attack. In the following game between a challenger $\mathcal{C}$ and $\mathcal{A}$, an adversary $\mathcal{A}$'s advantage $Adv_{\mathcal{S},\mathcal{A}}$ is determined by the probability of success:

- **Setup.** $\mathcal{C}$ runs **Setup** and gives $\mathcal{A}$ the resulting system parameters.
- **Sign Queries.** Adaptively, when $\mathcal{A}$ requests a signature on a message m_i, $\mathcal{C}$ outputs a signature σ_i.
- **Output.** At last, $\mathcal{A}$ returns σ^* on a message m^* and wins the game if
  i) $\mathbf{Vfy}(pk, m^*, \sigma^*) = 1$,
  ii) m^* has never asked to the **Sign** oracle.

Security of the post-quantum signature schemes are defined by existential unforgeability against adaptive chosen-message attacks in the same security models as the traditional schemes. The post-quantum signature schemes introduced in the survey were proved their existential unforgeability against adaptive chosen-message attacks under the hardness assumptions of the underlying mathematical problems in the random oracle model or standard model.

Signature schemes can be divided into the following two paradigms as:

- **Hash-and-Sign Paradigm:** After hashing the message, find a solution of the hard problem related to the hashed message $H(\mu)$, for a message μ.

TABLE II
NOTATIONS

Notations	
$\mathbb{F}_q$	Finite field with elements q
λ	Pre-quantum (Classical) security parameter
λ_q	Post-quantum security parameter
pk, sk	Public key, secret key
kB, kb	Kilobytes, kilobits,
ms, μs	Microsecond, nanosecond
TPA	Timing attack protection
Ops/s	Operations per second
SK, PK	Secret key, public key
Sig.Size	Signature size
Comm. cost	Communication cost
Comp. cost.	Computational cost

- **Fiat-Shamir Paradigm:** Use the Fiat-Shamir transform [30] from a zero-knowledge identification protocol into a signature scheme.

As in the traditional signature schemes, the five type post-quantum signature schemes are designed using the above two design paradigms. In spite of using these same paradigms, due to the use of the different mathematical hard problems, the post-quantum signature schemes have differences in their performance properties, key lengths, signature lengths and performance.

B. Notations

For the sake of clarity, we explain notations used in this paper.

C. MQ-Based Signature Scheme

MQ-based signature schemes mainly rely on the intractability of solving large multivariate systems of quadratic equations. MQ-schemes require only modest computational resources without using multiple-precision arithmetic. So, it is fit for resource constrained devices such as RFID chips and smart cards [32], [33]. Advantages of MQ-schemes using some additional structures are fast performance and short signature size, but they suffer from relatively large key sizes.

1) Underlying Hard Problems of MQ-Schemes: The security of MQ-schemes is based on the following mathematical hard problems.

- **Multivariate Quadratic (MQ) Problem:** Given a system $\mathcal{P} = (P^{(1)}, \cdots, P^{(m)})$ of m nonlinear equations defined on $\mathbb{F}_q$ with degree of 2 in variables $(x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_m) \in \mathbb{F}_q^m$, find values $(x'_1, \cdots, x'_n) \in \mathbb{F}_q^n$ such that $P^{(1)}(x'_1, \cdots, x'_n) = y_1, \cdots, P^{(m)}(x'_1, \cdots, x'_n) = y_m$.
- **Extended Isomorphism of Polynomials (EIP) Problem:** Given a nonlinear multivariate system $\mathcal{P}$ such that $\mathcal{P} = S \circ \mathcal{F} \circ T$ for $\mathcal{F}$ in a special class of nonlinear polynomial system $\mathcal{SC}$ and affine or linear maps S and T, find $(S', \mathcal{F}', T')$ such that $\mathcal{P} = S' \circ \mathcal{F}' \circ T'$, where $\mathcal{F}' \in \mathcal{SC}$ and linear or affine maps S' and T'.
- **MinRank Problem:** Given $(M_1, \cdots, M_l) \in \mathbb{F}_q^{m \times n}$ for $k, m, n, r \in \mathbb{N}$ and $m, r < n$, find a non-zero k-tuple $(\lambda_1, \cdots, \lambda_k) \in \mathbb{F}_q^k$ such that $Rank(\sum_{i=1}^{k} \lambda_i M_i) \leq r$.

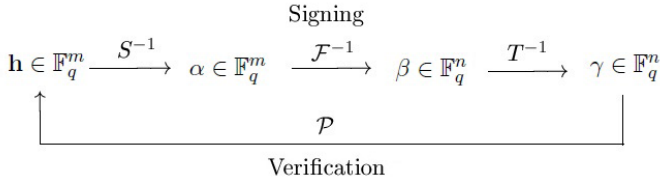

Fig. 2. Signing and verification processes in the MQ-signature schemes.

The MQ-problem is known to be NP-complete [34] even for the quadratic polynomials over $\mathbb{F}_2$. At Eurocrypt'96, Patarin [35] first described the IP problem, the IP problem is known to be harder than Graph-Isomorphism [36]. The MinRank problem that finds a linear combination with row rank of matrices originally introduced in [37] is known an NP-complete problem. An MQ-scheme with a single layer like UOV depends on the hardness of the MQ-problem and the IP problem. A multi-layered MQ-signature scheme like Rainbow additionally requires the hardness of the MinRank problem.

2) Structure of MQ-Schemes: MQ-PKC mainly relies on the intractability of the MQ-problem. It requires another structure, ASA (affine-substitution-affine) structure to hide a trapdoor in secret affine layers. The security of this structure is related to the EIP problem [35].

A main idea for the construction of MQ-schemes is to select an easily invertible system $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ (called a central map) of m multivariate quadratic equations with n variables. To destroy the special structure of the central map $\mathcal{F}$, it requires two invertible linear or affine maps $S : \mathbb{F}_q^m \to \mathbb{F}_q^m$ to mix the polynomials with different forms and $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ to mix variables. A public key is given by $\mathcal{P} = S \circ \mathcal{F} \circ T$ and is hard to invert since it is hardly distinguishable from a random system. A secret key $(S, \mathcal{F}, T)$ makes $\mathcal{P}$ easily invertible. This is called the ASA structure. In MQ-schemes with a single layer, S is an identity map, thus its secret key is $(\mathcal{F}, T)$. Then a public keys is a system $\mathcal{P} = (\mathcal{P}^{(1)}, \cdots, \mathcal{P}^{(m)})$ of m multivariate quadratic equations in n variables defined by

$$\mathcal{P}^{(k)}(x_1, \cdots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} p_{ij}^{(k)} x_i x_j + \sum_{i=1}^{n} p_i^{(k)} x_i + p_0^{(k)},$$

for $p_{ij}^{(k)}, p_i^{(k)}, p_0^{(k)} \in_R \mathbb{F}_q$ $(k = 1, \cdots, m)$. Signing and verification processes in the MQ-signature schemes are illustrated in Fig. 2.

MQ-schemes using the ASA structure are divided into the following two types:

- **Single-Field Case:** MQ-schemes using Oil-Vinegar polynomials such as Unbalanced Oil-and-Vinegar (UOV) and Rainbow.
- **Big(Mixed)-Field Case:** MQ-schemes using extension fields such as HFEv- variants [38], [39].

MQ-schemes [40], [41] obtained from Sakumoto *et al.*'s identification scheme [42] via the Fiat-Shamir transform [30], is based only on the MQ-problem, while the MQ-schemes using the ASA structure, HFEv- variants [38], [39] and Unbalanced Oil-and-Vinegar (UOV) variants [43], [44], is based

TABLE III
PERFORMANCE, SIGNATURE SIZES AND KEY SIZES OF MQ-SIGNATURE SCHEMES

λ	Scheme	Sig. Size (Bytes)	PK (Bytes)	SK (Bytes)	Sign (Cycles)	Verify (Cycles)	CPU
>128	MQDSS-31-64 [41]	40,952	72	64	8,510,616	5,752,616	Intel Core i7-4770K 3.5GHz
120	Gui-127 (127, 9, 4, 6) [39]	21	142,576	5,350	1,080,000	122,000	Intel Xeon E3-1245 3.4GHz
128	Rainbow ($\mathbb{F}_{2^8}, 36, 21, 22$) [29]	79	139,320	105,006	64,658	44,397	Intel Core i5-6600 3.3 GHz

TABLE IV
PERFORMANCE AND KEY SIZES OF MQ-SIGNATURE SCHEMES ON AN 8-bit MICROPROCESSOR [46]

λ	Scheme	Key Size [Byte] private	public	System private	Parameter public	Clockcyles x 1000 sign	verify	Time[ms]@32MHz sign	verify	Code Size [Byte] sign	verify
80	uov(28,37)	49728	60060	*	*	3,637	3,911	113.66	122.23	2188	466
	0/1 uov(28,37)	30044	11368	19684	48692	3,526	3,211	110.20	100.37	2258	578
	rainbow(18,13,14)	19682	27945	*	*	1,740	2,214	54.38	69.19	4162	466
	enTTS(9,36,52)	4591	49608	*	*	609	6,658	19.03	208.07	41232	827
128	uov(44,59)	194700	235664	*	*	13,314	14,134	416.07	441.70	2188	466
	0/1 uov(44,59)	116820	43560	77880	192104	12,782	13,569	399.43	424.04	2258	578
	rainbow(36,21,22)	97675	135880	*	*	8,227	9,216	257.11	288.01	4162	466
	enTTS(15,60,80)	13051	234960	*	*	2,142	30,789	66.94	962.17	116698	827

on the MQ-problem and the EIP problem or the MinRank problem.

3) Constructions and Implementation Results of MQ-Schemes: Since the first MQ-encryption scheme of Imai and Matsumoto [45] proposed, a number of MQ-schemes have been proposed. Most of the MQ-schemes have been broken except two types of MQ-signature schemes: variants HFEv- [38], [39] and Unbalanced Oil-and-Vinegar (UOV) [43], [44]. All the schemes have been constructed with actual parameters secure against known attacks, but they have no security reduction to the intractability of an random instance from the MQ-problem. Since they use the ASA structure related to the EIP problem, many schemes have been broken not by targeting the MQ-problem, but by targeting the EIP-problem.

The Fiat-Shamir type MQ-signature scheme, MQDSS, is the first provably secure MQ-signature scheme with a security reduction to the intractability of an random instance of the MQ-problem. Chen *et al.* [41] implemented MQDSS in [40]. Not relying on the EIP problem, MQDSS has short key sizes comparable to ECDSA, but sacrifice the most significant advantages of MQ-schemes, fast performance and short signature size.

At CHES 2012, Czypek *et al.* [46] presented practical feasibility of MQ-signature schemes on an 8-bit AVR microprocessor. Their target device is ATxMega128a1 with a clock frequency of 32 MHz, 8KB SRAM and 128KB flash program memory. We summarize performance, signature sizes and key sizes of MQ-based signatures schemes on 64-bit platforms and 8-bit platforms in Table III and IV, respectively. Details of the schemes in Table III and IV are as follows:

- Unbalanced Oil-and-Vinegar (UOV) [43]: Single-layer MQ-signature scheme.
- 0/1 UOV [47]: It is a shorter key size version of UOV.
- Rainbow [44]: Rainbow is a multi-layered version of UOV. In general, Rainbow means a two-layered Rainbow. In eBACS project [29], it contains the implementation result of Rainbow($\mathbb{F}_{31}$,26,20,20) at the higher security level than 80 bits, but it achieves about 94 or 95-bit security level. So, we provide our implementation result of Rainbow on Intel Core i5-6600, 3.3 GHz by choosing ($\mathbb{F}_{2^8}$, 36, 21, 22) as a parameter set of the 128-bit security level.
- enTTS [48], [46]: It is Rainbow with three layers using sparse polynomials.
- Gui [39]: It is a mixed field type MQ-scheme based on HFEv- using HFE polynomials with low degrees in $\{5, 9, 17\}$. We introduce their implementation result of Gui-127(127, 9, 4, 6) at a 120-bit security level in [39].

Bogdanov *et al.* [32] presented hardware implementation records of MQ-signature schemes, UOV, Rainbow, enTTS and amTTS. They showed that the MQ-schemes provided a much better time-area product than ECC: an optimized implementation of enTTS on FPGA is about 40 times faster than that of ECC with the given parameter in Table V. We summarize their hardware implementation records of the MQ-schemes in Table V, where F, T, L, S, FF and A represent frequency, time, luts, slices, flip-flops and area, respectively. At PQCrypto 2011, Tang *et al.* [49] provided hardware implementation of Rainbow programmed in VHDL on EP2S130F1020I4 FPGA device, a member of ALTERA Stratix II family. Table VI shows that Rainbow takes only 198 clock cycles for a signature generation, so it takes 3960 ms for signing with the frequency of 50 MHz. Note that their implementation is focused on speeding up the signing process. The size is about 150,000 GEs in terms of area, where GE stands for the gate equivalent.

D. Lattice-Based Signature Schemes

Advantages of lattice-based schemes are worst-case hardness of their underlying lattice problems and diverse functionalities. Their worst-case hardness comes from two

TABLE V
HARDWARE IMPLEMENTATION RECORDS OF MQ-SIGNATURE SCHEMES AND ECC ON FPGA [32]

λ	Scheme	CPU	F, MHz	μs	L/S/FF	A,kGE	L×T
80	ECC over GF(2^{163}) [50], NIST	XC2V200	100	41	8,300 /– /–	–	71.3
80	ECC over GF(2^{163}) [51], NIST	XCV200E-7	48	68.9	25,763 /– /–	–	372.3
64	UOV n = 60, m = 20	XC5VLX50-3	209	11	15,497/4,188/4,999	166.6	35.7
64	UOV n = 60, m = 20	XC3S1500	83	27.7	21,167/9,203/6,828	227.5	122.8
64	Rainbow n = 42, m = 24	XC5VLX50-3	105	30.3	5,929/1,681/1,869	63.7	37.6
64	Rainbow n = 42, m = 24	XC3S1500	79	39.1	7,114/1,968/2,377	76.4	58.2
	enTTS n = 24, m = 20	XC5VLX50-3	207	1.1	4,341/1,284/1,537	44.2	1.0
	enTTS n = 24, m = 20	XC3S1500	80	2.8	5,423/1,248/1,986	55.9	3.2

TABLE VI
PERFORMANCE OF RAINBOW ON FPGA [49]

λ	Scheme	Sign (Cycles)
80	Rainbow($\mathbb{F}_{2^8}, 17, 12, 17$)	198

major average-case problems: the SIS problem from Ajtai's breakthrough work at STOC'96 [52] and the LWE problem introduced by Regev at STOC'05 [53] and related to the Ajtai-Dwork cryptosystem [54]. These average-case problems are provably as intractable as solving the GapSVP problem (the decisional version of the shortest vector problem) and the SIVP (finding short linearly independent lattice vectors) problem in the worst case. Also, they provide new trendy functionalities such as multilinear maps and fully-homomorphic encryption schemes.

1) Underlying Hard Problems of Lattice-Based Schemes:

- **Shortest Vector Problem (SVP):** For any parameter $\gamma = \gamma(n) \geq 1$, γ-SVP, is the search problem, given a basis B for a lattice $\mathcal{L} \subset \mathbb{R}^n$, find a lattice vector x with $0 \leq \|x\| \leq \gamma \cdot \lambda_1(\mathcal{L})$, where $\lambda_1(\mathcal{L}) = min_{x \in \mathcal{L} \setminus \{0\}} \|x\|$ for the length of the shortest non-zero vector in the lattice.
- **GapSVP:** For any parameter $\gamma = \gamma(n) \geq 1$, a basis B of a lattice $\mathcal{L} \subset \mathbb{R}^n$ and a number $d > 0$, output yes if $\lambda_1(\mathcal{L}) < d$ and $\lambda_1(\mathcal{L}) < \gamma \cdot d$.
- **Small Integer Solution (SIS) Problem:** For a random matrix $A \in_R \mathbb{Z}_q^{n \times m}$ and a number $\beta > 0$, find a vector $v \in \mathbb{Z} \setminus \{0\}$ such that $Av = 0$ and $\| v \| \leq \beta$.
- **Computational Learning with Errors (LWE) Problem:** Let $n, q \in \mathbb{N}$ and let χ and ϕ be distributions on $\mathbb{Z}$. A LWE distribution for a given vector $s \in \mathbb{Z}_q^n$ is the set of pairs $(a, a \cdot s + e \pmod q)$, where $a \in \mathbb{Z}_q^n$ is uniformly sampled and e is sampled from ϕ. For a vector $s \leftarrow \chi^n$ and arbitrarily many samples from the LWE distribution for s, find s.
- **Decisional Learning with Errors (LWE) Problem:** Given arbitrarily many samples from $\mathbb{Z}_q^{n+1}$, distinguish whether the samples are uniformly distributed or whether they are distributed as the LWE distribution for a fixed vector $s \leftarrow \chi^n$.
- **Ring-LWE Problem:** Two polynomials a and s are uniformly chosen from a polynomial ring $R_q = \mathbb{Z}_q[x]/(f)$, where f is an irreducible polynomial of degree $n-1$. The remainder of this problem is the same as that of LWE except for the replacement with the polynomial ring R_q.

2) Constructions and Implementation Results of Lattice-Based Schemes: Since the construction of the NTRU Encryption scheme was introduced in [55], the use of algebraic lattices [56] can boost many lattice-based constructions. Although an efficient lattice-based encryption scheme, NTRUEncrypt, was proposed, lattice-based signature schemes have been problematic. For lattice-based signature schemes, the GGH scheme [57] was attempted earlier, but it was completely broken [59]. The NTRU signature scheme introduced in 2001 [58] was also broken by Nguyen and Regev [59]. Their lattice trapdoors leak some secret information. In 2008, to prevent such leakage, Gentry, Peikert, and Vaikuntanathan [60] proposed a hash-and-sign scheme provably secure under the hardness of worst-case lattice problems.

At Eurocrypt 2012, Lyubashevsky [61] constructed a signature scheme using the LWE problem and the SIS problem with a security reduction to the worst-case problems in general lattices. Its signing algorithm requires sampling from discrete Gaussians. At CHES 2012, Güneysu *et al.* [62] proposed a compression technique without requiring sampling from Gaussians with security reductions to the DCK and the Ring-SIS assumptions, but its full security analysis is not provides in their paper. Bai and Galbraith [63] introduced an improved compression technique for signature schemes using learning with errors (LWE). Their signatures are shorter than any previous provably-secure schemes using the standard lattice problems. At Crypto 2013 [64], Ducas *et al.* proposed a new lattice-based signature, BLISS, based on a modified rejection sampling algorithm from Lyubashevsky's signature scheme [61]. Their rejection sampling from a bimodal Gaussian distribution with a modified instantiation reduced to asymptotically square root complexity in the security parameter. We summarize performance, signature lengths and key sizes of BLISS at each security level in Table VII from [64].

In [65], Peikert showed that the security parameters of most practical lattice-based schemes were not instantiated following to their given security reductions. The reason is that they don't have tight security reductions, i.e. the relation between the intractability of the underlying assumption and their security are not proven to be linear. To provide a certain target security level, the parameter of a signature scheme without a tight security reduction must be chosen much larger to compensate for its loose reduction. Alkim *et al.* [66] proposed a new lattice-based signature scheme, TESLA, tightly related to the intractability assumption of the Ring-LWE problem.

TABLE VII
PERFORMANCE, SIGNATURE SIZES AND KEY SIZES OF BLISS [64]

λ	Scheme	Sig. Size	PK	SK	Sign	Verify
128	BLISS-I	5.6 kb	7 kb	2 kb	0.124 ms	0.030 ms
128	BLISS-II	5 kb	7 kb	2 kb	0.480 ms	0.030 ms
192	BLISS-III	6 kb	7 kb	3 kb	0.124 ms	0.031 ms
256	BLISS-IV	6.5 kb	7 kb	3 kb	0.124 ms	0.032 ms

TABLE VIII
PERFORMANCE, SIGNATURE SIZES AND KEY SIZES OF LATTICE-BASED SIGNATURE SCHEMES

λ	Scheme	Sig. Size (Bytes)	PK (Bytes)	SK (Bytes)	Sign (Cycles)	Verify (Cycles)	CPU
128	BG [63]	1,495	1,619,940	912,308	1,203,924	335,072	Intel Core i7-4770K(Haswell)
128	TESLA-416^t [66]	1,280	1,331,200	1,011,744	697,940	250,264	Intel Core i7-4770K(Haswell)
> 128	TESLA-768^t [66]	2,336	4,227,072	3,293,216	2,232,906	863,790	Intel Core i7-4770K(Haswell)
128	ring-TESLA-II^t [67]	1,568	3,328	1,920	510,981	167,791	Intel Core 3.4 GHz
125	Dilithium [68]	2,701	1,472	3,504	789,000	209,000	Intel Core i7-4770K (Haswell)

TABLE IX
PERFORMANCE OF BLISS-BI ON 8-bit AVR [69]

λ	Scheme	Sign (Cycles)	Verify (Cycles)	CPU
128	BLISS-BI	10,537,981	2,814,118	AX 128

In [67], the authors presented the first lattice-based signature scheme, ring-TESLA-II, with good performance when provably secure instantiated. They claimed that BLISS does not provide provably secure instantiation and good performance simultaneously. Recently, Ducas *et al.* [68] proposed a signature scheme, Dilithium, based on the 'Fiat-Shamir with Aborts' approach avoiding discrete Gaussian sampling. These lattice-based schemes are the Fiat-Shamir type signature schemes, but their differences are determined depending on the selection of the class of lattices underlying hard problems such as standard, module, ring, NTRU and distributions for key generation and signing such as uniform, Gaussian, bimodal Gaussian and hybrid.

Table VIII provides performance, signature sizes and key sizes of two lattice-based schemes, TESLA and ring-TESLA-II from [66], [67], respectively. Pöppelmann *et al.* [69] implemented BLISS-BI on 8-bit AVR: ATxmega128A1 clocked with 32 MHz, 128kB Flash, 8kB SRAM (AX 128), where BLISS-BI represent BLISS with a 128-bit security level. Their result is given in Table IX. Poppelmann *et al.* [70] provided a scalable implementation for signing and verification of BLISS on Xilinx Spartan-6 FPGA supporting either 128-bit (BLISS-I), 192-bit (BLISS-III), or 256-bit (BLISS-IV) security. To improve the performance, they integrated Huffman compression of signatures, parallel sparse multiplication, fast FFT/NTT-based polynomial multiplication and Keccak as hash function. The performance results of BLISS on FPGA at each security level are summarized in Table X and XI.

E. Hash-Based Signature Schemes

A cryptographic hash function is used to construct every signature scheme to compress message being signed. Has-based signature (HBS) schemes which use only hash functions are based on the properties of the used hash function such as collision resistance and second pre-image resistance. An advantage of HBS schemes is that the security proofs of some generalized HBS schemes against classical adversaries are still valid for quantum adversaries [71], but, for other types of PQ-signature schemes, it is not yet known.

1) Underlying Hard Problems of Hash-Based Schemes: HBS schemes using a hash function H are based on the following hard problems:

- **Collision resistance (CR):** Find any two values x and x' such that $H(x) = H(x')$.
- **Second pre-image resistance (SPR):** Given x, find a second preimage x' such that $H(x) = H(x')$.

If one can find a second pre-image of a hash function then one can find its collision. Its converse does not work. Thus, the SPR problem is harder than the CR problem.

2) Structure of Hash-Based Schemes: HBS schemes can be divided into two classes: stateful and stateless.

- **Stateful:** In signing, after generating a signature on a message, it generates an updated secret key not to use the key that has already been used.
- **Stateless:** It is a standard signature scheme without requiring the secret key update.

HBS schemes are built on one-time signature schemes or few-time signature schemes. HBS signature schemes can only sign a fixed number of messages securely since they are built on one-time signature schemes. In Merkle signature scheme (MSS) and extended MSS scheme (XMSS), a maximum of 2^h messages can be signed securely, where h is a height of the Merkle hash tree.

3) Constructions and Implementation Results of Hash-Based Schemes: We first introduce stateful hash-based signature schemes which require the secret key update for each signing due to the use of one-time signatures. Lamport [72] proposed a one-time HBS scheme in 1979. Merkle [73] proposed a Merkle signature scheme (MSS) based on the Merkle hash tree and one-time signatures such as the Lamport signature scheme. The security of MSS relies on the collision resistance of the hash function. Some variants of MSS were proposed: CMSS [74], GMSS [75],

TABLE X
PERFORMANCE OF BLISS ON XILINX SPARTAN-6 FPGA [70]

λ	Scheme	Sign (Cycles)	Verify (Cycles)	MHz	Ops/s
128	BLISS-I	15,864	9,607	140	8,825
192	BLISS-III	27,547	9,628	133	4,828
256	BLISS-IV	47,528	9,658	135	2840

TABLE XI
PERFORMANCE OF BLISS ON FPGA [70]

λ	Scheme	Sign (Ops/s)	Verify (Ops/s)	Device
128	BLISS-BI	8,761	17,101	XC6SLX25

TABLE XII
PERFORMANCE OF XMSS WITH SHA2-256 [82]

λ	Scheme	H	w	KeyGen (ms)	Sign (ms)	Verify (ms)	CPU
128	XMSS	20	4	382,903	3.26	0.20	Intel Core i7 3.5GHz
128	XMSS	20	16	762,132	6.56	0.36	Intel Core i7 3.5GHz
128	XMSS	20	64	2,038,605	17.51	1.00	Intel Core i7 3.5GHz

TABLE XIII
PERFORMANCE OF XMSS WITH SHA2-256 [82]

λ	Scheme	H	w	KeyGen (ms)	Sign (ms)	Verify (ms)
128	XMSS using Single buffer	20	4	191,982	1.81	0.11
		20	8	214,820	2.04	0.12
		20	16	282,582	2.71	0.14
		20	32	438,249	4.24	0.19
		20	64	693,187	5.95	0.35
128	XMSS using Multiple buffer	20	4	80,323	0.71	0.07
		20	8	81,130	0.82	0.10
		20	16	89,121	0.94	0.12
		20	32	123,588	1.35	0.18
		20	64	187,192	2.04	0.34

XMSS [76] and XMSS^{MT} [77]. CMSS [74] with two chained trees reduces the computational cost of key/signature generations allowing the signatures of 2^{40} documents. CMSS reduces the secret key size using a pseudo-random number generator. GMSS [75] reduces the signature generation cost and the signature length allowing a significantly large number of documents to be signed by one key pair. XMSS is an extended MSS scheme using the one-time signature scheme, WOTS+ [78], and a single-tree. It is proven existentially unforgeability of WOTS+ under adaptively chosen-message attacks instantiated with a family of pseudo-random functions. Later, XMSS^{MT} [77] (XMSS with a multi-tree) was proposed for allowing signatures of a large fixed number of documents. XMSS^{MT} [77] reduces the memory consumption and computational cost for key/signature generations and increase the number of signatures, but slightly the increase of the key sizes. XMSS and XMSS^{MT} require the second pre-image resistance of a hash function which induces the weaker assumption and smaller signature sizes. XMSS and XMSS^{MT} allow signing of up to 2^{20} and 2^{60} messages with one key pair, respectively. The stateful hash-based schemes, XMSS and XMSS^{MT}, developed through the Internet Engineering Task Force (IETF) are specified in RFC 8391 [79] and Leighton-Micali HBS scheme (LMS) based on the original Lamport-Diffie-Winternitz-Merkle one-time signature scheme [73] is specified in RFC 8554 [80]. Practical improvements have been proposed in [81] that alleviate the concerns of the stateful schemes.

Table XII, XIII and XIV show performance of MSS variants using AVX2 instructions on a Haswell i7-4770 at 3.4 GHz [82]. The implementations written in C language were compiled with GNU C Compiler v4.9.0. In the tables, H, d and w are the total height of the tree, the number of layers and Winternitz parameter, respectively. The performance of XMSS with WOTS+ using a single-buffer of SHA2 with 64-bit vector registers and a multi-buffer of SHA2 with 256-bit vector registers are given in Table XIII. A comparison of performance between GMSS and XMSS^{MT} with the selection of the parameters for 128-bit quantum security (λ_q) is given in Table XIV. In Table XII, XIII and XIV, the runtimes for signing and verification are measured by the average of one million signatures. At PKC 2016, Hülsing *et al.* [83] proposed XMSS-T which is XMSS with a tight security reduction. XMSS-T is originated from multi-target notions of hash-functions. In contrast to XMSS, XMSS-T is secure against the multi-target attacks. A comparison of performance between XMSS and XMSS-T is given in Table XV. Haswell processors. The results of SPHINCS-256 using AVX2 vector on single

TABLE XIV
PERFORMANCE, KEY SIZES AND SIGNATURE SIZES OF HASH-BASED SIGNATURE SCHEMES [82]

λ_q	Scheme	H	(d, w)	PK (Bytes)	SK (Bytes)	Sig. Size (Bytes)	KeyGen (ms)	Sign (ms)	Verify (ms)
128	GMSS _SHA2-384 _m48_n48	20	(1, 2)	100	32	6980	183,623	1.64	0.13
		20	(2, 2)	300	32	13,320	358	1.06	0.26
		20	(1, 4)	100	32	3844	240,368	2.25	0.26
		20	(2, 4)	300	32	7048	471	1.5	0.52
		40	(4, 4)	700	32	14,096	940	1.5	1.02
		60	(6, 4)	1,100	32	21,144	1,411	1.5	1.54
128	XMSS^{MT} _SHA2-256 _m32_n32	20	(1, 4)	1,956	1,920	4,932	80,323	0.71	0.07
		20	(2, 4)	1,036	1,280	9,228	156	0.47	0.14
		20	(1, 16)	2,276	2,240	2,820	89,121	0.94	0.12
		20	(2, 16)	1,772	1,600	5,004	174	0.59	0.52
		40	(4, 16)	2,044	1,600	10102	347	0.58	0.52
		60	(6, 16)	2,316	1,600	15,020	523	0.59	0.75

TABLE XV
PERFORMANCE, KEY SIZES AND SIGNATURE SIZES OF XMSS AND XMSS-T [83]

λ/λ_q	Scheme (Bytes)	Sig. Size (Bytes)	PK (Bytes)	SK (Cycles)	Sign (Cycles)	Verify	CPU
196/98	XMSS	1.3 kB	14.6 kB	8.3 kB	13,014,401	–	Intel Core i7 3.5GHz
196/98	XMSS-T	0.064 kB	14.6 kB	8.3 kB	37,025,552	–	Intel Core i7 3.5GHz

TABLE XVI
PERFORMANCE, KEY SIZES AND SIGNATURE SIZES OF MSS ON AN 8-bit MICROPROCESSOR [84]

λ	Scheme	H	(w, k)	PK (Bytes)	SK (Bytes)	Sig. Size (Bytes)	ROM (Bytes)	Sign (ms)	Verify (ms)
128	MSS using S/W AES	16	(2, 2)	16	1440	2350	6600	85	1230
		16	(2, 4)	16	1440	2350	6600	85	1230
		16	(4, 4)	16	1440	2350	6600	85	1230
128	MSS using H/W AES	16	(2, 2)	16	1440	2350	6100	24	362
		16	(2, 4)	16	1440	2350	6100	24	317
		16	(4, 4)	16	1472	1330	6100	38	504
128	MSS using S/W AES	10	(2, 2)	16	848	2290	6600	825	756
		10	(2, 4)	16	876	2290	6600	82	598
		10	(4, 4)	16	876	1234	6600	124	946

TABLE XVII
PERFORMANCE OF STATELESS HASH-BASED SIGNATURE SCHEME, SPHINCS [85]

λ/λ_q	Scheme (Bytes)	Sig. Size (Bytes)	PK (Bytes)	SK (Cycles)	Sign (Cycles)	Verify	CPU
256/128	SPHINCS 256^{e,s}	41,000	1,056	1,088	51,636,372	1,451,004	Intel Xeon E3-1275 3.5 GHz

core of Intel Xeon E3-1275 CPU at 3.5 GHz are given in Table XVI [85]. Rohde *et al.* [84] implemented MSS on 8-bit AVR microcontrollers. We summarize performance of MSS with S/W AES or H/W AES on the 8-bit AVR microcontrollers from [84] in Table XVI.

These stateful hash-based schemes should generate an updated secret key in signing after generating a signature on a message. The definition of digital signatures does not allow this kind of the state change for the secret key. Also, this does not fit standard APIs. It can lead to security threat since its security cannot be guaranteed if the update ends in failure. SPHINCS [85] is a stateless hash-based signature scheme and uses the one-time signature scheme, WOTS+, and a few-time signature scheme, HORST. The authors in [85] showed that SPHINCS is provably secure under weak standard model assumption avoiding the collision resistance property. The performance, signature sizes and key sizes of SPHINCS is given in Table XVII.

F. Code-Based Signature Schemes

Code-based cryptographic algorithms use error correcting codes. This primitive consists in adding an error to a word of C or in computing a syndrome to a parity check matrix of C. The first of them is McEliece public-key encryption scheme [86] the oldest known scheme based on coding theory.

1) Underlying Hard Problems of Code-Based Schemes:

- **Syndrome Decoding Problem:** For integers r, n, and w, (H, w, s) is a triple of a matrix $H \in \mathbb{F}_2^{r \times n}$, an integer $w < n$, and a vector $s \in \mathbb{F}_2^r$. Find a vector $e \in \mathbb{F}_2^n$ of weight $\mathtt{wt}(e) \leq w$ such that $He^T = s^T$.

2) Constructions and Implementation Results of Code-Based Schemes: At Asiacypt 2001, Courtois, Finiasz,

TABLE XVIII
PERFORMANCE OF CODE-BASED SIGNATURE SCHEME, CFS

λ	PK (Bytes)	SK (Bytes)	Sig. Size (Bytes)	Sign (Cycles)	Verify (Cycles)	TAP	CPU
80	20,968,300	4,194,300	75	4.2×10^9 (1.32 s) [89]	–	×	Intel Xeon W 3670 3.2GHz
				0.425×10^9 [89]	–	×	Ivy Bridge
				0.658×10^9 [88]	–	O	Intel AMD SSE
				–	2790 [88]	O	Intel Core 2 Quad Q6600

and Sendrier [87] proposed a way to build a signature scheme (CFS) based on McEliece scheme. CFS is a hash-and-sign scheme with a security reduction to the syndrome decoding problem. CFS suffers from large public key sizes and inefficient signing while it has short signatures. Bernstein *et al.* [88] presented the implementation of CFS signature scheme. Their implementation provided full protection against timing attacks: since one signs a single message at a time, some parts of the calculation are executed on only one stream of data, but even in those parts they utilized constant-time field arithmetic instead of the arithmetic using lookup-table in [89]. We summarize performance, signature sizes and key sizes of CFS in Table XVIII from [88], [89], where TAP represents timing attack protection. Ranksign [90] was also a code-based scheme using the approach of McEliece encryption. However, the public keys in these schemes can be distinguished from a random matrix [91], [92]. In these schemes, the possible existence of a structural attack recovers their hidden structures breaking the schemes. Debris-Alazard and Tillich [92] proposed a polynomial structural attack on Ranksign.

Like other PQ-signature schemes, the signature schemes using the Fiat-Shamir transform provide security reductions to generic problems, but results in a very large signature size due to repeated multiple commitments to prevent an attacker's cheating. Despite attempts to reduce this cheating probability, it seems implausible to get a truly efficient scheme in this way.

Recently, a new code-based signature scheme, WAVE, was constructed [93]. It is based on two problems: a distinguishing problem and a multiple target version of syndrome decoding. Subsequently, Barreto and Persichetti [94] showed that some information leakages occurring from honestly-generated signatures enables efficiently recovering the alternative private key of WAVE. They succeeded in breaking the suggested parameters of WAVE at the 128-bit security level in a minute and then proposed its variant, Tsunami. Song *et al.* [95] proposed the Rank Quasi-Cyclic Signature (RQCS) scheme using rank-metric quasi-cyclic codes based on the syndrome decoding problem. However, RQCS was broken by the key recovery attacks to recover the private key less than 10 seconds from only one signature [96]. Aragon *et al.* [97] proposed a new code-based scheme, Durandal, based on the Rank Syndrome problems and the Rank Support Learning. Like these, almost of code-based signature schemes were broken.

G. Supersingular Isogeny-Based Signature Schemes

Security of supersingular isogeny-based cryptosystems relies on the hardness of finding a path in the isogeny graph of supersingular elliptic curves. Due to Biasse-Jao-Sankar [98], the only known quantum algorithm for these problems has exponential complexity unlike other elliptic curve cryptosystems.

1) Underlying Hard Problems of Supersingular Isogeny-Based Schemes: Let p be a prime. et E and E' be supersingular elliptic curves over a finite field $\mathbb{F}_p$. An isogeny $\phi : E \to E'$ is a non-constant morphism from E to E' which maps the neutral element to the neutral element.

- **Supersingular Isogeny Problem [99]:** Given supersingular elliptic curves, E and E', over $\mathbb{F}_{p^2}$, chosen uniformly at random, find an isogeny $\phi : E \to E'$.

Let E be an ordinary elliptic curve over a finite field $\mathbb{F}_p$ with $\mathrm{End}(E) = \mathcal{O}$ or E a supersingular curve over $\mathbb{F}_p$ with $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}$, where $\mathcal{O}$ is an order in an imaginary quadratic field. Let $\mathrm{Cl}(\mathcal{O})$ be the ideal class group of $\mathcal{O}$. Define the action of an $\mathcal{O}$-ideal $\mathfrak{a}$ on the curve E as the image curve E' under the isogeny $\phi : E \to E'$ whose kernel is the subgroup

$$E[\mathfrak{a}] = \{P \in E(\overline{\mathbb{F}_p}) : \alpha(P) = 0, \alpha \in \mathfrak{a}\}.$$

We denote E' by $\mathfrak{a} * E$.

- **Group Action Problem [100]:** Given $E_A = \mathfrak{a} * E$ for some ideal $\mathfrak{a} = \prod_{i=1}^{n} l_i^{e_i}$, where the exponent vector $e = (e_1, \cdots, e_n)$ is uniformly sampled in $[-B, B]^n \subseteq \mathbb{Z}^n$, compute any ideal equivalent to $\mathfrak{a}$.

2) Constructions and Implementation Results of Supersingular Isogeny-Based Schemes: Stolbunov [101] proposed the first signature scheme based on the isogeny problems using class group actions. It was not analysed in the post-quantum setting and a naive implementation would leak the private key. Galbraith *et al.* [99] proposed a new identification protocol (GCS) in the hardness of the endomorphism ring computation problem using an algorithm of Kohel Lauter-Petit-Tignol for the quaternion version of the l-isogeny problem. They then constructed new signature schemes, GCS+FS and GCS+U from their identification protocol via the Fiat-Shamir transform [30] for classical security and via the Unruh transform [102]) for post-quantum security, respectively. In Table XIX, we summarize signature sizes and key sizes of their three schemes in general. In Table XX, we summarize concrete efficiency of the converted GCS schemes at the 128 and 256-bit security levels. All sizes are in bits.

Castryck *et al.* [103] proposed a key exchange, CSIDH, using the class group actions. At Eurocrypt 2019, Feo and Galbraith [100] constructed a signature from Lyubashevsky's "Fiat-Shamir with aborts" strategy [104]. They showed that their basic signature scheme using rejection sampling is unforgeable under a chosen message attack under the hardness assumption of the Group Action Problem in the random oracle

TABLE XIX
SIGNATURE SIZES, KEY SIZES AND COSTS OF GCS SCHEMES [99]

Scheme	SK size	PK size	Sig. Size	Sign cost	Verify cost
GCS+FS	2λ	6λ	$11\lambda^2$	$O(\lambda^3)$	$O(\lambda^3)$
GCS+U	4λ	12λ	$75\lambda^2$	$O(\lambda^5)$	$O(\lambda^5)$

TABLE XX
SIGNATURE SIZES AND KEY SIZES OF GCS SCHEMES [99]

λ	Scheme	SK size	PK size	Sig. Size
128	GCS+FS	256	768	180,224
	GCS+U	512	1536	1,228,800
256	GCS+FS	512	1536	720,896
	GCS+U	1024	3072	49,152,000

TABLE XXI
PERFORMANCE, SIGNATURE SIZES AND KEY SIZES OF FEO-GALBRAITH'S THREE SCHEMES [100]

Cost	Scheme	Rejection sampling	Shorter signatures	Smaller public keys
Comm. Cost	Sig. size	2144 B	978 B	3136 B
	PK size	64 B	4096 KB	32 B
	SK size	32 B	16 B	1024 KB
Comp. Cost	KeyGen	0.03 s	1966 s	1966 s
	Verify	36372 s	142 s	142 s

model. They also proposed two variants of the basic scheme with shorter signatures and smaller public keys. In Table XXI, we summarize performance, signature sizes and key sizes of their three schemes at the 128-bit security level. Signing time of their schemes is on average 3 times the estimated verification time. The isogeny-based signature schemes have relatively shorter key sizes, but their performance are the slowest of the five-type PQ-signature schemes.

IV. IMPLEMENTATION ATTACKS ON POST-QUANTUM SIGNATURE SCHEMES

Implementation attacks focus on capabilities of an attacker to break a cryptographic algorithm by exploiting vulnerabilities in their implementations rather than its underlying mathematical structure. Practical implementation attacks consist of side-channel analysis (SCA) and fault attacks. SCA is a passive attacker, where an attacker can use information leaked from execution time, power consumption and electromagnetic radiation corresponding to timing attack, power analysis, and electromagnetic attack, respectively, to recover the secret keys. Fault analysis is an active attack, where an attacker can maliciously inject faults into the cryptographic algorithm using clock glitch or power glitch and investigate the faulty outputs, which can reveal some information about the secret key. A cold-boot attack is a type of side-channel attack, where an attacker utilizes the phenomenon of memory remanence in SRAM or DRAM to read data out of a computer's memory after the computer has been powered off. Here, we focus on implementation attacks on PQ-signature schemes.

A. Side-Channel Attacks

For lattice-based schemes, Groot Bruinderink *et al.* [105] presented a cache attack on BLISS to extract side information on the coefficients of the commitment polynomial via cache side-channels and then recovered the secret key from the side-channel information using the lattice reduction. At ACM CCS 2017, Pessl *et al* [106] and Espitau *et al.* [107] demonstrated practical SCAs on lattice-based schemes, BLISS and BLISS-B variants, which have seen the first real adoption in StrongSwan, an IPSEC-based VPN suite. In [106], using an extension of Howgrave-Graham-Szydlo algorithm, they recovered the secret key from the relative norm leaked from the existing implementations of that rejection sampling step. They showed how this leakage can be used in practice by performing the SCA with electromagnetic analysis (EMA), both on an 8-bit AVR microcontroller, and a recent Intel CPU using branch tracing. They presented differential power analysis on the sparse polynomial multiplications carried out in BLISS by succeeding the recovery of the secret key in that setting from a single EMA trace utilizing integer linear programming. In [107], the authors presented an improved version of Groot Bruinderink *et al.*'s cache attack on BLISS and used their new key-recovery method to perform an asynchronous cache attack on the BLISS implementation in StrongSwan. In [108], Ravi *et al.* showed that the partial secret-key s_1 of Dilithium [68] is retrieved through a power analysis attack on the polynomial multiplier succeeding in forging signatures with only the extracted portion of the secret-key, without the knowledge of all the secret key.

For hash-based schemes, Kannwischer *et al.* [109] presented differential power analysis on stateful schemes, XMSS and XMSS^{MT}, standardized at IETF, as well as a stateless scheme, SPHINCS. They showed that the resistance of XMSS against the differential power analysis is reduced to resistance of the underlying pseudorandom number generator against the differential power analysis. Furthermore, they recovered at least a 32-bit chunk of SPHINCS secret key using a differential power analysis owing to its stateless construction. More precisely, they presented new differential power analysis on a pseudo-

random function based on BLAKE-256 for SPHINCS-256 and a pseudorandom number generator based on SHA-2 for XMSS in the Hamming weight model. The first one is not a threat to current versions of XMSS, if a customized pseudorandom number generator is not utilized. The second one is a threat to SPHINCS-256 hardware implementation.

For MQ-schemes, in [110], the authors presented differential power analysis on SFLASH to recover a random seed Δ used for the hash function SHA-1 not the secret key (S, T). Recently, at CHES 2018, the authors [111] presented correlation power analysis on Rainbow and UOV implementations in [46]. More precisely, they recovered the full secret keys of UOV and Rainbow when they are implemented with equivalent keys as in [46]. They then extended their attacks to Rainbow implementation with random affine maps instead of the equivalent keys: after recovering S by CPA, they can recover T by using algebraic key recovery attacks using good keys. For MQ-schemes, in [112] and [113], the authors proposed the differential power analysis with fault attacks on enTTS which is a special case of Rainbow and UOV, respectively.

Timing attacks and power analysis on McEliece encryption [114] based on Goppa codes [114]–[116], simple power, timing attacks and differential power analysis on McEliece with MDPC codes with a low-cost microcontroller [117]–[119] have been presented. The implementation security of code-based encryption schemes have been sufficiently analyzed, but that of the code-based signature scheme has never performed.

B. Fault Analysis

In fault analysis, after an attacker injects faults during the execution of cryptographic algorithms and analyze faulty outputs and information leaked from this incorrect behavior to recover partial or full information on the secret key. Algebraic fault analysis combines fault attacks with algebraic cryptanalysis, where an adversary invokes faults on the schemes collecting only a necessary number of faulty outputs such that the remaining problem can be solved mathematically.

Bindel *et al.* [120] presented skipping, zeroing and randomizing fault attacks on three lattice-based schemes, GLP [62], BLISS [64] and Ring-TESLA [66]. These attacks resulted in forging signatures without the knowledge of the secret keys or recovering the secret keys. Espitau *et al.* [121] presented several fault attacks on both hash-and-sign schemes including the GPV-based scheme of Ducas-Prest-Lyubashevsky and Fiat-Shamir type constructions including GLP [62], BLISS [64], PASSSign [122], and Ring-TESLA [67] that recover the full secret key with only a few faults or only one. They concretely carried out their fault attacks with clock glitches on an 8-bit AVR XMEGA microcontroller using the power analysis on the testing board ChipWhisperer-Lite. At CHES 2018, Groot and Pessl [123] demonstrated differential fault attacks on two deterministic lattice-based schemes, Dilithium and qTESLA. They demonstrated that a single random fault can result in recovering the secret key in a nonce-reuse scenario and extended this to fault-induced partial nonce-reuse attacks, They carried out their fault attacks with clock glitching on an ARM Cortex-M4 microcontroller. Dilithium [68] is a deterministic signature scheme, whose nonce is derived by hashing the key and the message, the attack can let a victim sign the same message twice, but invoke a fault in one of the signature generations. They succeeded in forging signatures on any messages using a tweaked signature algorithm without the knowledge of other parts of the secret key.

For hash-based schemes, Castelnovi *et al.* [124] presented fault attacks on current standardization candidates, XMSS, LMS, SPHINCS+, and Gravity-SPHINCS, succeeding in universally forging signatures within seconds. Genê *et al.* [125] performed the fault attack with a simple voltage glitch injection on an Arduino Due board featuring an ARM Cortex-M3 microprocessor running the original stateless signature scheme, SPHINCS. The fault attacks on the hash-based signature scheme force a one-time signature to be reused. They showed that caching one-time signatures can prevent the attack for stateful schemes, such as XMSS and LMS, while the countermeasure does not apply to stateless schemes, like SPHINCS, Gravity-SPHINCS and SPHINCS+ as efficiently as in stateful schemes.

For MQ-schemes, Hashimoto *et al.* [126] demonstrated general fault attacks on MQ-schemes including Single Field type (UOV, Rainbow, STS and TTM/TTS) and Big Field type (Matsumoto-Imai, HFEv- and SFLASH). They showed that the faulty outputs weakened their security against Kipnis-Shmair attacks. Recently, Shim and Koo [127] provided three types of fault analysis on Rainbow and UOV, which combined the key recovery attacks using good keys with fault attacks dividing the fault models into three cases depending on the leakage types of Vinegar values: reused, revealed and set to zero. They showed that $(m + 1)$, n, m faulty signatures generated by the entire faulty Vinegar values in the Vinegar values-reuse, reveal and set to zero scenarios led to full recoveries the equivalent key of UOV in polynomial time In general, some of faulty Vinegar values in the Vinegar values-reuse, reveal and set to zero scenarios significantly weaken the security of UOV and Rainbow against the key recovery attacks in terms of the number of the faulty Vinegar values.

C. Cold Boot Attacks

At USENIX 2008, Halderman *et al.* [128] presented that ordinary DRAMs typically lose their contents gradually over a period of seconds, and the residual data can be recovered using simple, non-destructive techniques which require only momentary physical access to the machine. Specifically, they demonstrated that a significant fraction of the bits of a secret key can be recovered if the key is ever stored in memory for DES, AES, and RSA, employed in disk encryption schemes. They recovered a 128-bit AES key within a few seconds with 10% of bits decayed and a 2048-bit RSA private key p and q from 6% corruption in minutes.

There have been presented the cold boot attacks on the post-quantum cryptographic algorithms. Dachman-Soled *et al.* [129] presented partial key exposure attacks in Ring-Learning with Errors (R-LWE)-based cryptosystems. More precisely, they recovered the full R-LWE secret for standard parameter settings given certain 1/4-fraction of the coordinates

TABLE XXII
KEY SIZES, SIGNATURE SIZES AND PERFORMANCE OF CLASSICAL SCHEMES AND PQ-SCHEMES ON 64-bit PLATFORM AT THE 128-bit SECURITY LEVEL

Scheme	Sig. Size (Bytes)	PK (Bytes)	SK (Bytes)	Sign (Cycles)	Verify (Cycles)	CPU
RSA-3072 [29]	361	384	3072	8,733,058	84,562	Intel Core i5-6600 3.3 GHz
ECDSA-256 [29]	64	64	96	162,778	308,510	Intel Core i5-6600 3.3 GHz
ed25519 [29]	64	32	64	49,840	163,206	Intel Core i5- 6600 3.3 GHz
BLISS-BI	700	875	250	358,400	102,000	Intel Core i7 3.4 GHz
Dilithium (125) [68]	2,701	1,472	3,504	789,000	209,000	Intel Core i7-4770K (Haswell)
XMSS^{MT}_SHA-256 _m32_n32 ($h = 20$)	4,932	1,036	1,280	2,485,000	245,000	Intel Core i7-3.5GHz
Rainbow ($\mathbb{F}_{2^8}, 36, 21, 22$)	79	139,320	105,006	64,658	44,397	Intel Core i5-6600 3.3 GHz

TABLE XXIII
PERFORMANCE OF CLASSICAL SCHEMES AND PQ-SCHEMES ON 8-bit MICROPROCESSORS

λ	Scheme	Sign (Cycles)	Verify (Cycles)	CPU
128	NIST P 256 [134]	34,903,000	–	AT 2560
128	Curve25519 [134]	13,900,397	–	AT 2560
128	BLISS-BI [69]	10,537,981	2,814,118	AX 128
128	Rainbow($\mathbb{F}_{2^8}, 36, 22, 21$) [46]	8,227,000	9,216,000	AX 128
128	enTTS($\mathbb{F}_{2^8}, 15, 60, 88$) [46]	2,142,000	30,789,000	AX 128

of the NTT transform of the R-LWE secret. Recently, Albrecht *et al.* [130] presented cold boot attacks on cryptographic algorithms based on the ring- and module- variants of the LWE problems. where an adversary is faced with the problem of recovering a secret key from a noisy version of that key. They showed that the encoding method that stores polynomial coefficients directly in memory is vulnerable to cold boot attacks only at very low bit-flip rates. Recently, Villanueva-Polanco presented the cold boot attacks on the lattice-based signature scheme, BLISS [131] and the MQ-signature scheme, LUOV [132].

V. COMPARISONS AND DISCUSSIONS

We provide comparisons between the five types of PQ-schemes and discussions on open research issues.

A. Comparisons

Finally, we provide comparisons between the five types of PQ-signature schemes and classical schemes in terms of key sizes, signature sizes and performance on 64-bit platform, 8-bit microprocessors and FPGA at the 128-bit security level. Table XXII compares the signature schemes in each type of PQ-schemes from the literatures introduced in the previous sections and classical schemes given by the eBACS project [29]. We exclude the code-based scheme from Table XXII since there is no its result at the 128-bit security level. We also exclude the supersingular isogeny-based schemes since they are very slow and there are no implementation results represented cycles. Details of the classical schemes are as follows:

- RSA-3072 (ronald3072) [29]: 3072-bit RSA signature with message recovery.
- ECDSA-256 (ecdonaldp256) [29]: ECDSA signature using NIST P-256 elliptic curve, a curve modulo the prime $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$.
- ed25519 [29]: EdDSA signatures using Curve25519 [133].

In Table XXIII, we provide comparisons between lattice-based BLISS-BI, MQ-based Rainbow and classical schemes in terms of key sizes, signature sizes and performance on 8-bit platform at the 128-bit security level. Details of the target devices in Table XXIII are as follows:

- AX 128: ATxMega128a1, 128kB Flash, 8KB SRAM, 32 MHz.
- AT 2560: ATmega2560, 256kB Flash, 8KB SRAM, 16 MHz.

Table XXIV compares the performance of classical-schemes and PQ-schemes on FPGA.

B. Discussions

We have surveyed the five types PQ-signature schemes. As investigated in previous sections, such primitives to protect classical and quantum attacks have been proposed and have inspired widespread confidence in their suitability as post-quantum replacements. However, most of these primitives have the features of large public key, signature sizes and/or slow performance compared to classical schemes, RSA and ECDSA. Now, we discuss open research issues for improving security and efficiency of PQ-signature schemes.

Lattice-based schemes are relatively fast and provide reasonably small keys and signatures for the suggested parameters. However, their quantitative parameters for required security levels are unclear. In 2013 [64], for a lattice-based signature scheme to achieve a 100-bit security level for a given parameter set in 2012 and to correct that to only 75-80-bit security levels. Depending on the selection of some types of lattices, it is hard to choose optimal parameters for given security level, i.e. it is not flexible. Methodology for the selection of parameters from the complexity of algorithms for solving the lattice-based problems should be clarified.

TABLE XXIV
PERFORMANCE OF CLASSICAL SCHEMES AND PQ-SCHEMES ON FPGA

λ	Scheme	Sign (Ops/s)	Verify (Ops/s)	Device
128	ECDSA secp256r1	139	110	XC5VLX110T
128	ECDSA-256 prime curve	2,631	–	XC5LX100
128	ECDSA Curve25519	2,518	–	XC7Z020
128	BLISS-BI	8,761	17,101	XC6SLX25

Due to simple operations and the use of small finite fields without multi-precision arithmetics, MQ-schemes are very fast and have short signatures. From efficiency perspective, MQ-based schemes are superior to other PQ-schemes with respect to speed and signature size. Since they require only very moderate resources, they are excellent candidates for resource constraint devices. However, the major obstacle of MQ-signature scheme is relatively large key sizes. In IoT, a certain environment using constrained devices like sensors and wearable small devices needs a signature scheme for device authentication and message authentication, so the devices are required to perform only signature generation from a secret key without storing the associated public key. In that case, the MQ-based signature scheme will be the best choice. Because as in Table XXIII, an MQ-signature scheme is the fastest scheme on the 8-bit microprocessors. In wired internet, these key size problems are not a big deal. Thus, for the practical use of constraint devices for general IoT environments, their key sizes should be reduced to an adequate level. Unlike the public key, the secret key size of MQ-schemes can be significantly reduced using several methods such as sparse polynomials and PRNG. If the secret key size is small (if it uses a small seed, the secret key size is 32 bytes at the 128-bit security level) and an application requires only signature generations on constraint devices without storing any public key then MQ-schemes are the best candidate for it.

Practical hash-based schemes including XMSS and XMSS^{MT} standardized in IETF are stateful. It is difficult to use them securely unless their state management problems are solved. In stateful schemes, the most commonly raised concern is statefulness, since they use one-time signatures and their secret key should be used only once. If two different messages are signed with the same secret key, then an adversary can use these signatures to forge a signature on a new message. Thus, after signing on a message, the signer must update the state so that the same secret key is not reused, thus an updated secret key is generated and stored. This doesn't match the standard definition of signatures in cryptography and it doesn't fit standard APIs. While the theory of hash-based schemes is highly developed, a discussion of the system security issues arising from their state managements has been lacking. For the practical use of the schemes, methods for state managements should be studied.

The supersingular isogeny-based signature schemes have relatively shorter key sizes, but their performance are the slowest of the five-type PQ-signature schemes. The scheme exceeds hundreds of seconds for verification and its signing time on average 3 times the verification time. Thus, it seems difficult to use in real applications.

Many implementation attacks on PQ-signature schemes have been proposed: unlike lattice-based and hash-based schemes, other PQ-signature schemes have little effort with respect to implementation security. Further vulnerability analysis and study of countermeasures on PQ-signature schemes need to be designed before using the schemes in IoT embedded devices. For the practical use of IoT constraint devices, various types of implementation attacks, their countermeasures on the PQ-signature schemes should be studied. These countermeasures are useful in selecting a appropriate set of countermeasures against the implementation attacks for the secure use of the schemes.

VI. CONCLUSION

We have targeted to the five well-known directions of cryptographic primitives believed to be resist both classical and quantum attacks: multivariate quadratic-based, hash-based, lattice-based, code-based and supersingular isogeny-based schemes. We have investigated theoretical backgrounds of the five types PQ-signature schemes in terms of their underlying mathematically hard problems and structures. We have also included their state-of-the-art constructions, implementation results and security results against implementation attacks, side-channel attacks and fault analysis. The software implementations for these signature schemes cover various platform from 64-bit to 8-bit platforms. This survey focuses mainly on the 128-bit security level including various security level and quantum security level. It provides invaluable guidelines to find tradeoffs between size, performance, cost, and security for various practical applications ranging from powerful servers and resource constrained 8-bit devices. Our investigation have shown that most of these primitives have the features of enormous public key, signature sizes and/or slow performance when compared to classical primitives, RSA and ECC based on the intractability of integer factorization problem and the elliptic curve discrete logarithm problem, respectively. So, for these primitives, further research for more confidence in their security, particularly against adversaries with quantum computers, and improvements their performance and key sizes are need for secure communications in the post-quantum era.

REFERENCES

[1] Gartner. *Gartner Says 8.4 Billion Connected, 'Things' Will be in use*, 2017. Accessed: May 2, 2021. [Online]. Available: https://www.gartner.com/newsroom/id/3598917
[2] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.
[3] NSA. (Aug. 19, 2015). *NSA Suite B Cryptography*. [Online]. Available: https://www.nsa.gov/ia/ programs/suiteb_cryptography/

[4] NIST. (2016). *Post-Quantum Cryptography: NIST's Plan for the Future*. [Online]. Available: http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf

[5] Google. (2016). *Experimenting With Post-Quantum Cryptography*. [Online]. Available: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html?m=1

[6] Microsoft. (2016). *SIDH Library*. [Online]. Available: https://www.microsoft.com/en-us/download/ details.aspx?id=52438&751be11f-ede8-5a0c-058c-2ee190a24fa6=True

[7] R. Xu, C. Cheng, Y. Qin, and T. Jiang, "Lighting the way to a smart world: Lattice-based cryptography for Internet of Things," 2018, *arXiv:1805.04880*.

[8] S. Paul and P. Scheible, "Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication," IACR Cryptol. ePrint Arch., Tech. Rep. 2020/1322, 2020.

[9] T. C. McGwier, R. W. McGwier, and L. Chen, "Post-quantum cryptography and 5G security: Tutorial," in *Proc. ACM WiSec*, Miami, FL, USA, 2019, p. 285, doi: 10.1145/3317549.3324882.

[10] P. S. L. M. Barreto, J. E. Ricardini, M. A. Simplicio, and H. K. Patil, "QSCMS: Post-quantum certificate provisioning process for V2X," IACR Cryptol. ePrint Arch., Tech. Rep. 2018/1247, 2018.

[11] D. Butin, S.-L. Gazdag, and J. Buchmann, "Real-world post-quantum digital signatures," *Cyber Security and Privacy Forum*. Cham, Switzerland: Springer, 2015, pp. 41–52.

[12] P. Palmieri, "Hash-based signatures for the Internet of Things," in *Proc. 15th ACM Int. Conf. Comput. Frontiers*, May 2018, pp. 332–335.

[13] S. Rohde, T. Eisenbarth, E. Dahmen, J. Buchmann, and C. Paar, "Fast hash-based signatures on constrained devices," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, 2008, pp. 104–117.

[14] S. Ghosh, R. Misoczki, and M. R. Sastry, "Lightweight post-quantum-secure digital signature approach for IoT motes," IACR Cryptol. ePrint Arch., Tech. Rep. 2019/122, 2019.

[15] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, Feb. 2017.

[16] Z. Liu, K.-K. R. Choo, and J. Großschädl, "Securing edge devices in the post-quantum Internet of Things using lattice-based cryptography," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 158–162, Feb. 2018.

[17] *Website: Grobal Risk Institute*. Accessed: Oct. 4, 2021. [Online]. Available: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

[18] S. Vogt and H. Funke, "How quantum computers threat security of PKIs and thus eIDs," in *Open Identity Summit* (Lecture Notes in Informatics). Bonn, Germany: Gesellschaft für Informatik, 2021, pp. 83–94.

[19] K. L. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput. (STOC)*, 1996, pp. 212–219. [Online]. Available: https://arxiv.org/pdf/quant-ph/9605043v3.pdf

[20] D. J. Bernstein and T. Lange, "Post-quantum cryptography–dealing with the fallout of physics success," IACR Cryptol. ePrint Arch., Tech. Rep. 2017/314, 2017.

[21] S. Hallgren, "Polynomial-time quantum algorithm for Pell's equation and the principal ideal problem," in *Proc. 34th Annu. ACM Symp. Theory Comput.*, 2002, pp. 653–658.

[22] S. Hallgren, "Fast quantum algorithms for computing the unit group and class group of a number field," in *Proc. 37th Annu. ACM Symp. Theory Comput. (STOC)*, 2005, pp. 468–474.

[23] K. Eisenträger, S. Hallgren, A. Kitaev, and F. Song, "A quantum algorithm for computing the unit group of an arbitrary degree number field," in *Proc. 46th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, May 2014, Art. no. 293302.

[24] J.-F. Biasse and F. Song, "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields," in *Proc. 27th Annu. ACM-SIAM Symp. Discrete Algorithms*, Jan. 2016, pp. 893–902.

[25] P. Campbel, M. Groves, and D. Shepherd. (2014). *SOLILOQUY, a Cautionary Tale*. [Online]. Available: http://docbox.etsi.org/Workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf

[26] R. Cramer, L. Ducas, C. Peikert, and O. Regev, "Recovering short generators of principal ideals in cyclotomic rings," IACR Cryptol. ePrint Arch., Tech. Rep. 2015:313, 2015.

[27] N. P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes," in *Public Key Cryptography* (Lecture Notes in Computer Science), P. Q. Nguyen and D. Pointcheval, Eds. Berlin, Germany: Springer-Verlag, 2010, pp. 420–443.

[28] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2013, pp. 1–17.

[29] D. J. Bernstein and T. Lange. *eBACS: ECRYPT Benchmarking of Cryptographic Systems*. Accessed: May 22, 2017. [Online]. Available: https://bench.cr.yp.to

[30] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1987, pp. 186–194.

[31] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, 1988.

[32] A. Bogdanov, T. Eisenbarth, A. Rupp, and C. Wolf, "Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves?" in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2008, pp. 45–61.

[33] A. I.-T. Chen *et al.*, "SSE implementation of multivariate PKCs on modern X86 CPUs," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2009, pp. 33–48.

[34] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (A Series of Books in the Mathematical Sciences). San Francisco, CA, USA, 1979.

[35] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1996, pp. 33–48.

[36] C. Bouillaguet, P.-A. Fouque, and A. Véber, "Graph-theoretic algorithms for the 'isomorphism of polynomials' problem," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2013, pp. 211–227.

[37] J. O. Shallit, G. S. Frandsen, and J. F. Buss, "The computational complexity of some problems of linear algebra," BRICS Series Rep., Aarhus, Denmark, Tech. Rep. RS-96-33, 1996.

[38] J. Patarin, N. Courtois, and L. Goubin, "Quartz, 128-bit long digital signatures," in *Topics in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2001, pp. 282–297.

[39] A. Petzoldt, M.-S. Chen, B.-Y. Yang, C. Tao, and J. Ding, "Design principles for HFEv-based multivariate signature schemes," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2015, pp. 311–334.

[40] S. M. El Yousfi Alaoui, O. Dagdelen, P. Veron, D. Galindo, and P.-L. Cayrel, "Extended security arguments for signature schemes," *Progress in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2012, pp. 19–34.

[41] M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe, "From 5-pass MQ-based identification to MQ-based signatures," in *Progress in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2016, pp. 135–165.

[42] K. Sakumoto, T. Shirai, and H. Hiwatari, "Public-key identification schemes based on multivariate quadratic polynomials," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2011, pp. 706–723.

[43] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1999, pp. 206–222.

[44] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2005, pp. 164–175.

[45] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1988, pp. 419–453.

[46] P. Czypek, S. Heyse, and E. Thomae, "Efficient implementations of MQPKS on constrained devices," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2012, pp. 374–389.

[47] A. Petzoldt, E. Thomae, S. Bulygin, and C. Wolf, "Small public Keys and fast verification for multivariate quadratic public key systems," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2011, pp. 475–490.

[48] B.-Y. Yang and J.-M. Chen, "Building secure tame-like multivariate public-key cryptosystems: The new TTS," in *Information Security and Privacy* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2005, pp. 518–531.

[49] S. Tang, H. Yi, J. Ding, H. Chen, and G. Chen, "High-speed hardware implementation of rainbow signature on FPGAs," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2011, pp. 228–243.

[50] B. Ansari and M. A. Hasan, "High performance architecture of elliptic curve scalar multiplication," CACR, Tech. Rep. 2006-01, Jan. 2006.

[51] C. Shu, K. Gaj, and T. El-Ghazawi, "Low latency elliptic curve cryptography accelerators for NISTcurves over binary fields," in *Proc. IEEE Int. Conf. Field-Program. Technol.*, Dec. 2005, pp. 309–310.

[52] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. STOC*, 1996, pp. 99–108.

[53] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annu. ACM Symp. Theory Comput. (STOC)*, 2005, pp. 84–93.

[54] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in *Proc. 29th Annu. ACM Symp. Theory Comput. (STOC)*, 1997, pp. 284–293.

[55] J. Hoffstein, J. Pipher, and H. J. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1998, pp. 267–288.

[56] D. Micciancio, "Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions," in *Proc. 43rd Annu. IEEE Symp. Found. Comput. Sci.*, Nov. 2002, pp. 356–365.

[57] O. Goldreich, S. Goldwasser, and S. Halevi, "Public-key cryptosystems from lattice reduction problems," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 1997, pp. 112–131.

[58] J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte, "NTRUSIGN: Digital signatures using the NTRU lattice," in *Topics in Cryptology*, vol. 140. Berlin, Germany: Springer-Verlag, 2003, p. 122.

[59] P. Q. Nguyen and O. Regev, "Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures," in *Advances in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2006, pp. 271–288.

[60] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 40th Annu. ACM Symp. Theory Comput.*, May 2008, Art. no. 197206.

[61] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2012, pp. 738–755. [Online]. Available: https://eprint.iacr.org/2011/537

[62] T. Guneysu, V. Lyubashevsky, and T. Poppelmann, "Practical lattice-based cryptography: A signature scheme for embedded systems," in *Cryptographic Hardware and Embedded Systems*. Berlin, Germany: Springer-Verlag, 2012, pp. 530–547.

[63] S. Bai and S. D. Galbraith, "An improved compression technique for signatures based on learning with errors," in *Topics in Cryptology* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2014, pp. 28–47.

[64] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 2013, pp. 40–56.

[65] C. Peikert, "How (not) to instantiate ring-LWE," IACR Cryptol. ePrint Arch., Tech. Rep. 2016:351, 2016.

[66] E. Alkim, N. Bindel, J. Buchmann, O. Dagdelen, and P. Schwabe, "TESLA: Tightly-secure efficient signatures from standard lattices," IACR Cryptol. ePrint Arch., Tech. Rep. 2015/755, 2015.

[67] S. Akleylek, N. Bindel, J. Buchmann, J. Kramer, and G. A. Marson, "An efficient lattice-based signature scheme with provably secure instantiation," in *Progress in Cryptology*. 2016, pp. 44–60.

[68] L. Ducas *et al.*, "CRYSTALS-Dilithium: A lattice-based digital signature scheme," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2018, no. 1, pp. 238–268, 2018.

[69] T. Pöppelmann, T. Oder, and T. Güneysu, "High-performance ideal lattice-based cryptography on 8-bit ATxmega microcontrollers," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 9230. Berlin, Germany: Springer-Verlag, 2015, pp. 346–365.

[70] T. Poppelmann, L. Ducas, and T. Guneysu, "Enhanced lattice-based signatures on reconfigurable hardware," IACR Cryptol. ePrint Arch., Tech. Rep. 2014/254, 2014.

[71] F. Song, "A note on quantum security for post-quantum cryptography," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 8772. Berlin, Germany: Springer-Verlag, 2014, pp. 246–265.

[72] R. Lamport, "Constructing digital signatures from a one way function," SRI Int., Palo Alto, CA, USA, Tech. Rep. CSL-98, 1979.

[73] R. Merkle, "Secrecy, authentication, and public key systems," Inf. Syst. Lab., Stanford Univ., Stanford, CA, USA, Tech. Rep. 1979-1, 1979.

[74] J. Buchmann, L. C. C. García, E. Dahmen, M. Döring, and E. Klintsevich, "CMSS—An improved Merkle signature scheme," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 4329. Berlin, Germany: Springer-Verlag, 2006, pp. 349–363.

[75] J. Buchmann, E. Dahmen, E. Klintsevich, K. Okeya, and C. Vuillaume, "Merkle signatures with virtually unlimited signature capacity," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 4521. Berlin, Germany: Springer-Verlag, 2007, pp. 31–45.

[76] J. Buchmann, E. Dahmen, and A. Hülsing, "XMSS—A practical forward secure signature scheme based on minimal security assumptions," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 7071. Berlin, Germany: Springer-Verlag, 2011, pp. 117–129. [Online]. Available: https://huelsing.wordpress.com/publications/

[77] A. Hülsing, L. Rausch, and J. Buchmann, "Optimal parameters for XMSS," in *Security Engineering and Intelligence Informatics* (Lecture Notes in Computer Science), vol. 8128. Berlin, Germany: Springer-Verlag, 2013, pp. 194–208.

[78] A. Hülsing, "WOTS+ shorter signatures for hash-based signature schemes," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 7918. Berlin, Germany: Springer-Verlag, 2013, pp. 173–188.

[79] A. Hülsing, D. Butin, S. Gazdag, J. Rijneveld and A. Mohaisen. (2018). *RFC 8391—XMSS: EXtended Merkle Signature Scheme*. IETF. [Online]. Available: https://tools.ietf.org

[80] D. McGrew, M. Curcio, and S. Fluhrer. (2019). *RFC 8554—Leighton-Micali Hash-Based Signatures*. IETF. [Online]. Available: https://tools.ietf.org

[81] D. McGrew, P. Kampanakis, S. Fluhrer, S.-L. Gazdag, D. Butin, and J. Buchmann, "State management for hash-based signatures," in *Security Standardisation Research* (Lecture Notes in Computer Science), vol. 10074. Berlin, Germany: Springer-Verlag, 2016, pp. 244–260.

[82] A. Karina, D. S. de Oliveira, and J. Lopez, "An efficient software implementation of the hash-based signature scheme MSS and its variants," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 9230. Berlin, Germany: Springer-Verlag, 2015, pp. 366–383.

[83] A. Hülsing, J. Rijneveld, and F. Song, "Mitigating multi-target attacks in hash-based signatures," in *Public-Key Cryptography* (Lecture Notes in Computer Science), vol. 9614. Berlin, Germany: Springer-Verlag, 2016, pp. 387–416.

[84] S. Rohde, T. Eisenbarth, E. Dahmen, J. Buchmann, and C. Paar, "Fast hash-based signatures on constrained devices," in *Smart Card Research and Advanced Applications* (Lecture Notes in Computer Science), vol. 518. Berlin, Germany: Springer-Verlag, 2008, pp. 104–117.

[85] D. J. Bernstein *et al.*, "Wilcox-O'Hearn, SPHINCS: Practical stateless hash-based singatures," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 9056. Berlin, Germany: Springer-Verlag, 2015, pp. 368–397.

[86] R. McEliece, "A public-key cryptosystem based on algebraic coding theory," DSN Progress Report Jet Propulsion Laboratories, Pasadena, CA, USA, Tech. Rep. 42-44, 1978.

[87] N. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 2248. Berlin, Germany: Springer-Verlag, 2001, pp. 157–174.

[88] D. J. Bernstein, T. Chou, and P. Schwabe, "McBits: Fast constant-time code-based cryptography," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 8086. Berlin, Germany: Springer-Verlag, 2013, pp. 250–272.

[89] G. Landais and N. Sendrier, "Implementing CFS," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 7668. Berlin, Germany: Springer-Verlag, 2012, pp. 474–488.

[90] P. Gaborit, O. Ruatta, J. Schrek, and G. Zemor, "Ranksign: An efficient signature algorithm based on the rank metric (extended version on arxiv)," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 8772. Berlin, Germany: Springer-Verlag, 2014, pp. 88–107.

[91] J.-C. Faugere, V. Gauthier, A. Otmani, L. Perret, and J.-P. Tillich, "A distinguisher for high rate McEliece cryptosystems," IACR Cryptol. ePrint Arch., Tech. Rep. 2010/331, 2010.

[92] T. Debris-Alazard and J.-P. Tillich, "A polynomial attack on a NIST proposal: Ranksign, a code-based signature in rank metric," IACR Cryptol. ePrint Arch., Tech. Rep., Apr. 2018.

[93] T. Debris-Alazard, N. Sendrier, and J.-P. Tillich, "Wave: A new family of trapdoor one-way preimage sampleable functions based on codes," 2018, *arXiv:1810.07554*.

[94] P. S. L. M. Barreto and E. Persichetti, "Cryptanalysis of the wave signature scheme," IACR Cryptol. ePrint Arch., Tech. Rep. 2018/1111, 2018.

[95] Y. Song, X. Huang, Y. Mu, and W. Wu, "A new code-based signature scheme with shorter public key," IACR Cryptol. ePrint Arch., Tech. Rep. 2019/053, 2019.

[96] K. Xagawa, "Cryptanalysis of a new code-based signature scheme with shorter public key," Cryptol. ePrint Archive, Tech. Rep. 2019/120, 2019.
[97] N. Aragon, O. Blazy, P. Gaborit, A. Hauteville, and G. Zemorz, "Durandal: A rank metric based signature scheme," IACR Cryptol. ePrint Arch., Tech. Rep. 2018/1192, 2018.
[98] J. F. Biasse, D. Jao, and A. Sankar, "A quantum algorithm for computing isogenies between supersingular elliptic curves," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 8885. Berlin, Germany: Springer-Verlag, 2014, pp. 428–442.
[99] S. D. Galbraith, P. Christophe, and J. Silva, "Identification protocols and signature schemes based on supersingular isogeny problems," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 10624. Berlin, Germany: Springer-Verlag, 2017, pp. 3–33.
[100] L. D. Feo and S. D. Galbraith, "SeaSign: Compact isogeny signatures from class group actions," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 11478. Berlin, Germany: Springer-Verlag, 2019, pp. 759–789.
[101] A. Stolbunov, "Cryptographic schemes based on isogenies," M.S. thesis, Inf. Technol., Math. Elect. Eng., Norwegian Univ. Sci. Technol., 2012.
[102] D. Unruh, "Non-interactive zero-knowledge proofs in the quantum random Oracle model," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 9057. Berlin, Germany: Springer-Verlag, 2015, pp. 755–784.
[103] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "CSIDH: An efficient post-quantum commutative group action," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 11274. Berlin, Germany: Springer-Verlag, 2018, pp. 395–427.
[104] V. Lyubashevsky, "Fiat-Shamir with aborts: Applications to lattice and factoringbased signatures," *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 5912. Berlin, Germany: Springer-Verlag, 2019, pp. 598–616.
[105] L. G. Bruinderink, A. Hülsing, T. Lange, and Y. Yarom, "Flush, Gauss, and reload: A cache attack on the BLISS lattice-based signature scheme," in *Proc. Int. Workshop Cryptogr. Hardw. Embedded Syst.*, 2016, pp. 323–345, 2016.
[106] P. Pessl, L. G. Bruinderink, and Y. Yarom, "To BLISS-B or not to be: Attacking strongSwan's implementation of post-quantum signatures," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1843–1855.
[107] T. Espitau, P.-A. Fouque, B. Gérard, and M. Tibouchi, "Side-channel attacks on BLISS lattice-based signatures: Exploiting branch tracing against strongSwan and electromagnetic emanations in microcontrollers," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1857–1874.
[108] P. Ravi, M. P. Jhanwar, J. Howe, A. Chattopadhyay, and S. Bhasin, "Side-channel assisted existential forgery attack on dilithium—A NIST PQC candidate," IACR Cryptol. ePrint Arch., Tech. Rep. 2018: 821, 2018.
[109] M. J. Kannwischer, A. Genét, D. Butin, J. Krämer, and J. Buchmann, "Differential power analysis of XMSS and SPHINCS," in *Constructive Side-Channel Analysis and Secure Design* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2018, pp. 168–188.
[110] T. B. R. Steinwandt and W. Geiselmann, "A theoretical DPA based cryptanalysis of the NESSIE candidates FLASH and SFLASH," in *Proc. ISC*, 2001, pp. 280–293.
[111] A. Park, K.-A. Shim, N. Koo, and D.-G. Han, "Side-channel attacks on post-quantum signature schemes based on multivariate quadratic equations: Rainbow and UOV," in *Proc. IACR Trans. Cryptograph. Hardw. Embedded Syst.*, Aug. 2018, pp. 500–523.
[112] H. Yi and W. Li, "On the importance of checking multivariate public key cryptography for side-channel attacks: The case of enTTS scheme," *Comput. J.*, vol. 60, no. 8, pp. 1197–1209, Aug. 2017.
[113] H. Yi and Z. Nie, "Side-channel security analysis of UOV signature for cloud-based Internet of Things," *Future Gener. Comput. Syst.*, vol. 86, pp. 704–708, Sep. 2018.
[114] T. Eisenbarth, T. Güneysu, S. Heyse, and C. Paar, "MicroEliece: McEliece for embedded devices," in *Cryptographic Hardware and Embedded Systems* (Lecture Notes in Computer Science), vol. 5747. Berlin, Germany: Springer-Verlag, 2009, pp. 49–64.
[115] S. Heyse, A. Moradi, and C. Paar, "Practical power analysis attacks on software implementations of McEliece," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 6061. Berlin, Germany: Springer-Verlag, 2010, pp. 108–125.
[116] H. G. Molter, M. Stöttinger, A. Shoufan, and F. Strenzke, "A simple power analysis attack on a Mceliece cryptoprocessor," *J. Cryptograph. Eng.*, vol. 1, no. 1, pp. 29–36, Apr. 2011.
[117] I. V. Maurich and T. Guneysu, "Lightweight code-based cryptography: QC-MDPC Mceliece encryption on reconfigurable devices," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, 2014, pp. 1–6.
[118] I. von Maurich and T. Güneysu, "Towards side-channel resistant implementations of QC-MDPC McEliece encryption on constrained devices," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 8772. Berlin, Germany: Springer-Verlag, 2014, pp. 266–282.
[119] C. Chen, T. Eisenbarth, I. von Maurich, and R. Steinwandt, "Differential power analysis of a McEliece cryptosystem," IACR Cryptol. ePrint Arch., Tech. Rep. 2014/534, 2014. [Online]. Available: https://eprint.iacr.org
[120] N. Bindel, J. Buchmann, and J. Kramer, "Lattice-based signature schemes and their sensitivity to fault attacks," in *Proc. Workshop Fault Diagnosis Tolerance Cryptogr. (FDTC)*, Aug. 2016, pp. 63–77.
[121] T. Espitau, P.-A. Fouque, B. Gérard, and M. Tibouchi, "Loop-abort faults on lattice-based signature schemes and key exchange protocols," *IEEE Trans. Comput.*, vol. 67, no. 11, pp. 1535–1549, Nov. 2018.
[122] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, and W. Whyte, "Practical signatures from the partial Fourier recovery problem," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 8479. Heidelberg, Germany: Springer, 2014, pp. 476–493.
[123] L. G. Bruinderink and P. Pessl, "Differential fault attacks on deterministic lattice signatures," *IACR Trans. Cryptogr. Hardw. Embedded Syst.*, vol. 2018, no. 3, pp. 21–43, 2018.
[124] L. Castelnovi, A. Martinelli, and T. Prest, "Grafting trees: A fault attack against the SPHINCS framework," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2018, pp. 165–184.
[125] A. Genêt, M. J. Kannwischer, H. Pelletier, and A. McLauchlan, "Practical fault injection attacks on SPHINCS," IACR Cryptol. ePrint Arch., Tech. Rep. 2018:674, 2018.
[126] Y. Hashimoto, T. Takagi, and K. Sakurai, "General fault attacks on multivariate public key cryptosystems," in *Post-Quantum Cryptography* (Lecture Notes in Computer Science), vol. 7071. Berlin, Germany: Springer-Verlag, 2011, pp. 1–18.
[127] K.-A. Shim and N. Koo, "Algebraic fault analysis of UOV and rainbow with the leakage of random vinegar values," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2429–2439, 2020.
[128] J. A. Halderman *et al.*, "Lest we remember: Cold boot attacks on encryption keys," *Proc. USENIX*, 2008, pp. 45–60.
[129] D. Dachman-Soled, H. Gong, M. Kulkarni, and A. Shahverdi, "Partial key exposure in ring-LWE-based cryptosystems: Attacks and resilience," IACR Cryptol. ePrint Arch., Tech. Rep. 2018/1068, 2018.
[130] M. R. Albrecht, A. Deo, and K. G. Paterson, "Cold boot attacks on ring and module LWE keys under the NTT," in *Proc. IACR Trans. Cryptograph. Hardw. Embedded Syst.*, Aug. 2018, pp. 173–213.
[131] R. Villanueva-Polanco, "Cold boot attacks on bliss," in *Progress in Cryptology* (Lecture Notes in Computer Science), vol. 11774. Berlin, Germany: Springer-Verlag, 2019, pp. 40–61.
[132] R Villanueva-Polanco, "Cold boot attacks on LUOV," *Appl. Sci.*, vol. 10, no. 12, p. 4106, 2020.
[133] D. J. Bernstein, "Curve25519: New Diffie–Hellman speed records," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 3958. Berlin, Germany: Springer-Verlag, 2006, pp. 207–228.
[134] M. Düll *et al.*, "High-speed curve25519 on 8-bit, 16-bit, and 32-bit microcontrollers," *Des., Codes Cryptogr.*, vol. 77, nos. 2–3, pp. 493–514, Dec. 2015.

Kyung-Ah Shim (Member, IEEE) received the Ph.D. degree in mathematics from Ewha Womans University, Seoul, South Korea.

She is currently a Senior Researcher at the National Institute for Mathematical Sciences. Her research interests include public-key cryptography, post-quantum cryptography, cryptographic protocols, and information security.