SoK: How (not) to Design and Implement Post-Quantum Cryptography

James Howe[1] , Thomas Prest[1] , and Daniel Apon[2]

[1] PQShield, Oxford, UK.
{james.howe,thomas.prest}@pqshield.com
[2] National Institute of Standards and Technology, USA.
daniel.apon@nist.gov

Abstract Post-quantum cryptography has known a Cambrian explosion in the last decade. What started as a very theoretical and mathematical area has now evolved into a sprawling research field, complete with side-channel resistant embedded implementations, large scale deployment tests and standardization efforts. This study systematizes the current state of knowledge on post-quantum cryptography. Compared to existing studies, we adopt a transversal point of view and center our study around three areas: (i) paradigms, (ii) implementation, (iii) deployment. Our point of view allows to cast almost all classical and post-quantum schemes into just a few paradigms. We highlight trends, common methodologies, and pitfalls to look for and recurrent challenges.

1 Introduction

Since Shor's discovery of polynomial-time quantum algorithms for the factoring and discrete logarithm problems, researchers have looked at ways to manage the potential advent of large-scale quantum computers, a prospect which has become much more tangible of late. The proposed solutions are cryptographic schemes based on problems assumed to be resistant to quantum computers, such as those related to lattices or hash functions. *Post-quantum cryptography* (PQC) is an umbrella term that encompasses the design, implementation, and integration of these schemes. This document is a Systematization of Knowledge (SoK) on this diverse and progressive topic.

We have made two editorial choices. First, an exhaustive SoK on PQC could span several books, so we limited our study to signatures and key-establishment schemes, as these are the backbone of the immense majority of protocols. This study will not cover more advanced functionalities such as homomorphic encryption schemes, threshold cryptography, et cetera.

Second, most surveys to-date are either (i) organized around each *family* [BBD09] – (a) lattices, (b) codes, (c) multivariate equations, (d) isogenies, (e) hash and one-way functions – or (ii) focused on a single family [Pei15; Feo17]. Our study instead adopts a transversal approach, and is organized as follows: (a) paradigms, (b) implementation, and (c) deployment. We see several advantages to this approach:

- Compared to previous surveys, it provides a new point of view that abstracts away much of the mathematical complexity of each family, and instead emphasizes common paradigms, methodologies, and threat models.
- In practice, there are challenges that have been solved by one family of scheme and not another. This document's structure makes it easy to highlight *what* these problems are, and *how* they were solved. Consequently, it aims to provide specific direction for research; i.e., (i) problems to solve, and (ii) general methodologies to solve them.
- If a new family of hardness assumptions emerges – as isogeny-based cryptography recently has – we hope the guidelines in this document will provide a framework to safely design, implement, and deploy schemes based on it.

1.1 Our Observations

A first observation is that almost all post-quantum (PQ) schemes fit into one of four paradigms: Fiat-Shamir signatures, Hash-then-sign, Diffie-Hellman key-exchange, and encryption. Moreover, the same few properties (e.g., homomorphism) and folklore tricks are leveraged again and again.

Successful schemes do not hesitate to *bend* paradigms in order to preserve the security proof *and* the underlying assumption. In contrast, forcing an assumption into a paradigm may weaken the assumption, the security proof, or both.

Our second observation is that PQC has and will add significant implementation complexities compared to their classical counterparts. These complexities have led to an abundance of new challenges which range from larger keys, securely sampling from non-uniform distributions, decryption failures, and a re-examining of constant/isochronous runtime and more. We also find some PQ schemes are significantly more amenable to implementations in hardware, software, their efficiencies with masking, which then translates into how they perform in various use-cases.

Our third observation is that all real-world efforts to deploy post-quantum cryptography will have to contend with new, unique problems. They may require a diverse combination of computational assumptions *woven together* into a single hybrid scheme. They may require special attention to *physical management* of sensitive state. And they have very unbalanced performance profiles, requiring distinct solutions for different application scenarios.

2 The Raw Material: Hard Problems

We first present the raw material from which cryptographic schemes are made: hard problems (and the assumption that they are indeed hard to solve). Although there exists a myriad of post-quantum hard problems, many of them share similarities that we will highlight.

2.1 Baseline: Problems that are not Post-Quantum

We first present problems that are classically hard but quantumly easy. The first family of problems relates to the discrete logarithm in finite groups; that is, the Discrete Logarithm (DLOG) problem, the Decisional Diffie-Hellman (DDH), and the Computational Diffie-Hellman (CDH) problems.

Definition 1 (DLOG/DDH/CDH). *Let $\mathbb{G}$ be a cyclic group of generator g. The discrete logarithm problem (DLOG) and the decisional/computational Diffie-Hellman problems (DDH/CDH) are defined as follows:*

- **DLOG:** *Given g^a for a random $a \in |\mathbb{G}|$, find a.*
- **DDH:** *Given g^a, g^b and g^c for random $a, b \in |\mathbb{G}|$, determine if $c = ab$.*
- **CDH:** *Given g^a, g^b for random $a, b \in |\mathbb{G}|$, compute g^{ab}.*

In cryptography, $\mathbb{G}$ is usually the ring $\mathbb{Z}_p$ for a large prime p, or the group of rational points of an elliptic curve. The following algebraic relations are extremely useful to build cryptosystems, for example Schnorr signatures [Sch90] use (1) and (2) whereas the Diffie-Hellman key-exchange [DH76] uses (2):

$$g^a \cdot g^b = g^{a+b}, \tag{1}$$

$$(g^a)^b = \left(g^b\right)^a = g^{ab}. \tag{2}$$

The second family of problems relates to factoring.

Definition 2 (RSA and Factoring). *Let p, q be large prime integers, $N = p \cdot q$ and e be an integer.*

- *Factoring: Given N, find p and q.*
- *RSA: Efficiently invert the following function over a non-negligible fraction of its inputs:*

$$x \in \mathbb{Z}_N \mapsto x^e \bmod N. \tag{3}$$

For adequate parameters, the problems in Def. 1 and 2 are believed hard to solve by classical computers. However, Shor has shown that they are solvable in polynomial time by a quantum computer [Sho94]. As these problems underlie virtually all current public-key cryptosystems, Shor's discovery motivated the following research for alternative, quantum-safe problems.

2.2 Problems on Lattices

The most well-known problems based on lattices are Learning With Errors (LWE) [Reg05; LPR10], Short Integer Solution (SIS) [Ajt96; LS15] and "NTRU" [HPS98].

Definition 3 (SIS, LWE, and NTRU). *Given a monic polynomial $\phi \in \mathbb{Z}[x]$ and an integer modulus q, let $\mathcal{R} = \mathbb{Z}_q[x]/(\phi(x))$ be a ring, and $\mathbf{A} \in \mathcal{R}^{n \times m}$ be uniformly random. The Short Integer Solution (SIS) and Learning with Errors (LWE) problems are defined as follows:*

- *SIS: Find a short nonzero $\mathbf{v} \in \mathcal{R}^m$ such that $\mathbf{A}\mathbf{v} = 0$.*
- *LWE: Let $\mathbf{b} = \mathbf{A}^t \mathbf{s} + \mathbf{e}$, where $\mathbf{s} \in \mathcal{R}^n$ and $\mathbf{e} \in \mathcal{R}^m$ are sampled from the 'secret' distribution and 'error' distribution, respectively.*
  - *Decision: Distinguish $(\mathbf{A}, \mathbf{b})$ from uniform.*
  - *Search: Find $\mathbf{s}$.*
- *NTRU: Let $h = f/g \in \mathcal{R}$, where $f, g \in \mathcal{R}$ are 'short.' Given h, find f, g.*

SIS, LWE, and NTRU exist in many variants [Reg05; LPR10; LS15; PP19], obtained by changing $\mathcal{R}, n, m$, or the error distributions. To give a rough idea, a common choice is to take $\mathcal{R} = \mathbb{Z}_q[x]/(x^d + 1)$, with d a power-of-two, and n, m such that nd and md are in the order of magnitude of 1000. The versatility of SIS, LWE, and NTRU is a blessing and a curse for scheme designers, as it offers freedom but also makes it easy to select insecure parameters [Pei16].

We are not aware of closed formulae for the hardness of SIS, LWE, and NTRU. However, the most common way to attack these problems is to interpret them as lattice problems, then run lattice reduction algorithms [APS15; ACD+18]. For example, the BKZ algorithm [SE94] with a blocksize $B \le nd$ is estimated to solve these in time $\tilde{O}(2^{0.292 \cdot B})$ classically [BDG+16], and $\tilde{O}(2^{0.265 \cdot B})$ quantumly [LMP15] via Grover's algorithm.

2.3 Problems on Codes

Error-correcting codes provide some of the oldest post-quantum cryptosystems. These usually rely on two problems:

- The Syndrome Decoding (SD) problem, see Def. 4.
- Hardness of distinguishing a code in a family $\mathcal{F}$ from a pseudorandom one.

We first present SD. Note that it is similar to SIS (Def. 3).

Definition 4 (SD). *Given a matrix $\mathbf{H} \in \mathbb{F}_2^{k \times n}$ and a syndrome $\mathbf{s} \in \mathbb{F}_2^k$, the Syndrom Decoding (SD) problem is to find $\mathbf{e} \in \mathbb{F}_2^n$ of Hamming weight w such that $\mathbf{H}\mathbf{e} = \mathbf{s}$.*

Since 1962, several algorithms have been presented to solve the SD problem, their complexity gradually improving from $2^{0.1207n}$ [Pra62] to $2^{0.0885n}$ [BM18]. These algorithms share similarities in their designs and [TS16] recently showed that when $w = o(n)$, they all have the same asymptotic complexity $\approx 2^{w \log_2(n/k)}$. For many of these algorithms, quantum variants have been proposed. They achieve quantum complexities that are essentially square roots of the classical ones, by using either Grover or quantum walks.

The second problem is not as clearly defined, as it is rather a class of problems. Informally, it states that for a given family $\mathcal{C} = (C_i)_i$ of codes, a matrix $\mathbf{G}$ generating a code $C_i \in \mathcal{C}$ is hard to distinguish from a random matrix. For example, two variants of BIKE [ABB+19] assume that it is hard to distinguish from random either of these *quasi-cyclic codes* (or QC codes):

$$h_0/h_1 \tag{4}$$
$$g, g \cdot h_0 + h_1 \tag{5}$$

where $g, h_0, h_1 \in \mathbb{F}_2[x]/(x^r - 1)$, g is random and h_0, h_1 have small Hamming weight. Note that (4) and (5) are reminiscent of NTRU and (ring-)LWE, respectively (see Def. 3). Hence all the lattice problems we have defined have code counterparts, and reciprocally. Besides the QC codes of (4)-(5), another popular family of codes are Goppa codes [McE78; CFS01; BCL+19a].

2.4   Problems on Multivariate Systems

The third family of problems is based on multivariate systems. In practice, only multivariate *quadratics* (i.e., of degree 2) are used. They are the Multivariate Quadratic (MQ) and Extended Isomorphism of Polynomials (EIP) problems.

Definition 5 (MQ and EIP). *Let $\mathbb{F}$ be a finite field. Let $\mathbf{F} : \mathbb{F}^n \to \mathbb{F}^m$ of the form $\mathbf{F}(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$, where each $f_i : \mathbb{F}^n \to \mathbb{F}$ is a multivariate polynomial of degree at most 2 in the coefficients of $\mathbf{x}$.*

- **MQ:** *Given $\mathbf{y} \in \mathbb{F}^m$ and the map $\mathbf{F}$:*
  - **Decision:** *Is there an $\mathbf{x}$ such that $\mathbf{F}(\mathbf{x}) = \mathbf{y}$?*
  - **Search:** *Find $\mathbf{x}$ such that $\mathbf{F}(\mathbf{x}) = \mathbf{y}$.*
- **EIP:** *Let $\mathbf{S} : \mathbb{F}^n \to \mathbb{F}^n$ and $\mathbf{T} : \mathbb{F}^m \to \mathbb{F}^m$ be uniformly random affine maps. Given $\mathbf{P} = \mathbf{S} \circ \mathbf{F} \circ \mathbf{T}$ and the promise that the map $\mathbf{F}$ is in a publicly known set $\mathcal{F}$, find $\mathbf{F}$.*

Note that MQ is solvable in polynomial time for $m^2 = O(n)$ or $n^2 = O(m)$; therefore this problem is more interesting when $n = \Theta(m)$, which we assume henceforth. Also note that EIP can be parameterized by the set $\mathcal{F}$ to which the secret map $\mathbf{F}$ belongs. For example, the Unbalanced Oil and Vinegar (UOV) and Hidden Field Equation (HFEv) problems, used by Rainbow [DCP+19] and GeMSS [CFM+19] respectively, are instantiations of the EIP "framework".

Algorithms solving MQ or EIP include F4/F5 [Fau02], XL [CKP+00; Die04] or Crossbred [JV17]. The best ones [YC04; BFP12; JV17] combine algebraic techniques – e.g., solving Gröbner bases – with exhaustive search, which can be sped up using Grover's algorithm in the quantum setting, see e.g. [BY17]. The asymptotic complexities of these algorithms are clearly exponential in n, but we did not find simple formulae to express them (either classically or quantumly), except for special cases ($q = 2$ and $n = m$) which do not accurately reflect concrete instantiations such as the signature schemes Rainbow [DCP+19] and MQDSS [SCH+19].

2.5   Problems on One-Way and Hash Functions

The most peculiar family of PQ problems relates to properties of (generic) one-way and hash functions. These problems are algebraically unstructured, which is desirable security-wise, but tends to imply more inefficient schemes.

Definition 6 (Problems on hash functions). *Let $H : X \to Y$ be a function, where $Y = 2^n$.*

- **Preimage:** *Given $y \in Y$, find $x \in X$ such that $H(x) = y$.*
- **Second preimage:** *Given $x_1 \in X$, find $x_2 \neq x_1$ such that $H(x_1) = H(x_2)$.*
- **Collision:** *Find $x_1 \neq x_2$ such that $H(x_1) = H(x_2)$.*

The best classical algorithm against (second) preimage is exhaustive search, hence a complexity $O(2^n)$. Grover's famous quantum algorithm [Gro96] performs this search with a quadratic speed-up, hence a complexity $O(2^{n/2})$. Regarding collision, the best classical algorithm is the birthday attack with a complexity $O(2^{n/2})$, and (disputed) results place the complexity of the best quantum attack between $O(2^{2n/5})$ [CNS17] and $\Theta(2^{n/3})$ [Zha15].

2.6   Problems on Isogenies

Isogeny problems provide a higher-level twist on Def. 1. Elliptic curve cryptography posits that when given g and g^a, with g being a point on an elliptic curve E, it is hard to recover a. Similarly, isogeny-based cryptography posits that given elliptic curves E and E' over $\mathbb{F}_{p^2}$, it is hard to find a surjective group morphism (or *isogeny*, in this context) $\phi : E \to E'$.

Isogeny-based cryptography is a fast-moving field. Elliptic curves can be ordinary ($E[p] \simeq \mathbb{Z}_p$) or supersingular ($E[p] \simeq \{0\}$). Recall that the torsion subgroup $E[n]$ is the kernel of the map $P \in E \mapsto [n]P$. Most isogeny schemes work with supersingular curves, which parameters scale better. Two problems (or variations thereof) have emerged. Def. 7 provides simplified descriptions of them.

Definition 7 (Problems on isogenies). *We define the Supersingular Isogeny Diffie-Hellman (SIDH) and Commutative SIDH (CSIDH) problems as follows:*

- **SIDH:** *Given two elliptic curves E, E_A and the value of an isogeny $\phi : E \to E_A$ on $E[\ell^e]$, find ϕ.*
- **CSIDH:** *Given two elliptic curves E, E_A, find an efficiently computable isogeny $\phi \in \mathcal{C\ell}(\mathcal{O})$ s.t. $E_A = \phi \cdot E$, where $\mathcal{C\ell}(\mathcal{O})$ is the class group of $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.*

Note that the CSIDH problem adapts DDH to the isogeny setting, and one can similarly adapt CDH (see Def. 1). Note that both problems are quantumly equivalent [GPS+18], whereas CDH and DDH are not known to be classically equivalent, except in special cases.

For SIDH, the best classical attack is via a claw-finding algorithm due to van Oorschot-Wiener [vW99]. Surprisingly, a recent result [JS19] shows that the best known quantum attack performs *worse* than [vW99]. The hardness of CSIDH reduces to solving a hidden shift problem, for which Kuperberg proposed quantum sub-exponential algorithms [Kup05; Kup13]. The actual quantum security of CSIDH is still being debated [BS20; Pei20].

2.7   Summary of Problems

Fig. 1 summarizes the classical and quantum hardness estimates of the problems we presented. Quantum estimates are particularly prone to change, notably due to (a) the lack of clear consensus on the cost of quantum memory, (b) the prospect of future algorithmic improvements.

Figure 1: Classical and quantum hardness of some problems.

Problem	Factoring /DLOG	SIS /LWE	SD	MQ	EIP	SIDH	CSIDH	(Second) Preimage	Collision
Classical	$e^{\tilde{O}\left((\log p)^{1/3}\right)}$	$2^{0.292 \cdot B}$	$2^{0.0885 \cdot n}$	?	?	$O(p^{1/4})$	$O(p^{1/4})$	$O(2^n)$	$O(2^{n/2})$
Quantum	poly(N)	$2^{0.265 \cdot B}$	$2^{0.05804 \cdot n}$	?	?	$O(p^{1/4})$	$e^{\tilde{O}\left(\sqrt{\log p}\right)}$	$O(2^{n/2})$	$\Theta(2^{n/3})$

3   Paradigms are Guidelines, not Panaceas

In the classical world, there are two paradigms for signing:

- Fiat-Shamir (FS) [FS87], proven in the random oracle model (ROM) by [PS96]. One example is Schnorr signatures and (EC)DSA.
- Hash-then-sign. The most prominent formalization of this paradigm is the Full Domain Hash [BR93] (FDH), proven in the ROM by [BR96; Cor00]. Numerous instantiations exist, such as RSA-PSS and Rabin signatures.

There are also two paradigms for key establishment:

- Public-key encryption, like El Gamal [ElG85] or RSA [RSA78].
- Diffie-Hellman (DH) key-exchange [DH76].

At a conceptual level, this section shows that most PQ signature or key establishment schemes can be cast under one of these four paradigms. This is summarized by Table 1, which also provides us with two open questions:

(Q1) Can we have isogeny-based Hash-then-sign schemes?
(Q2) Can we have secure and efficient multivariate key establishment schemes?

The prospect that we will have practical key establishment schemes based on symmetric primitives only seems unlikely, see [BM17]. For (Q1) and (Q2), we hope that the guidelines provided in this section will help to answer them.

Table 1: Correspondence between post-quantum schemes and problems.

	Signature		Key Establishment	
	Hash-&-Sign	Fiat-Shamir	DH-style	PKE
Lattices	[PFH$^+$19; CGM19]	[LDK$^+$19; BAA$^+$19]	[DXL12; Pei14]	[SAB$^+$19; DKR$^+$19; ZCH$^+$19]
Codes	[DST19]	[Ste94; Vér96]	[AGL$^+$10]	[BCL$^+$19a; ABB$^+$19]
Isogenies	?	[DG19; BKV19]	[JD11; DKS18; CLM$^+$18]	[JAC$^+$19]
Multivariate	[DCP$^+$19; CFM$^+$19]	[SCH$^+$19]	?	?
Symmetric	[HBD$^+$19]	[ZCD$^+$19; Bd20]	-	-

Our main takeaway is that scheme designers should treat paradigms as guidelines. In particular, a fruitful approach is to weaken some properties, as long as the final scheme achieves meaningful security notions. For example:

- Efficient PQ variants of the FDH framework discards trapdoor permutations for weakened definitions, which suffice for signatures, see Sec. 3.4.
- *Fiat-Shamir with Aborts* changes the protocol flow and may only prove knowledge of an approximate solution. This suffices for signatures, see Sec. 3.1

On the other hand, fitting a problem into a predefined paradigm is an interesting first step, but may limit the efficiency of the scheme, a limitation that is usually resolved by slight paradigm tweaks. Examples are rigid adaptations of:

- DH with lattices [GKR$^+$20] and isogenies [DKS18], see Sec. 3.5.
- FDH with codes [CFS01] or lattices [HHP$^+$03], see Sec. 3.4.

3.1 Schnorr Signatures over Lattices

Fig. 2 recalls the structure of an identification scheme, or ID scheme. Any ID scheme can be converted into a signature via the Fiat-Shamir transform [FS87]. A efficient ID scheme is Schnorr's 3-move protocol [Sch90]. It instantiates Fig. 2 with the parameters in Table 2 (column 2). It also requires additive and multiplicative properties similar to (1)-(2).
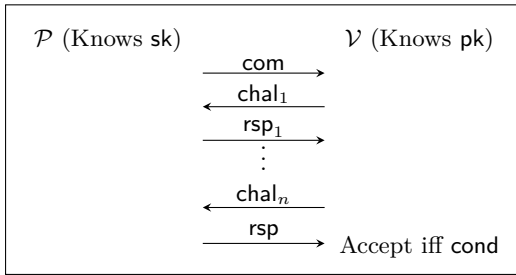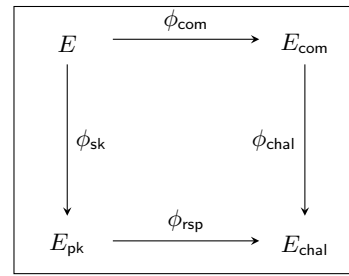

Figure 2: A $(2n + 1)$-move ID scheme.

Figure 3: SQISign.

Fortunately, lattice and code problems do have properties similar to (1)-(2). An early attempt to propose Schnorr lattice signatures is NSS [HPS01], which was broken by statistical attacks [GJS$^+$01]. The high-level explanation is that the ID scheme in NSS did not satisfy the *honest verifier zero-knowledge* (HVZK) property. Each transcript leaked a bit of information about sk, which [GJS$^+$01] exploited to recover sk. This was fixed by Lyubashevsky's scheme [Lyu09], by giving the prover the possibility to abort the protocol with a probability chosen to factor out the dependency to sk from the signature. This changes the flow of the ID scheme, but allows to prove HVZK. It is also invisible to the verifier as the signer will simply restart the signing procedure in case of an abort. An example instantiation is shown in Table 2 (column 3).

Table 2: Instantiations of Schnorr Signatures.

Element	Schnorr	Lyubashevsky (w/ LWE)
sk	Uniform x	Short $(\mathbf{s}_1, \mathbf{s}_2)$
pk	$g, h = g^x$	$\mathbf{A}, \mathbf{t} = \mathbf{A} \cdot \mathbf{s}_1 + \mathbf{s}_2$
com	g^r for uniform r	$\mathbf{A} \cdot \mathbf{r}_1 + \mathbf{r}_2$ for short $(\mathbf{r}_1, \mathbf{r}_2)$
chal	Uniform c	Short c
rsp	$r - cx$	$(\mathbf{z}_1, \mathbf{z}_2) = (\mathbf{r}_1 - c\mathbf{s}_1, \mathbf{r}_2 - c\mathbf{s}_2)$
cond	com $= g^{\mathsf{rsp}} \cdot h^c$	$(\mathsf{com} = \mathbf{A}\mathbf{z}_1 + \mathbf{z}_2 - c\mathbf{t}) \wedge ((\mathbf{z}_i)_i$ short$)$
Abort?	No	Yes

On the other hand, properties of lattices enable specific tricks tailored to this setting. For example, for LWE, least significant bits (LSBs) do not really matter. Let $\lfloor \mathbf{u} \rfloor_b$ be a lossy representation of $\mathbf{u}$ that discards the b LSBs for each coefficient of $\mathbf{u}$. Finding a search-LWE solution

$(\mathbf{s}_1, \mathbf{s}_2)$ for $(\mathbf{A}, \lfloor \mathbf{t} \rfloor_b)$ implies a solution $(\mathbf{s}_1, \mathbf{s}_2')$ for $(\mathbf{A}, \mathbf{t})$, with $\|\mathbf{s}_2 - \mathbf{s}_2'\|_\infty \leq 2^b$. This indicates that, as long as b is not too large, LSBs are not too important for LWE.

This intuition was formalized by [BG14], who show that dropping $\mathbf{z}_2$ and checking only the high bits of com allowed to reduce the signature size by about 2, for essentially the same (provable) security guarantees. Similarly, [GLP12] applied this idea to reduce the public key size. The idea was refined by Dilithium [LDK+19]. However, qTESLA [BAA+19] shows what can go wrong when applying this idea without checking that the security proof is preserved (in this case, soundness), as it was shown to be completely insecure.

Remark 1. The Schnorr-Lyubashevsky approach to signatures has recently been adapted to rank metric assumptions [GPT91] by the Durandal signature [ABG+19]. This naturally raises the question of whether tricks similar to [BG14; LDK+19] can be leveraged in this setting.

3.2   The SQISign Approach for Signatures

SQISign [DKL+20] applies the Fiat-Shamir transform to the ID scheme in Fig. 3. Given a public elliptic curve E, the private key is an isogeny $\phi_{sk} : E \to E_{pk}$ and the public key is E_{pk}. The prover commits to E_{com}, the challenge is a description of $\phi_{chal} : E_{com} \to E_{chal}$ and the response is an isogeny $\phi_{rsp} : E_{pk} \to E_{chal}$.

A valuable (and unique over isogeny-based signatures) feature of SQISign is the high soundness of each round, which makes it require only a single round. On the other hand, computing ϕ_{rsp} requires a lot of care in order for the HVZK property to hold, as shown by [DKL+20].

3.3   Beyond High Soundness Signatures

For the (vast majority of) problems that do not possess the (algebraic) properties needed to provide high soundness (thus few-rounds) Fiat-Shamir signatures, there still exist several tricks that enable efficient signatures. Scheme designers need to consider two things:

- The soundness error ϵ of the ID protocol is often too large. For example, Stern's protocols [Ste94] have $\epsilon \geq 1/2$. A solution is to repeat the protocol k times so that $\epsilon^k \leq 2^{-\lambda}$ for bit-security λ, but this is not a panacea.
- For some problems, a 3-move ID protocol may be less efficient than an n-move protocol with $n > 3$, or may even not be known.

We first elaborate on the first point. When the soundness ϵ of an ID protocol is too small, the protocol is repeated k times. Typically, all k iterations are performed in parallel (as opposed to sequentially). Parallel repetition is often *expected* by scheme designers to provide exponential soundness ϵ^k, however it is not the case in general; it is proven effective for 3-move *interactive* protocols, but counter-examples exist for higher-move protocols [BIN97; KZ20], see also remark 2.

Next, we present 3-moves and 5-moves ID schemes. As long as the underlying problem admits some linearity properties, one can build an ID scheme on it [BBS+18]. It is the case of all the schemes presented below.

PKP: A 5-move protocol based on the Permuted Kernel Problem (PKP) was proposed in [Sha90], with a soundness error of $\frac{p}{2p-2} \approx 1/2$, where p is the cardinal of the underlying ring. It was later instantiated by PKP-DSS [BFK+19].

MQ: The first ID schemes for MQ were proposed by [SSH11b]. A key idea of [SSH11b] was to use the polar form of $\mathbf{F}$: $\mathbf{G}(\mathbf{x}_1, \mathbf{x}_2) = \mathbf{F}(\mathbf{x}_1 + \mathbf{x}_2) - \mathbf{F}(\mathbf{x}_1) - \mathbf{F}(\mathbf{x}_2)$.

G is bilinear, and this was exploited to propose a 3-move protocol with soundness error $2/3$, and a 5-move one with soundness error $1/2 + 1/q \approx 1/2$. The latter protocol was instantiated by MQDSS [CHR$^+$16; SCH$^+$19] using the Fiat-Shamir transform.

<u>Codes:</u> Many code-based schemes derive from Stern's elegant protocols [Ste94; Ste96], which are based on the SD problem. Stern proposed a 3-move with soundness error $2/3$, and a 5-move protocol with soundness error $1/2$. The 3-move version was improved by Veron [Vér96] using the generator matrix of a code instead of its parity check matrix, hence it is often seen as a dual of Stern's protocol. However, most derivatives of Stern's protocol are based on the 5-move variant.

<u>Isogenies:</u> The CSIDH problem has been used to propose an ID scheme that, interestingly, is very similar to the well-known proof of knowledge for graph isomorphism. A useful trick used by SeaSign [DG19] is to use n public keys; this improves the soundness error down to $\frac{1}{n+1}$. CSI-Fish [BKV19] improved it to $\frac{1}{2n+1}$ by using symmetries specific to isogenies. Both schemes combine this with Merkle trees, which provides a trade-off between signing time and soundness error.

<u>Cut-and-choose:</u> This *generic* technique [KKW18] provides a trade-off between signing time and soundness error. It had been used by [Beu20] to provide MQ-based and PKP-based signatures that are more compact than MQDSS and PKP-DSS.

Remark 2. [KZ20] shows that for 5-round ID schemes with k parallel repetitions, the soundness error may be larger than ϵ^k, and provides a combinatorial attack against MQ-based schemes of [CHR$^+$16; SCH$^+$19] and the PKP-based scheme of [BFK$^+$19]. It warns that it might apply on 5-round variants of Stern's protocol. This shows that "intuitive" properties may not always be taken for granted.

3.4 Full Domain Hash signatures

Hash-then-sign schemes are among the most intuitive schemes at a high level. A standard way to construct them is via the *Full Domain Hash* (FDH) framework. We note $D(X)$ a distribution over a set X, $U(Y)$ the uniform distribution over a set Y and $\approx^s$ for statistical indistinguishability. Let $(\mathsf{sk}, \mathsf{pk})$ be an asymmetric keypair. Associate to it a pair $(f_\mathsf{pk}, g_\mathsf{sk})$ of efficiently computable functions $f_\mathsf{pk} : X \to Y$ (surjective) and $g_\mathsf{sk} : Y \to X$ (injective). Consider these properties:

(T1) Given only pk, f_pk is computationally hard to invert on (almost all of) Y.
(T2) $f_\mathsf{pk} \circ g_\mathsf{sk}$ is the identity over Y, and $X = Y$ (hence $f_\mathsf{pk}, g_\mathsf{sk}$ are permutations).
(T3) There exists a distribution $D(X)$ over X such that for almost any $y \in Y$:
$\{x \leftarrow D(X), \text{conditioned on } f_\mathsf{pk}(x) = y\} \approx^s \{x \leftarrow g_\mathsf{sk}(y)\}$.
(T4) $\{(x, y) | x \leftarrow D(X), y \leftarrow f_\mathsf{pk}(x)\} \approx^s \{(x, y) | y \leftarrow U(Y), x \leftarrow g_\mathsf{sk}(y)\}$.

We say that $(f_\mathsf{pk}, g_\mathsf{sk})$ is:

– A trapdoor permutation (TP) if it satisfies (T1), (T2);
– A trapdoor preimage sampleable function (TPSF) if it satisfies (T1), (T3);
– An average TPSF if it satisfies (T1), (T4).

Note that since $(T2) \Rightarrow (T3) \Rightarrow (T4)$[1], we have the following relation:

$$\text{TP} \Rightarrow \text{TPSF} \Rightarrow \text{Average TPSF}.$$

---

sign(msg, sk)

 − Compute $H(\mathsf{msg}) = y \in Y$;
 − Return $\mathsf{sig} \leftarrow f_{\mathsf{sk}}^{-1}(y)$.

verify(msg, pk, sig)

 − Accept iff $f_{\mathsf{pk}}(\mathsf{sig}) = H(\mathsf{msg})$.

Figure 4: The Full-Domain Hash (FDH) framework.

The FDH framework [BR93; BR96] allows, in its original form, to build hash-then-sign schemes from a hash function and a TP family as in Fig. 4. Note that the function of (3) induces a RSA-based TP if one knows the factorization $N = p \cdot q$.

Notable efforts at transposing the FDH framework in a post-quantum setting are the code-based schemes CFS [CFS01] and RankSign [GRS$^+$14]. The bit-security of CFS scales logarithmically in its parameters, making the scheme impractical, and [FGO$^+$13] showed that its security proof requires infeasible parameters. Similarly, [DT18] showed that RankSign's proposed parameters made the underlying problem easy, and that it required impractical parameters for the scheme to be secure. Both CFS and RankSign indicate that a rigid transposition of FDH framework (using TP) in a post-quantum setting seems highly non-trivial

Early lattice-based attempts such as GGHSign [GGH97] and NTRUSign [HHP$^+$03] instead chose to replace TPs with trapdoor one-way functions (with $|X| \gg |Y|$), that only satisfied (T1) and a *weakened* form of (T2) (dropping the requirement $X = Y$). In particular, this weaker form of (T2) no longer implied (T3). However, (T3) plays an important role in the original security proof of the FDH, which did no longer apply. More critically, each $y \in Y$ now admitted many $x_i \in X$ such that $f_{\mathsf{pk}}(x_i) = y$, and the x_i picked by the signing algorithm depended of sk. This dependency was exploited by learning attacks [NR06; DN12] to recover the signing key.

For lattices, the first real progress was done by [GPV08]. Its main contribution was to introduce TPSFs, to prove that they can be used to instantiate the FDH, and to propose provably secure lattice-based TPSFs. Several follow-up schemes have been proposed [MP12; DLP14], including Falcon [PFH$^+$19].

However, it is not known how to instantiate efficient TPSFs from code-based assumptions. Hence the work of [DST19; CD20] relaxed – again – this notion by proposing average TPSFs, showed that they suffice to instantiate the FDH framework, and proposed a signature scheme based on code-based average TPSFs, Wave. Interestingly, this idea was proposed independently by [CGM19], which showed that lattice-based average TPSFs require milder parameters than TPSFs, hence improving the efficiency of some TPSF-based lattice signatures [BFR$^+$18].

Multivariate schemes encountered and solved this problem independently. It was first noticed in [SSH11a] that some multivariate hash-then-sign schemes relied on a trapdoor function that only verified (T1) and a weak form of (T2). Hence [SSH11a] added a salt when hashing the message in order to satisfy (T3) and enable a FDH-style proof. This trick is reminiscent of RSA-PSS [BR96] and was also used in lattice-based signatures [GPV08], but the exact purpose in each case was slightly different. This solution is used by GeMSS [CFM$^+$19] and Rainbow [DCP$^+$19].

---

[1] (T2) implies (T3) with $D(X) = U(X)$.

3.5 Diffie-Hellman and El Gamal

The Diffie-Hellman (DH) key-exchange protocol [DH76] and the derived encryption scheme by El Gamal [ElG85] are staples of classical public key cryptography. El Gamal has been notably easier to adapt to PQ assumptions than DH. Classically, DH relies on (2), which provides a simple way for two parties to agree on a shared secret g^{ab}, by instantiating Fig. 5 with Fig. 6 (column 2). Unfortunately, such a simple relation is harder to obtain with PQ assumptions, as we will see.

Isogenies over elliptic curves are natural candidates to instantiate Fig. 5, with Alice (resp. Bob) knowing a private isogeny $\phi_A : E \to E_A$ ($\phi_B : E \to E_B$) and sending E_A (resp. E_B) to the other party. Unfortunately, existing instantiations requires either ordinary curves [Cou06; RS06] – which parameters don't scale well [DKS18] –, or supersingular curves with a restricted class of isogenies like CSIDH [CLM$^+$18] – which quantum security is debated [BS20; Pei20]. SIDH [JD11; FJP14] uses supersingular curves of smooth order, which security scales well but, unlike [Cou06; RS06; DKS18; CLM$^+$18], don't provide a clean relation similar to (2).

For SIDH to work, Alice needs to transmit, in addition to E_A, the image $\phi_A(E_2)$ of its private isogeny $\phi_A : E \to E_A$ over the torsion subgroup $E_2 = E[2^{\ell_2}]$. Similarly, Bob applies ϕ_B to $E_3 = E[3^{\ell_3}]$. With this extra information, the two parties can agree on a common curve E_{AB}. A mild constraint of this solution is that, prior to the protocol, each party must "pick a side" by agreeing who picks E_2 or E_3. Alternatively, one can apply the protocol twice.
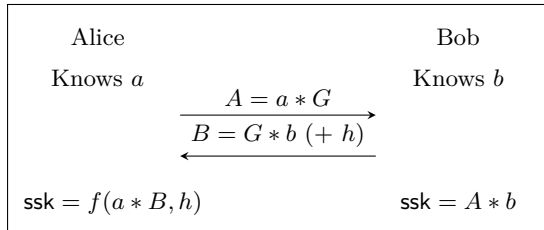

Figure 5: DH with Reconciliation

	(EC)DH	SIDH	LWE
G	$g \in \mathbb{G}$	$(P_i, Q_i)_i$	$\mathbf{A} \in R_q^{k \times k}$
a	$a \in |\mathbb{G}|$	ϕ_A	$(\mathbf{s}_a, \mathbf{e}_a)$ short
A	g^a	$E_A, \phi_A(E_2)$	$\mathbf{s}_a^t \cdot \mathbf{A} + \mathbf{e}_a^t$
B	g^b	$E_B, \phi_B(E_3)$	$\mathbf{A} \cdot \mathbf{s}_b + \mathbf{e}_b$
h	-	-	Yes
Static?	Yes	No	No

Figure 6: Instantiations of Fig. 5.

A straightforward adaptation of DH to codes and lattices is challenging as well, this time due to *noise*. For example, a rigid transposition with LWE gives:

$$(\mathbf{s}_a^t \cdot \mathbf{A} + \mathbf{e}_a^t)\mathbf{s}_b \approx \mathbf{s}_a^t(\mathbf{A} \cdot \mathbf{s}_b + \mathbf{e}_b) \tag{6}$$

Both parties would end up with "noisy secrets" that differ on their lower bits, which is problematic. In a purely non-interactive setting, this approach does not seem to work, except if q is very large, say $q \geq 2^\lambda$, which is impractical [GKR$^+$20]. This is resolved in [DXL12; Pei14] by having Bob send a hint indicating "how to round the noisy secret". Note that this solution seems to preclude non-interactivity, as h depends on what Alice sent to Bob.

Fig. 6 summarizes the two approaches to achieve "post-quantum DH" (besides CSIDH). These solutions cannot be used with static key shares, as it would enable key-recovery attacks [Flu16; GPS$^+$16]. The last one is also interactive. Thus they cannot be used as drop-in replacements to (non-interactive) (semi-)static DH.

Many desirable properties of classical DH are lost in translation when transposing it to a PQ setting. As such, most practical schemes take El Gamal as a starting point instead, replacing DLOG with LWE [NAB$^+$19; SAB$^+$19], LWR [DKR$^+$19], or SIDH [JAC$^+$19]. Schemes that rely on "trapdoors" – like McEliece [McE78; BCL$^+$19a] or BIKE-2 [ABB$^+$19] – are more akin to RSA encryption, though this analogy is a weaker one.

4   Return of Symmetric Cryptography

Another takeaway is that, despite PQC being mostly a public-key matter, symmetric cryptography plays a surprisingly important role and should not be neglected. In particular, two families of signatures based on one-way and hash functions have emerged, with two radically different philosophies:

- Hash-based signatures treat hash functions as *black boxes* and build signatures using only generic data structures and combinatorial tricks, see Sec. 4.1.
- Signatures based on zero-knowledge proofs treat one-way functions as *white boxes* and leverage knowledge of their internal structure to maximize their efficiency, see Sec. 4.2.

Interestingly, some techniques developed by these schemes have also benefited more "standard" schemes. Examples are Merkle trees, used by multivariate [BPS19] and isogeny-based [DG19; BKV19] schemes, or the *cut-and-choose* technique [KKW18].

4.1   Hash-based signatures

Hash-based signatures (HBS) are a peculiar family of schemes for two reasons; (a) they rely solely on the hardness properties of hash functions, (b) they follow a paradigm of their own. At a high level:

- The public key pk commits secret values using one or more hash functions.
- Each signature reveals (intermediate) secret values that allow to recompute pk and convince the verifier that the signer does indeed know sk.

Lamport's HBS [Lam79] epitomizes this idea. In its simplest form, the public key is: $\mathsf{pk} = (\mathsf{pk}_{i,0}, \mathsf{pk}_{i,1})_{i \in [\lambda]} = (H(\mathsf{sk}_{i,0}), H(\mathsf{sk}_{i,1}))_{i \in [\lambda]}$, and the signature of a message $\mathsf{msg} = (b_i)_i \in \{0,1\}^\lambda$ is $\mathsf{sig} = (\mathsf{sk}_{i,b_i})_i$. The verifier can then hash sig component-wise and check it against pk. It is easily shown that Lamport's signature scheme is secure under the preimage resistance of H. However, there are two caveats:

- pk and sig require $O(\lambda^2)$ bits, which is rather large.
- It is a one-time signature (OTS), meaning it is only secure as long as it performs no more than one signature.

For four decades, several tricks have been proposed to mitigate these caveats. Because of the unstructured nature of hash functions, these tricks typically rely on combinatorics and/or generic data structures.

<u>Generic Structures:</u> One line of research proposes efficient data structures that use OTS as building blocks. By hashing public keys into a tree, Merkle trees [Mer90] allow to improve efficiency and sign more than one message. Goldreich trees [Gol87] use trees' leaves to sign other trees' roots. Both ideas can be combined, as done by SPHINCS($^+$) [BHH$^+$15; BHK$^+$19; HBD$^+$19]. Finally, efficient Merkle tree traversal algorithms were proposed [Szy04].

<u>OTS:</u> Another line of research proposed more efficient OTS. The most efficient one so far is a variant of Winternitz's OTS (see [Mer90; BDE$^+$11]), called WOTS+ [Hül13], which uses bitmasks to rely on second-preimage resistance – instead of collision resistance for the original scheme. Stateless few-time signatures (FTS) were also proposed, such as BiBa [Per01], HORS (Hash to Obtain Random Subsets) [RR02], a HORS variant with trees, HORST [BHH$^+$15], one with PRNGs, PORS [AE18], and another one with forests, FORS [BHK$^+$19; HBD$^+$19]. These can be used to build *stateless* signatures, discussed below.

Combining these tools allows to build hash-based *stateful* and *stateless* signatures.

Stateful schemes require the signer to maintain an internal state in order to keep track of the key material used. This encompasses XMSS, its multi-tree variant XMSS$^{\text{MT}}$ and LMS, all recently standardized by NIST [CAD$^+$20]. Stateful schemes can be efficient but their statefulness is often an undesirable property.

Stateless signatures set their parameters so that, even without maintaining a state, signing many messages will preserve security with overwhelming probability. As a result, they are less efficient than their stateful counterparts, but more flexible. For example, SPHINCS$^+$ [BHK$^+$19; HBD$^+$19] combines Merkle and Goldreich trees with WOTS+ as an OTS, FORS as a FTS, plus a few other tricks.

4.2   Signatures based on ZKPs and OWFs

Signatures based on zero-knowledge proofs (ZKPs) and one-way functions (OWFs) leverage this principle:

– The public key is $\mathsf{pk} = F(\mathsf{sk})$, where F is a OWF.
– A signature is a ZKP that $\mathsf{pk} = F(\mathsf{sk})$; using the MPC-in-the-head [IKO$^+$07].

Note that all Fiat-Shamir signatures can already be interpreted as ZKP that $\mathsf{pk} = F(\mathsf{sk})$, however they usually leverage algebraic structure to gain efficiency, and as a result rely on assumptions that are algebraic in nature.

The protocols discussed here are fully generic as they work with any OWF. This is done by leveraging the *MPC-in-the-head* technique [IKO$^+$07]. This technique creates non-interactive proofs for an arbitrary circuit (Boolean or arithmetic), by simulating the execution of an MPC (*multiparty computation*) protocol, committing to the execution, and revealing the state of a subset of the parties in order to let the verifier (partially) check correctness of the execution. Two parallel yet connected lines of research turned this abstract idea into a reality.

Protocols: The first line of research provides protocols for generic statements. These have only recently become practical, see ZKB++[CDG$^+$17] and KKW [KKW18]. For bit-security λ and a circuit with $|C|$ AND gates, total proof sizes are $O(\lambda|C|)$, for ZKB++, and $O(\lambda|C|/\log n)$, for KKW, respectively, where the *cut-and-choose* approach of KKW allows a trade-off between signing and signature size, via the parameter n. For boolean (resp. arithmetic) circuits of cryptographic sizes, these two schemes (resp. the sacrificing method [BN20]) are the current state of the art.

Circuits: The second line of research provides circuits with low multiplicative complexity. Because of their unusual constraints, their internal structure is typically very different from classical symmetric primitives and they require new approaches to be studied. Prominent examples are LowMC [ARS$^+$15], which has been extensively studied [DKP$^+$19; JNR$^+$20; LIM20], or the Legendre PRF [Dam90; GRR$^+$16], which security has recently been shown to rely on a sparse *multivariate* system [SHB21]. Note that these primitives have applications that go far beyond PQC; for example, the Legendre PRF is used by the Ethereum 2.0 protocol.

Combining these two lines of research, one obtain signature schemes. For example, Picnic [ZCD$^+$19] combines LowMC with either ZKB++ or KKW, and LegRoast [Bd20] combines the Legendre PRF with the sacrificing method [BN20]. Due to the novely of this approach, it is likely that we will see many more schemes based on it in the future. Two works instantiate F with AES: BBQ [dDO$^+$19] uses KKW, and Banquet [BSGK$^+$21] improves efficiency via amortization techniques.

5 The Implementation Challenges in PQC

This section discusses the implementation challenges in PQC; specifically discussing attacks via implementation pitfalls and side-channels, countermeasures, and finally the jungle of embedded devices and use-cases for PQC schemes. We somewhat focus on NIST PQC candidates due to similarities in the operations each PQC family requires.

5.1 Decryption Failures and Reaction Attacks

Attacks based on decryption failures – also known as reaction attacks – were first discovered about 20 years ago, with an attack [HGS99] on the McEliece [McE78] and Ajtai-Dwork [AD97] cryptosystems, and another [HNP+03] on NTRU [HPS98]. They were forgotten for more than a decade before being recently rediscovered. It is clear by now that designers of noisy cryptosystems, such as lattice-based and code-based, need to take these into account. We explain how reaction attacks work and how to thwart them. At a high level, *all* lattice-based and code-based encryption schemes follow this high-level description: $\mathsf{ct} = \mathsf{pk} \cdot \mathbf{e} + \mathbf{e}' + \mathsf{Encode}(\mathsf{msg})$, where $\mathsf{Encode}(\mathsf{msg})$ is an encoding of msg and $(\mathbf{e}, \mathbf{e}')$ is a noisy error vector. The decryption key sk is used to obtain $\mathsf{Encode}(\mathsf{msg})$ plus some noise, then recover msg. However, this may fail for a small portion of the admissible $(\mathbf{e}, \mathbf{e}')$, and this portion depends on sk. The high-level strategy of reaction attacks uses:

- **Precomputation.** Precompute "toxic" errors $(\mathbf{e}, \mathbf{e}')$ that have a high probability of leading to decryption failures.
- **Query.** Use these toxic errors to send ciphertexts to the target; observe decryption failures.
- **Reconstruction.** Deduce sk from the decryption failures.

Note that reaction attacks are CCA attacks. In CCA schemes, $(\mathbf{e}, \mathbf{e}')$ is generated by passing msg and/or pk into a pseudo-random generator (PRG), so adversaries have to find toxic vectors through exhaustive search. Hence precomputation is often the most computationally intensive phase.

Reaction attacks have been proposed against code-based schemes in the Hamming metric [GJS16], in the rank metric [SSP+19], and for lattice-based schemes [DGJ+19; DVV19; GJY19]. Interestingly, attacks against schemes that use lattices or the Hamming metric are very geometric (learning the geometry of the private key), whereas those that target rank metric schemes learn algebraic relations.

For lattice-based schemes, *directional failure boosting* [DRV20] allows, once a toxic error $(\mathbf{e}, \mathbf{e}')$ has been found, to find many more at little cost. Therefore, lattice schemes *must* keep their failure probability negligible, as they are otherwise directly vulnerable to reaction attacks. No such conclusion has been made for code-based schemes yet, but we recommend scheme designers to err on the safe side. Scheme designers need to consider two things with respect to reaction attacks. First, the probability of decryption failures should be negligible.

- This can be achieved by selecting the parameters accordingly, as done by Kyber [SAB+19], Saber [DKR+19], and FrodoKEM [NAB+19]. One may even eliminate them completely like NTRU [ZCH+19] and NTRU Prime [BCL+19b], but this may result in slightly larger parameters.
- Another solution is to use redundancy; KEMs need to encapsulate a symmetric key of λ bits, however schemes can often encrypt a much larger message msg. One can use the extra bits to embed an error-correcting code (ECC). However, this solution has two caveats. First, the ECC should be constant-time (e.g., XEf [ZCH+19] and Melas codes [Ham19]), as timing attacks have been observed when that was not the case [DTV+19]. Second, this requires to

perform a tedious analysis of the noise distribution; incorrect analyses have led to theoretical attacks [DVV19; GJY19].

Second, schemes with decryption failures – even negligible – should use CCA transforms that take these into account. In effect, most PQ KEMs in this situation use variants of the transforms described [HHK17], which do handle them.

5.2 Implementation Attacks in PQC

Isochrony: Before NIST began their PQC standardization effort, many PQC schemes were susceptible to implementation attacks; meaning that due to bad coding practices, some attack vectors were found which led to successful attacks. Definition 5 in [HPR+20] provides a fairly formal definition for isochronous algorithms (i.e., an algorithm with no timing leakage) which allows us to differentiate between these initial implementation attacks, of which many did not qualify. Good programming practices exist for ensuring timing analysis resilience and have been well discussed before[1]. These practices cover much more low-level instances of isochronous designs; as conditional jumps, data-dependent branching, and memory accesses of secret information can also lead to detrimental attacks. Some tools such as `ctgrind`, `ctverif`, and `flow-tracker` exist to check whether functions are isochronous, however with operations in PQC such as rejection sampling it is not clear how effective these tools will be. Thus, it would also be prudent to check post-compilation code of the sensitive operations within an implementation.

Implementation attacks: The first types of implementation attacks on PQC were mainly on the BLISS signature scheme and exploited the cache-timing leakages from the Gaussian samplers, as they mostly operate by accessing pre-computed values stored in memory [BHL+16; PBY17]. The attacks use the FLUSH+RELOAD [YF14] technique and exploit cache access patterns in the samplers to gain access to some coefficients of values that are added during the signature's calculation. However, optimisations to the Gaussian samplers, such as using guide-tables, and non-isochronous table access enabled these attacks. More leakage sources and implementation attacks against the StrongSwan implementation of BLISS were also found [EFG+17], which range from data dependent branches present in the Gaussian sampling algorithm to using branch tracing in the signature's rejection step. These attacks can be mitigated by bypassing conditional branches; that is, using a consistent access pattern (e.g., using linear searching of the table) and having isochronous runtime. In particular, making Gaussian samplers provably secure and statistically proficient have been researched [HPR+20] and thus should be followed for secure implementations of lattice-based schemes such as Falcon and FrodoKEM or more advanced primitives such as IBE and FHE. More implementation attacks were also found in early code-based public-key encryption schemes such as McEliece, Niederreiter, and others [Str10; AHP+12; Str13; ELP+18].

Sensitive modules: Although these attacks are on a scheme's implementation, rather than something inherently insecure in its algorithm, they have acted as a cautionary note for how some schemes have operations, which do not use secret information, but could be described as *sensitive* or *fragile* as if they are implemented incorrectly, it can lead to a successful attack. A clear example of this is for Gaussian samplers, which is why they were not used in Dilithium. Once an attacker finds the error vector, $\mathbf{e}$, using these side-channels from a LWE equation of the form $\mathbf{b} = \mathbf{A} \times \mathbf{s} + \mathbf{e} \mod q$, then gaining the secret can be achieved using Gaussian elimination. Moreover, it is not always necessary to find the entire secret, as was the case in the past for RSA [Cop97].

---

[1] For example, see https://www.bearssl.org/constanttime.html.

Attacks on sparse multipliers: Some of the timing leakage found in StrongSwan's BLISS implementation [EFG+17] exploited the sparseness of one of the polynomials in the multiplication. The NIST PQC candidate HQC [AAB+19] was also susceptible to a similar attack during decryption. At one point in time they proposed a sparse-dense multiplier to improve the performance, however the multiplication would only access the secret-key polynomial h times, for a secret-key containing only h 1's. To shield this algorithm they then proposed to permute on the memory-access locations, however the secret can also be recovered by observing the memory cells.

FO transform attacks: A sensitive component that can potentially affect all PQC candidates is in the Fujisaki-Okamoto (FO) transformation, required in most PQ KEMs in order to covert the CPA-secure part into an IND-CCA secure scheme in the random-oracle model (ROM). However, it has been shown that this operation is also sensitive to timing attacks, even though the operations do not use any secret information. This attack [GJN20] was shown on FrodoKEM, and was enabled due to its use of non-isochronous `memcmp` in the implementation of the ciphertext comparison step, which allows recovery of the secret key with about 2^{30} decapsulation calls. This attack is directly applied to FrodoKEM, but is likely that other PQC candidates such as BIKE, HQC, and SIKE are also susceptible. Initial fixes of this were also shown to be vulnerable in FrodoKEM[2] and SIKE[3].

Masking the comparison required in the FO transform has been investigated for first-order [OSP+18] and higher-order [BPO+20] levels, as inconsistencies in this key component can lead to an attack. Although these masked implementations appeared secure, they are shown to be vulnerable in a variety of ways, and fixes to these masked operations are proposed [BDH+21]. The importance of securing this component is again highlighted, thus the authors proposed a framework for testing the leakage in vulnerable parts of the FO transform.

Implementations of the random oracle (RO) required in NIST PQC KEMs were shown to not always follow the correct domain separation [BR93]. Typically, NIST PQC KEMs require multiple uses of ROs, which can be separated by prefixing the input to the ith RO with i itself, know as 'oracle cloning'. However, some candidates were shown not to do this, or did this incorrectly; which lead to key recovery attacks [BDG20].

An algorithm used within the FO transform is Keccak, or more specifically SHAKE, which was standardized by NIST in FIPS-202 for SHA-3 and is used extensively within NIST PQC candidates for so-called seed-expansion and computation of the shared secret. This symmetric operation is also sensitive to side-channels and could potentially lead to recovery of the shared-secret generated in the KEM. In particular, the case for a single trace attack in the ephemeral key setting. An attack on the Keccak permutation [KPP20] is shown to be vulnerable for 8-bit devices, however these are highly unlikely to be able to run a PQ KEM. However, it is another cautionary note on protecting sensitive modules within PQC and countermeasures may be required for real-world implementations.

Decryption in BIKE: The BIKE decryption algorithm is designed to proceed in a repetitive sequence of steps, whereby an increase in repetitions increases the likelihood of proper decryption. This makes the procedure inherently non-isochronous, unlikely other NIST PQC candidates. Thus, it was proposed to artificially truncate this procedure at some fixed number. Experimentally, a round-count as small as 10 is sufficient to guarantee proper decryption. However, unlike lattice-based KEMs, there is no mathematical guarantee that this is sufficient to reduce the decryption failure rate below 2^λ, where $\lambda \in \{128, 192, 256\}$ is the concrete security parameter.[4]

---

[2] https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/kSUKzDNc5ME.
[3] https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/QvhRo7T2OL8.
[4] Known, formal analyses guarantees are closer to 2^{-40} at 128-bit security.

Thus, despite BIKE being designed as CPA scheme as well as a CPA-to-CCA scheme, they have only formally claimed CPA-security (ephemeral keys) for their construction, as opposed to CCA-security (long-term keys). It remains open to provide the proper analysis to solve this issue.

5.3   Side-Channels and Countermeasures

In the Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process [AASA+20b] it is stated that:

> *NIST hopes to see more and better data for performance in the third round. This performance data will hopefully include implementations that protect against side-channel attacks, such as timing attacks, power monitoring attacks, fault attacks, etc.*

In their initial submission requirements [NIS16] NIST also noted "schemes that can be made resistant to side-channel attacks at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks". Thus, some of the remaining candidates have offered masked implementations, or this has been done by the research community. Also, see [AH21] for an extensive summary of attacks against NIST PQC third round candidates.

SCA with hints: Building upon the idea of gaining partial knowledge of the secret key has been investigated for both lattice-based [DDG+20] and code-based [HPR+21] cryptographic schemes. In lattice-based cryptography, lattice reduction algorithms are often used to evaluate a scheme's security level, as shown in [ACD+18] for example. This is somewhat equivalent to using information set decoding (ISD) in code-based cryptography. The cryptanalytic idea is that partial knowledge of the secret (or error), i.e. "hints", which are insufficient for a full side-channel attack, can be used in these algorithms (lattice reduction or ISD) to perform an analysis on the security of the scheme.

One can then predict the performance of these algorithms and estimate the security loss for a given amount of side-channel information. This may become useful in future when certifying these PQ cryptographic modules, as some certifiers for symmetric cryptography require a certain amount of key candidates remain *after* side-channel analysis [AH21].

DPA on multiplication: NTRU and NTRU Prime both have the potential of using a combination of Toom-Cook and Karatsuba to speed-up their polynomial multiplication, thus whether they can reuse techniques from Saber's masked implementation is an important research question. NTRU Prime in particular requires masking since some power analysis attacks can read off the secret key with the naked eye [HCY20]. Attacks on these multiplication methods, which are in the time-domain, are likely to be simpler than those in the NTT or FFT domains as there is only one multiplication per coefficient of the secret, which thus makes protection of this multipliers more urgent. A single-trace power analysis attack on FrodoKEM exploits the fact that the secret matrix is used multiple times during the matrix multiplication operation, enabling horizontal differential power analysis [BFM+19]. The analysis targets three key stages of the implementation; the loading of the secret values, the multiplication, and the updating of the accumulation. A similar attack was shown in practice on an older version of FrodoKEM (and NewHope) as a key-exchange scheme [ATT+18].

Although there has been less focus on MQ schemes, Park et al. [PSK+18] provide results on the security of Rainbow (and UOV) by using correlation power analysis and algebraic key recovery attacks. The attack targets the secret maps, within the MQ signature schemes, during the matrix-vector computations. It targets the inversion of one of the secret-maps (i.e., S^{-1} for the secret-map used as a matrix, S). This result is then used to recover the other maps

using key recovery. This attack is relevant for many MQ schemes that use the affine-substitution quadratic-affine (ASA) structure. Park et al. [PSK+18] also discuss countermeasures to SPA and DPA attacks by using standard methods seen before such as shuffling of the indices or adding a pseudo-random matrix (i.e., additive masking).

Attacks on syndrome decoding: A variant of McEliece PKE, QcBits, a variant of McEliece public-key encryption scheme based on quasi-cyclic moderate density parity check codes, was shown to be susceptible to DPA [RHH+17]. The attack partially recovers the secret key using DPA during the syndrome computation of the decoding phase, and using this information recovers the remainder of the secret solving a system of linear equations. Rossi et al. also propose a simple countermeasure for the syndrome calculation stage, which exploits the fact that since QC-MDPC codes are linear, the XOR of two codewords is another codeword. Thus, a codeword can be masked by XORing it with another random codeword before the syndrome calculation.

This attack was then extended [SKC+19] to recover the *full* secret of QcBits, with more accuracy, using a multi-trace attack. Moreover, using the DPA countermeasures proposed in [RHH+17] and in the ephemeral key setting, they provide a single-trace attack on QcBits. Lastly and most interestingly, they describe how these attacks can be applied to BIKE, by targetting the private syndrome decoding computation stage where long-term keys are utilized, for BIKE-1, BIKE-2, and BIKE-3. For ephemeral keys, the multi-target attacks are not applicable, however the single-trace attack can be applied to recover the private key and also the secret message.

Classic McEliece is also not immune from side-channel attacks targeting this operation. A reaction attack [LNP+20] using iterative chunking and information set decoding can enable recovery of the values of the error vector using a single decryption oracle request. The attack targets the hardware design of Classic McEliece and provides simulated results, which is then compared to theoretical predictions, as well as a practical evaluation on FPGA. A recent attack has also shown vulnerabilities in Classic McEliece's syndrome computation to fault attacks by changing the matrix-vector multiplication to be over $\mathbb{N}$, instead of $\mathbb{F}_2$, which then makes linear programming solvers much easier to recover the message [CCD+21].

Cold-boot attacks: PQC schemes have also been shown to be susceptible to cold-boot attacks [Pol18; ADP18], which was previously shown on NTRU [PV17]. Cold-boot attacks exploit the fact that secret data can remain in a computers memory (DRAM) after it is powered down and supposedly deleted. Albrecht et al. [ADP18] describe how to achieve this by attacking the secret-keys stored for use in the NTT multiplier in Kyber and NewHope, and after some post-processing using lattice reductions, is able to retrieve the secret-key.

Key reuse: These attacks, which have been shown to cause issues for real-world implementations in EMV [DLP+12], are also applicable in PQC; such as lattice-based schemes [Flu16], supersingular isogeny-based schemes [GPS+16], and potentially more.

Masking Dilithium: Migliore et al. [MGT+19] demonstrate DPA weaknesses in the unmasked Dilithium implementation, and in addition to this provide a masking scheme using the ISW probing model following the previous techniques for masking GLP and BLISS [BBE+18; BBE+19]. Like the previous provably secure masking schemes, they alter some of the procedures in Dilithium by adding in efficient masking of its sensitive operations. Moreover, some parameters are changed to gain extra performance efficiencies in the masked design, such as making the prime modulus a power-of-two, which increases the performance by 7.3-9x compared to using the original prime modulus during masking. A power-of-two modulus means the optimised multiplication technique, the NTT multiplier, is no longer possible so they proposed Karatsuba multiplication. The results for key generation and signing are between 8-12x slower for order 2 masking and 13-28x slower for order 3 masking, compared to the reference implementations. This is also backed-up by experimental leakage tests on the masked designs.

<u>Masking Saber:</u> Verhulst [Ver19] provides DPA on the original reference implementation of Saber, as well as developing a masking scheme for Saber's decryption protocol, which is later extended in [BDK+20]. The masking schemes use additive first-order masking for the polynomial multiplication and addition, and Boolean masking for the bit extraction. Compared to Saber's reference implementation, the masked decryption is 2-2.5x slower. However, like previously proposed provably masking schemes, these may still be vulnerable to template attacks [OM07]. Saber lends itself to practical masking due to its use of LWR, as opposed to other lattice-based candidates which use variants of LWE. However, Saber uses a less efficient multiplication method (a combination of Toom-Cook, Karatsuba, and schoolbook multiplication) compared to schemes which use NTT; thus it is an interesting open question as to whether NTT is the most practical multiplication method (due to its conflict with efficient masking) and how these masked PQC schemes practically compare, particularly with the recent research improving the performance of Saber and others using NTTs [CHK+20].

<u>Masking matrix multiplication:</u> Masking schemes which use matrix multiplication have the potential to be efficiently masked using affine masking (i.e., a combination of additive and multiplicative masking) similarly used in AES [FMP+11]. First-order additive masking has already been proposed for FrodoKEM [HMO+19]. Warnings for side-channel protection were also seen in Picnic, where the attack was able to recover the shared secret and the secret key, by targetting the MPC-LowMC block cipher, a core component to the signature scheme [GSE20].

<u>Fault attacks:</u> Fault attacks have also been investigated for PQC schemes. One of the most famous (microarchitectural) fault attacks is the Rowhammer exploit (CVE-2015-0565), which allows unprivileged attackers to corrupt or change data stored in certain, vulnerable memory chips, and has been extended to other exploits such as RAMBleed (CVE-2019-0174). QuantumHammer [MIS20] utilises this exploit to recover secret key bits on LUOV, a second round NIST PQC candidate for multivariate-quadratic signatures. Specifically, the attack collects faulty signatures, from which a few secret key bits can be recovered. From this, they employ a divide-and-conquer attack which exploits this structure to solve the system of equations for the full secret key more efficiently, using the few key bits recovered via bit-tracing. The attack does somewhat exploit the 'lifted' algebraic structure that is present in LUOV, so whether this attack could be applied to other PQC schemes is an open question.

Determinism in signatures is generally considered preferable from a security perspective, as attacks are possible on randomly generated nonces (e.g., [fail10]). This prompted EdDSA, which uses deterministically generated nonces. NIST [AASA+20b] noted the potential for nonce reuse in PQC schemes such as Kyber. Indeed, fault attacks which exploit the scheme's determinism have been demonstrated on SPHINCS+ [CMP18] and Dilithium [BP18; RJH+19], with EdDSA also showing susceptibility to DPA [SBB+18]. As such, some PQC candidates offer an optional non-deterministic variant, such as SPHINCS+ using `OptRand`, or random *salt* used in Dilithium, Falcon, GeMSS, Picnic, and Rainbow.

<u>Hedging:</u> An interesting alternative to mitigating these fault attacks (and randomness failures) is by using *hedging*, which creates a middle-ground between fully deterministic and fully probabilistic signatures, by deriving the per-signature randomness from a combination of the secret-key, message, and a nonce. This is formalized for Fiat-Shamir signatures and apply the results to hedged versions of XEdDSA, a variant of EdDSA used in the Signal messaging protocol, and to Picnic2, and show hedging mitigates many of the possible fault attacks [AOT+20].

5.4   Embedded Devices and Use Cases

Benchmarking: A key evaluation criteria for NIST PQC candidates is their performance; this includes standard CPUs (e.g., Intel x86), using optimizations (e.g., AVX2), and also incorporates designs for microcontrollers and FPGAs for evaluating specific use cases such as IoT. NIST[5] specifically asked the research community to focus on ARM Cortex-M4 and Xilinx Artix-7 devices for benchmarking. A number of repositories exist for such benchmarking, including SUPERCOP, PQClean[6], pqm4[7], as well as 'wikis' such as PQCzoo[8] and PQC wiki[9].

As well as side-channel analysis, NIST [AASA+20b] has also asked for hardware benchmarking (i.e., FPGA, ASIC, or hardware/software co-designs) to inspire discussions. Hardware implementations which have been done to-date are for the candidates BIKE [RBG20], FrodoKEM [HOK+18; HMO+19; BUC19], Kyber [BUC19; XL21] and Dilithium [BUC19; RMJ+21], NTRU Prime [Mar20], Picnic [KRR+20], Saber [RB20], and SIKE [MLR+20; EAMK20; KAE+20]. In general, they show that lattice-based schemes are significantly more amenable to hardware implementations, showing balance between resource consumption and performance for key generation, encapsulation/signing, and decapsulation/verifying. Moreover, many of these designs show significantly better performances in comparison to equivalent cryptographic schemes from RSA and elliptic curves.

Bottlenecks: As per the pqm4 report [KRS+19], Classic McEliece, GeMSS, Picnic, and Rainbow have keys which are too large for the device's memory, which indicates these schemes may have been selected for the third round (or as alternates) for specific use cases and not general purpose applications [AASA+20b]. The use of external libraries (OpenSSL and NTL) by BIKE and HQC also raised integration issues. The report also notes that a significant amount of computing time is spent on the hashing parts of these implementations; with KEMs spending upwards of 50% of their total runtime using SHAKE and for signatures, this value can reach upwards of 70% in some cases. It is then an interesting open question to see how much more performant these schemes could become with faster seed expander (e.g., [HMO+19]), with dedicated instructions for SHAKE (similar to Intel's AES-NI), or using candidates from the ongoing NIST Lightweight Cryptography[10] standardization process.

Energy costs: Power consumption is another important performance metric with respect to IoT. Energy requirements for round 2 PQC candidates, that fit on the ARM Cortex M4, show that structured lattices consume less energy in comparison to equivalent schemes using isogenies on elliptic curves. Furthermore, schemes such as NTRU Prime and SIKE consume significantly more energy and are orders of magnitude apart from the energy consumption required for Kyber or Saber.[11]

Floating-points: The signature scheme Falcon [PFH+19] requires "*extensive floating-point operations, and random sampling from several discrete Gaussian distributions*" [AASA+20b]. Floating-point operations in Falcon require 53 bits of (double) precision, which will use hardware FPU when available or will be emulated using integer operations (e.g., on the ARM Cortex-M4). Both of these options are provided in [Por19], as well as in its provably secure and isochronous Gaussian sampler [HPR+20]. However, more side-channel investigations should be performed on Falcon for these different implementations on a variety of platforms using the device's FPU.

---

[5] https://csrc.nist.gov/CSRC/media/Presentations/the-2nd-round-of-the-nist-pqc-standardization-proc/images-media/moody-opening-remarks.pdf.
[6] https://github.com/PQClean/PQClean.
[7] https://github.com/mupq/pqm4.
[8] https://pqczoo.com/.
[9] https://pqc-wiki.fau.edu/.
[10] https://csrc.nist.gov/projects/lightweight-cryptography.
[11] https://github.com/mjosaarinen/pqps.

6   Integrating PQC into the Real World

6.1   PQC Standardization Efforts Around The World

NIST PQC: In 2017, the National Institute of Standards and Technology (NIST) initiated a process[12] to solicit, evaluate, and standardize one or more post-quantum PKEs/KEMs and digital signature schemes. NIST received 69 submissions from around the world, which began the first round of analysis. Of these, 26 cryptosystems advanced [AASA+19] to the second round in January of 2019. The third round candidates (seven Finalists and eight Alternates, shown in Table 3) were announced [AASA+20a] in July 2020. Round 3 will continue for another 12-18 months, then initial PQC standards are expected to be chosen from the Finalists. The remaining Alternates will be considered in a subsequent fourth round.

Table 3: Third round candidates in the NIST Post-Quantum Cryptography standardization project.

	KEMs	Digital Signatures
Third Round Finalists	Classic McEliece CRYSTALS-Kyber NTRU SABER	CRYSTALS-Dilithium Falcon Rainbow
Alternative Candidates	BIKE FrodoKEM HQC NTRU Prime SIKE	GeMSS Picnic SPHINCS+

NSA: In 2020, the National Security Agency (NSA)'s Cybersecurity Directorate (CSD) posted a statement on their website [NSA20] that they have independently reviewed the security analysis and performance characteristics of the NIST PQC proposals, and they are confident in lattice-based schemes with strong dependence on well-studied mathematical problems and in hash-based signatures for certain niche solutions. While NIST includes, e.g., Classic McEliece and Rainbow in its Finalists, NSA states, "*At the present time, NSA CSD does not anticipate the need to approve other post-quantum cryptographic technologies for National Security System usage, but recognizes circumstances could change going forward*".

CACR: In 2018, the Chinese Association for Cryptographic Research (CACR)[13] began their own PQC standardization process [Din19; Xia21] and, similar to the NIST call, asked for submissions for PKE/KEM and digital signatures. The winners of the competition are the RLWE encryption scheme LAC.PKE [LLZ+18] and the asymmetrical module LWE encryption scheme, Aigis-enc, and signature scheme Aigis-sig [ZYF+20]. LAC was also a submission to the NIST PQC process, but it was not selected for Round 3, due to a large variety of cryptanalytic attacks targeting, e.g., non-isochronous implementations and leakage from decryption failures [GJY19].

Russia: In 2020, the technical committee for standardisation in Russia began plans for standardising PQC and announced they have teams developing signature and key exchange schemes [Fed21], expecting to announce standards by the end of 2021. Once the proposals have been accepted, they will be integrated into GOST their national standards. The presentation also notes

---

[12] https://www.nist.gov/pqcrypto.
[13] CACR homepage https://cacrnet.org.cn/.

the types of proposals they are considering: a hash-based signature, a code-based signature, a lattice-based signature, and an isogeny-based key exchange scheme called 'Forsythia'. Unlike the NIST and CACR PQC processes, they also note that their process is not a 'competition', but rather they are likely to accept all proposals that satisfy their security requirements.

ETSI: In 2013, the European Telecommunications Standards Institute (ETSI) began a Quantum-Safe Cryptography (QSC) working group who aims to assess and make recommendations for quantum-safe cryptographic primitives protocols and implementation considerations, which will complement the NIST PQC effort. ETSI's Quantum-Safe Cryptography (QSC) focus is on practical implementation, including performance considerations, implementation capabilities, protocols, benchmarking, and architectural considerations for specific applications. This is demonstrated their recent report (TR 103 617) on QSC VPNs. As of their latest work programme [ETSI20], ETSI plans to publish standards in quantum-safe hybrid key exchange, signatures, and migration techniques this year.

ISO/IEC: In 2015, the ISO/IEC JTC 1/SC 27 Working Group 2 (WG2) created a study period to investigate the area of post-quantum cryptography and to prepare standardization activities of SC 27 in the field [Che19]. This lasted two years and resulted in several standing documents (SD8) on areas in PQC.[14] There are also plans to integrate specifications for stateful hash-based signatures in ISO/IEC 14888 part 4 [CS21].

IETF: The Internet Engineering Task Force (IETF), who develop and promote voluntary Internet standards (i.e., TCP/IP), have a Crypto Forum Research Group who have chosen to standardize two stateful hash-based signatures; the Leighton-Micali signature scheme (RFC 8554) and the extended Merkle signature scheme (RFC 8391). The IETF intends to wait until the resolution of the NIST PQC process to make recommendations for key agreement and signatures [Sul19].

ITU: The International Telecommunication Union (ITU), a specialized agency of the United Nations for information communications technology, is creating X.5Gsec-q, which is a security guideline for applying quantum-safe algorithms in 5G systems. As with the ETSI and ISO PQC documents, this is still an ongoing project, and aims to have a collaborative approach for standardizing PQC [Pec19].

Miscellaneous: Many other countries will follow and/or support the NIST PQC process for deciding their own government standards. This was expressed by the Canadian Centre for Cyber Security (CCCS) [CCCS20], the UK's National Cyber Security Centre (NCSC) [NCSC20], and the German Federal Office for Information Security (BSI) [BSI18]. Without considering use cases, the BSI [BSI21] also extends this by recommending FrodoKEM and Classic McEliece as "*suitable for long-term confidentiality protection*". The NCSC also intend to develop a lattice-based identity-based encryption scheme[15], to replace its current standard MIKEY-SAKKE. Most if not all agencies also suggest migrating via a classical/PQC hybrid approach.

6.2 New and Future Protocols

Despite this variety of approaches to PQ standardization, every group share the same goal: secure and safe, real-world and large-scale deployment of post-quantum cryptography. In the end, this will come down to significant but necessary modifications of protocols and practices. We highlight a few important ideas and unusual properties of the coming protocols.

---

[14] https://www.din.de/en/meta/jtc1sc27/downloads.

[15] https://www.ncsc.gov.uk/news/ncsc-supports-industry-drive-towards-common-standards-secure-communication.

Post-Quantum Wireguard: PQ-Wireguard [HNS+20] is a new, real-world VPN protocol achieving post-quantum security with forward secrecy and authentication. *Pre*-quantum sub-algorithms are generally balanced (between publie key size and ciphertext size) in their costs, whereas PQ Wireguard needs to manage PQ algorithms with greater and unbalanced costs. Their solution is to "amortize" the large public-key size of Classic McEliece by including such a long-term key along with the (non-cryptographic) software install package to gain advantage of the scheme's small ciphertexts. In the online phase, an *ephemeral*, balanced-and-fast KEM is employed (from lattices). This uniquely diverse mix of algorithms allows for all messages between parties to fit within a single IPv6 packet, minimizing communication costs.

Stateful hash-based signatures: NIST has standardized the existing *stateful* hash-based signatures LMS and XMSS in SP 800-208 [CAD+20]. NIST requires that the state management of LMS and XMSS be controlled by a Hardware Security Module. NIST adds a verifiable "physical security requirement" for the physical devices controlling and maintaining the highly sensitive state of stateful hash-based signatures. This aims to ensure that the state is spawned from a known entropic process, and that additional entropy is not introduced into the state variable from an external source during the course of execution, nor is the state ever cloned and exported beyond the boundaries of the device unless the security of the device is *physically* violated.

KEMTLS: Inspired by OPTLS [KW16], KEMTLS [SSW20] proposed an alternative to the TLS 1.3 handshake that replaces signatures (for server authentication) with *implicit* authentication via KEMs. This is motivated by the fact that in a post-quantum world, KEMs are *generally* more bandwidth-efficient than signatures – though this may not always be the case [DKL+20]. For some choices of KEM and signature, KEMTLS can replace TLS 1.3 with less than half the bandwidth and with an almost 90% decrease in server CPU cycles. Another stated advantage of KEMTLS is to eliminate code for signatures generation from the server side.

Secure messaging: Protocols for secure messaging highlight some challenges that a post-quantum transition may pose. The Signal protocol (and its sub-protocols: *X3DH* for the initial handshake, *Double Ratchet* for continuous communication) is the most prominent of these protocols, however it makes a non-black-box use of Diffie-Hellman properties, and is therefore not trivially post-quantum. It was shown in [ACD19] how to instantiate the Double Ratchet with generic KEMs (including post-quantum ones). Replicating the properties of X3DH with generic primitives seemed challenging [BFG+19], but was recently addressed in [HKK+21].

6.3 Large Scale Experiments

Key establishment in TLS: Some experiments have been run for Combined Elliptic-Curve and Post-Quantum (CECPQ) in TLS using Chrome Canary. The experiments combine 32 bytes of shared secret material using X25519 key exchange, with a further 32 bytes being derived using either NewHope with SHAKE-128 (CECPQ1), NTRU with SHA-2 (CECPQ2), or SIKE with SHA-2 (CECPQ2b). These bytes are concatenated and form a pre-master secret for deriving shared keys. In 2016[16], Google first ran the CECPQ1 experiment and it was later noted in by Langley[17] that "*post-quantum confidentiality in TLS should probably be based on structured lattices*". In 2019, Google and Cloudflare[18] trialled CECPQ2/b, showing that, despite SIKE having 2-3x smaller keys, NTRU significantly outperformed SIKE with Langley[19] noting that "*the computational demands of SIKE out-weigh the reduced network traffic*". Amazon has also conducted experiments with BIKE and SIKE, see [Wei20].

---

[16] https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.
[17] https://www.imperialviolet.org/2018/04/11/pqconftls.html.
[18] https://blog.cloudflare.com/towards-post-quantum-cryptography-in-tls/.
[19] https://www.imperialviolet.org/2019/10/30/pqsivssl.html.

<u>Signatures for TLS:</u> Sikeridis et al. [SKD20] show the PQC performances of a number of different Round 2 signature candidates in TLS 1.3 and compare these to RSA and ECDSA. The authors note that "*Most PQ signature candidates we studied (except SPHINCS+) are not likely to be a significant performance concern*", where the better performing schemes, which were the lattice-based signatures Dilithium and Falcon, were shown to have comparable performance results compared to RSA3072 and ECDSA384.

7 Conclusion

The aim of this paper is to systematically traverse the area of post-quantum cryptography; starting at the theoretical and protocol design side, continuing through the challenges found in implementing these schemes, and finally providing an overview of the current and future integrations of PQC into the real-world. Due to the comprehensive nature of this SoK, we hope that it will be used as a handbook to those, from academia to industry, wanting to become versed in this growing area, and require a concise review of the current state-of-the-art.

We use the concise categorization of cryptographic hardness problems in Section 2 to give an overview of PQC, not by their respective families, but instead by the paradigms they utilise. This allows us to simplify many of their complexities away and add a layer of accessibility to readers not completely familiar in the area. We also discuss requirements and pit-falls of these paradigms in order to give a reader, interested in designing their own PQC scheme, an idea of how and why schemes failed or succeeded; giving caution where it is required. Thus, as new PQC schemes emerge, we hope that this SoK provides a useful framework for it to be safely designed.

In Section 5 we discussed a wide range of issues when implementing PQC. This will be one of the most challenging aspects for this new era of cryptography, with these schemes potentially increasing code size, hardware footprint, memory requirements, transmission costs, energy costs, and attack vectors, *but* this will also open many doors for more innovations in this area. Indeed, one of the most important aims of this section is to give caution to practitioners; by showing themes of historical attacks on PQC implementations. We highlight these *sensitive* modules so implementers, who have predominately focused on classical cryptography such as RSA and ECC, will be better prepared to address the complexities in designing secure and efficient implementations of PQC, for the right use cases.

We then provide an overview of how PQC has and will be integrated into the real-world. We summarize the public standardization efforts from government agencies and international standards bodies, as well as describing the current and future protocols at the core of secure communications that are beginning to incorporate PQC. Much of this also includes challenges which have not yet been fully realised, especially in the grand scale of use cases which affect people in the millions, if not more.

References

[AAB+19]   C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, and G. Zémor. *HQC*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[AASA+19]   G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone. *NISTIR 8240: Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process.* 2019.

[AASA+20a]   G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone. *NISTIR 8309: Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*. 2020.

[AASA+20b]   G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, et al. "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process". In: *NIST, Tech. Rep., July* (2020).

[ABB+19]   N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. Aguilar Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, G. Zémor, and V. Vasseur. *BIKE*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[ABG+19]   N. Aragon, O. Blazy, P. Gaborit, A. Hauteville, and G. Zémor. "Durandal: A Rank Metric Based Signature Scheme". In: *EUROCRYPT*. Ed. by Y. Ishai and V. Rijmen. Vol. 11478. LNCS. Springer, Heidelberg, May 2019, pp. 728–758. DOI: 10.1007/978-3-030-17659-4_25.

[ACD19]   J. Alwen, S. Coretti, and Y. Dodis. "The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol". In: *EUROCRYPT*. Ed. by Y. Ishai and V. Rijmen. Vol. 11476. LNCS. Springer, Heidelberg, May 2019, pp. 129–158. DOI: 10.1007/978-3-030-17653-2_5.

[ACD+18]   M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer. "Estimate All the LWE, NTRU Schemes!" In: *SCN 18*. Ed. by D. Catalano and R. De Prisco. Vol. 11035. LNCS. Springer, Heidelberg, Sept. 2018, pp. 351–367. DOI: 10.1007/978-3-319-98113-0_19.

[AD97]   M. Ajtai and C. Dwork. "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence". In: *29th ACM STOC*. ACM Press, May 1997, pp. 284–293. DOI: 10.1145/258533.258604.

[ADP18]   M. R. Albrecht, A. Deo, and K. G. Paterson. "Cold Boot Attacks on Ring and Module LWE Keys Under the NTT". In: *IACR TCHES* 2018.3 (2018). https://tches.iacr.org/index.php/TCHES/article/view/7273, pp. 173–213. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i3.173-213.

[AE18]   J.-P. Aumasson and G. Endignoux. "Improving Stateless Hash-Based Signatures". In: *CT-RSA*. Ed. by N. P. Smart. Vol. 10808. LNCS. Springer, Heidelberg, Apr. 2018, pp. 219–242. DOI: 10.1007/978-3-319-76953-0_12.

[AGL+10]   C. Aguilar, P. Gaborit, P. Lacharme, J. Schrek, and G. Zemor. *Noisy Diffie-Hellman protocols*. Rump session of PQCrypto. https://www.yumpu.com/en/document/view/53051354/noisy-diffie-hellman-protocols. 2010.

[AH21]   D. Apon and J. Howe. *Attacks on NIST PQC 3rd Round Candidates*. IACR Real World Crypto Symposium. URL: https://iacr.org/submit/files/slides/2021/rwc/rwc2021/22/slides.pdf. 2021.

[AHP+12]   R. Avanzi, S. Hoerder, D. Page, and M. Tunstall. "Erratum to: Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems". In: *Journal of Cryptographic Engineering* 2.1 (May 2012), p. 75. DOI: 10.1007/s13389-011-0026-7.

[Ajt96]   M. Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)". In: *28th ACM STOC*. ACM Press, May 1996, pp. 99–108. DOI: 10.1145/237814.237838.

[AOT+20]   D. F. Aranha, C. Orlandi, A. Takahashi, and G. Zaverucha. "Security of Hedged Fiat-Shamir Signatures Under Fault Attacks". In: *EUROCRYPT*. Ed. by A. Canteaut and Y. Ishai. Vol. 12105. LNCS. Springer, Heidelberg, May 2020, pp. 644–674. DOI: 10.1007/978-3-030-45721-1_23.

[APS15]   M. R. Albrecht, R. Player, and S. Scott. "On the concrete hardness of Learning with Errors". In: *J. Math. Cryptol.* 9.3 (2015), pp. 169–203. URL: http://www.degruyter.com/view/j/jmc.2015.9.issue-3/jmc-2015-0016/jmc-2015-0016.xml.

[ARS+15]   M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner. "Ciphers for MPC and FHE". In: *EUROCRYPT*. Ed. by E. Oswald and M. Fischlin. Vol. 9056. LNCS. Springer, Heidelberg, Apr. 2015, pp. 430–454. DOI: 10.1007/978-3-662-46800-5_17.

[ATT+18]   A. Aysu, Y. Tobah, M. Tiwari, A. Gerstlauer, and M. Orshansky. "Horizontal side-channel vulnerabilities of post-quantum key exchange protocols". In: *HOST*. 2018, pp. 81–88.

[BAA+19]   N. Bindel, S. Akleylek, E. Alkim, P. S. L. M. Barreto, J. Buchmann, E. Eaton, G. Gutoski, J. Kramer, P. Longa, H. Polat, J. E. Ricardini, and G. Zanon. *qTESLA*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[BBD09]   D. J. Bernstein, J. Buchmann, and E. Dahmen, eds. *Post-Quantum Cryptography*. 2009. DOI: 10.1007/978-3-540-88702-7.

[BBE+18]   G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, B. Grégoire, M. Rossi, and M. Tibouchi. "Masking the GLP Lattice-Based Signature Scheme at Any Order". In: *EUROCRYPT*. Ed. by J. B. Nielsen and V. Rijmen. Vol. 10821. LNCS. Springer, Heidelberg, 2018, pp. 354–384. DOI: 10.1007/978-3-319-78375-8_12.

[BBE+19]   G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi, and M. Tibouchi. "GALACTICS: Gaussian Sampling for Lattice-Based Constant-Time Implementation of Cryptographic Signatures, Revisited". In: *ACM CCS*. Ed. by L. Cavallaro, J. Kinder, X. Wang, and J. Katz. ACM Press, Nov. 2019, pp. 2147–2164. DOI: 10.1145/3319535.3363223.

[BBS+18]   M. Backendal, M. Bellare, J. Sorrell, and J. Sun. "The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants". In: *NordSec*. Vol. 11252. Lecture Notes in Computer Science. Springer, 2018, pp. 154–170.

[BCL+19a]   D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wang. *Classic McEliece*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[BCL+19b]   D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal. *NTRU Prime*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[Bd20]   W. Beullens and C. de Saint Guilhem. "LegRoast: Efficient Post-quantum Signatures from the Legendre PRF". In: *Post-Quantum Cryptography - 11th International Conference, PQCrypto*. Ed. by J. Ding and J.-P. Tillich. Springer, Heidelberg, 2020, pp. 130–150. DOI: 10.1007/978-3-030-44223-1_8.

[BDE+11]   J. Buchmann, E. Dahmen, S. Ereth, A. Hülsing, and M. Rückert. "On the Security of the Winternitz One-Time Signature Scheme". In: *AFRICACRYPT 11*. Ed. by

A. Nitaj and D. Pointcheval. Vol. 6737. LNCS. Springer, Heidelberg, July 2011, pp. 363–378.

[BDG20]   M. Bellare, H. Davis, and F. Günther. "Separate Your Domains: NIST PQC KEMs, Oracle Cloning and Read-Only Indifferentiability". In: *EUROCRYPT*. Ed. by A. Canteaut and Y. Ishai. Vol. 12106. LNCS. Springer, Heidelberg, May 2020, pp. 3–32. DOI: 10.1007/978-3-030-45724-2_1.

[BDG+16]   A. Becker, L. Ducas, N. Gama, and T. Laarhoven. "New directions in nearest neighbor searching with applications to lattice sieving". In: *SODA*. Ed. by R. Krauthgamer. SIAM, 2016, pp. 10–24. DOI: 10.1137/1.9781611974331.ch2. URL: https://doi.org/10.1137/1.9781611974331.ch2.

[BDH+21]   S. Bhasin, J.-P. D'Anvers, D. Heinz, T. Pöppelmann, and M. V. Beirendonck. *Attacking and Defending Masked Polynomial Comparison for Lattice-Based Cryptography*. Cryptology ePrint Archive, Report 2021/104. https://eprint.iacr.org/2021/104. 2021.

[BDK+20]   M. V. Beirendonck, J.-P. D'Anvers, A. Karmakar, J. Balasch, and I. Verbauwhede. *A Side-Channel Resistant Implementation of SABER*. Cryptology ePrint Archive, Report 2020/733. https://eprint.iacr.org/2020/733. 2020.

[Beu20]   W. Beullens. "Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes". In: *EUROCRYPT*. Ed. by A. Canteaut and Y. Ishai. Vol. 12107. LNCS. Springer, Heidelberg, May 2020, pp. 183–211. DOI: 10.1007/978-3-030-45727-3_7.

[BFG+19]   J. Brendel, M. Fischlin, F. Günther, C. Janson, and D. Stebila. *Challenges in Proving Post-Quantum Key Exchanges Based on Key Encapsulation Mechanisms*. Cryptology ePrint Archive, Report 2019/1356. https://eprint.iacr.org/2019/1356. 2019.

[BFK+19]   W. Beullens, J.-C. Faugère, E. Koussa, G. Macario-Rat, J. Patarin, and L. Perret. "PKP-Based Signature Scheme". In: *INDOCRYPT*. Ed. by F. Hao, S. Ruj, and S. Sen Gupta. Vol. 11898. LNCS. Springer, Heidelberg, Dec. 2019, pp. 3–22. DOI: 10.1007/978-3-030-35423-7_1.

[BFM+19]   J. W. Bos, S. Friedberger, M. Martinoli, E. Oswald, and M. Stam. "Assessing the Feasibility of Single Trace Power Analysis of Frodo". In: *SAC*. Ed. by C. Cid and M. J. Jacobson Jr: vol. 11349. LNCS. Springer, Heidelberg, Aug. 2019, pp. 216–234. DOI: 10.1007/978-3-030-10970-7_10.

[BFP12]   L. Bettale, J. Faugère, and L. Perret. "Solving polynomial systems over finite fields: improved analysis of the hybrid approach". In: *ISSAC*. ACM, 2012, pp. 67–74.

[BFR+18]   P. Bert, P.-A. Fouque, A. Roux-Langlois, and M. Sabt. "Practical Implementation of Ring-SIS/LWE Based Signature and IBE". In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto*. Ed. by T. Lange and R. Steinwandt. Springer, Heidelberg, 2018, pp. 271–291. DOI: 10.1007/978-3-319-79063-3_13.

[BG14]   S. Bai and S. D. Galbraith. "An Improved Compression Technique for Signatures Based on Learning with Errors". In: *CT-RSA*. Ed. by J. Benaloh. Vol. 8366. LNCS. Springer, Heidelberg, Feb. 2014, pp. 28–47. DOI: 10.1007/978-3-319-04852-9_2.

[BHH+15]   D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn. "SPHINCS: Practical Stateless Hash-Based Signatures". In: *EUROCRYPT*. Ed. by E. Oswald and M. Fischlin. Vol. 9056. LNCS. Springer, Heidelberg, Apr. 2015, pp. 368–397. DOI: 10.1007/978-3-662-46800-5_15.

[BHK+19]   D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe. "The SPHINCS+ Signature Framework". In: *ACM CCS*. Ed. by L. Cavallaro, J. Kinder, X. Wang, and J. Katz. ACM Press, Nov. 2019, pp. 2129–2146. DOI: 10.1145/3319535.3363229.

[BHL+16]   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: *CHES*. Ed. by B. Gierlichs and A. Y. Poschmann. Vol. 9813. LNCS. Springer, Heidelberg, Aug. 2016, pp. 323–345. DOI: 10.1007/978-3-662-53140-2_16.

[BIN97]   M. Bellare, R. Impagliazzo, and M. Naor. "Does Parallel Repetition Lower the Error in Computationally Sound Protocols?" In: *38th FOCS*. IEEE Computer Society Press, Oct. 1997, pp. 374–383. DOI: 10.1109/SFCS.1997.646126.

[BKV19]   W. Beullens, T. Kleinjung, and F. Vercauteren. "CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations". In: *ASIACRYPT*. Ed. by S. D. Galbraith and S. Moriai. Vol. 11921. LNCS. Springer, Heidelberg, Dec. 2019, pp. 227–247. DOI: 10.1007/978-3-030-34578-5_9.

[BM17]   B. Barak and M. Mahmoody-Ghidary. "Merkle's Key Agreement Protocol is Optimal: An $O(n^2)$ Attack on Any Key Agreement from Random Oracles". In: *Journal of Cryptology* 30.3 (July 2017), pp. 699–734. DOI: 10.1007/s00145-016-9233-9.

[BM18]   L. Both and A. May. "Decoding Linear Codes with High Error Rate and Its Impact for LPN Security". In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto*. Ed. by T. Lange and R. Steinwandt. Springer, Heidelberg, 2018, pp. 25–46. DOI: 10.1007/978-3-319-79063-3_2.

[BN20]   C. Baum and A. Nof. "Concretely-Efficient Zero-Knowledge Arguments for Arithmetic Circuits and Their Application to Lattice-Based Cryptography". In: *PKC*. Ed. by A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas. Vol. 12110. LNCS. Springer, Heidelberg, May 2020, pp. 495–526. DOI: 10.1007/978-3-030-45374-9_17.

[BP18]   L. G. Bruinderink and P. Pessl. "Differential Fault Attacks on Deterministic Lattice Signatures". In: *IACR TCHES* 2018.3 (2018). https://tches.iacr.org/index.php/TCHES/article/view/7267, pp. 21–43. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i3.21-43.

[BPO+20]   F. Bache, C. Paglialonga, T. Oder, T. Schneider, and T. Güneysu. "High-Speed Masking for Polynomial Comparison in Lattice-based KEMs". In: *IACR TCHES* 2020.3 (2020). https://tches.iacr.org/index.php/TCHES/article/view/8598, pp. 483–507. ISSN: 2569-2925. DOI: 10.13154/tches.v2020.i3.483-507.

[BPS19]   W. Beullens, B. Preneel, and A. Szepieniec. "Public Key Compression for Constrained Linear Signature Schemes". In: *SAC*. Ed. by C. Cid and M. J. Jacobson Jr: vol. 11349. LNCS. Springer, Heidelberg, Aug. 2019, pp. 300–321. DOI: 10.1007/978-3-030-10970-7_14.

[BR93]   M. Bellare and P. Rogaway. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols". In: *ACM CCS 93*. Ed. by D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, and V. Ashby. ACM Press, Nov. 1993, pp. 62–73. DOI: 10.1145/168588.168596.

[BR96]   M. Bellare and P. Rogaway. "The Exact Security of Digital Signatures: How to Sign with RSA and Rabin". In: *EUROCRYPT'96*. Ed. by U. M. Maurer. Vol. 1070. LNCS. Springer, Heidelberg, May 1996, pp. 399–416. DOI: 10.1007/3-540-68339-9_34.

[BS20]   X. Bonnetain and A. Schrottenloher. "Quantum Security Analysis of CSIDH". In: *EUROCRYPT*. Ed. by A. Canteaut and Y. Ishai. Vol. 12106. LNCS. Springer, Heidelberg, May 2020, pp. 493–522. DOI: `10.1007/978-3-030-45724-2_17`.

[BSGK+21]   C. Baum, C. D. de Saint Guilhem, D. Kales, E. Orsini, P. Scholl, and G. Zaverucha. *Banquet: Short and Fast Signatures from AES*. PKC. `https://eprint.iacr.org/2021/068`. 2021.

[BSI18]   G. F. O. for Information Security (BSI). *BSI Magazine 2018/02*. `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2018-02.html`. (accessed August 31, 2020).

[BSI21]   G. F. O. for Information Security (BSI). *BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths*. `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf`. (accessed August 31, 2020).

[BUC19]   U. Banerjee, T. S. Ukyab, and A. P. Chandrakasan. "Sapphire: A Configurable Crypto-Processor for Post-Quantum Lattice-based Protocols". In: *IACR TCHES* 2019.4 (2019). `https://tches.iacr.org/index.php/TCHES/article/view/8344`, pp. 17–61. ISSN: 2569-2925. DOI: `10.13154/tches.v2019.i4.17-61`.

[BY17]   D. J. Bernstein and B.-Y. Yang. *Asymptotically faster quantum algorithms to solve multivariate quadratic equations*. Cryptology ePrint Archive, Report 2017/1206. `https://eprint.iacr.org/2017/1206`. 2017.

[CAD+20]   D. Cooper, D. Apon, Q. Dang, M. Davidson, M. Dworkin, and C. Miller. *Recommendation for Stateful Hash-Based Signature Schemes*. `https://doi.org/10.6028/NIST.SP.800-208`. 2020.

[CCCS20]   C. C. for Cyber Security (CCCS). *Addressing the Quantum Computing Threat to Cryptography (ITSE.00.017)*. `https://www.cyber.gc.ca/en/guidance/addressing-quantum-computing-threat-cryptography-itse00017`. (accessed August 31, 2020).

[CCD+21]   P.-L. Cayrel, B. Colombier, V.-F. Dragoi, A. Menu, and L. Bossuet. "Message-recovery Laser Fault Injection Attack on the Classic McEliece Cryptosystem". In: *EUROCRYPT*. 2021.

[CD20]   A. Chailloux and T. Debris-Alazard. "Tight and Optimal Reductions for Signatures Based on Average Trapdoor Preimage Sampleable Functions and Applications to Code-Based Signatures". In: *PKC*. Ed. by A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas. Vol. 12111. LNCS. Springer, Heidelberg, May 2020, pp. 453–479. DOI: `10.1007/978-3-030-45388-6_16`.

[CDG+17]   M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha. "Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives". In: *ACM CCS*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press, 2017, pp. 1825–1842. DOI: `10.1145/3133956.3133997`.

[CFM+19]   A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. *GeMSS*. Tech. rep. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions`. National Institute of Standards and Technology, 2019.

[CFS01]   N. Courtois, M. Finiasz, and N. Sendrier. "How to Achieve a McEliece-Based Digital Signature Scheme". In: *ASIACRYPT*. Ed. by C. Boyd. Vol. 2248. LNCS. Springer, Heidelberg, Dec. 2001, pp. 157–174. DOI: `10.1007/3-540-45682-1_10`.

[CGM19]   Y. Chen, N. Genise, and P. Mukherjee. "Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures". In: *ASIACRYPT*. Ed. by S. D. Galbraith

and S. Moriai. Vol. 11923. LNCS. Springer, Heidelberg, Dec. 2019, pp. 3–32. DOI: [10.1007/978-3-030-34618-8_1](10.1007/978-3-030-34618-8_1).

[Che19]   L. Chen. *Update on Standardization of Quantum-Resistant Cryptography in ISO/IEC JTC1 SC27*. 7th ETSI QSC/IQC Workshop. https://docbox.etsi.org/Workshop/2019/201911_QSCWorkshop/TECHNICAL_TRACK/02_COLLABORATIVEEFFORTS/ISO_IECJTC1SC27_CHEN.pdf. 2019.

[CHK+20]   C.-M. M. Chung, V. Hwang, M. J. Kannwischer, G. Seiler, C.-J. Shih, and B.-Y. Yang. *NTT Multiplication for NTT-unfriendly Rings*. Cryptology ePrint Archive, Report 2020/1397. https://eprint.iacr.org/2020/1397. 2020.

[CHR+16]   M.-S. Chen, A. Hülsing, J. Rijneveld, S. Samardjiska, and P. Schwabe. "From 5-Pass MQ-Based Identification to MQ-Based Signatures". In: *ASIACRYPT*. Ed. by J. H. Cheon and T. Takagi. Vol. 10032. LNCS. Springer, Heidelberg, Dec. 2016, pp. 135–165. DOI: [10.1007/978-3-662-53890-6_5](10.1007/978-3-662-53890-6_5).

[CKP+00]   N. Courtois, A. Klimov, J. Patarin, and A. Shamir. "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations". In: *EURO-CRYPT*. Ed. by B. Preneel. Vol. 1807. LNCS. Springer, Heidelberg, May 2000, pp. 392–407. DOI: [10.1007/3-540-45539-6_27](10.1007/3-540-45539-6_27).

[CLM+18]   W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *ASIACRYPT*. Ed. by T. Peyrin and S. Galbraith. Vol. 11274. LNCS. Springer, Heidelberg, Dec. 2018, pp. 395–427. DOI: [10.1007/978-3-030-03332-3_15](10.1007/978-3-030-03332-3_15).

[CMP18]   L. Castelnovi, A. Martinelli, and T. Prest. "Grafting Trees: A Fault Attack Against the SPHINCS Framework". In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto*. Ed. by T. Lange and R. Steinwandt. Springer, Heidelberg, 2018, pp. 165–184. DOI: [10.1007/978-3-319-79063-3_8](10.1007/978-3-319-79063-3_8).

[CNS17]   A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher. "An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography". In: *ASIACRYPT*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. LNCS. Springer, Heidelberg, Dec. 2017, pp. 211–240. DOI: [10.1007/978-3-319-70697-9_8](10.1007/978-3-319-70697-9_8).

[Cop97]   D. Coppersmith. "Small Solutions to Polynomial Equations, and Low Exponent RSA Vulnerabilities". In: *Journal of Cryptology* 10.4 (Sept. 1997), pp. 233–260. DOI: [10.1007/s001459900030](10.1007/s001459900030).

[Cor00]   J.-S. Coron. "On the Exact Security of Full Domain Hash". In: *CRYPTO*. Ed. by M. Bellare. Vol. 1880. LNCS. Springer, Heidelberg, Aug. 2000, pp. 229–235. DOI: [10.1007/3-540-44598-6_14](10.1007/3-540-44598-6_14).

[Cou06]   J.-M. Couveignes. *Hard Homogeneous Spaces*. Cryptology ePrint Archive, Report 2006/291. http://eprint.iacr.org/2006/291. 2006.

[CS21]   L. Chen and H. Shi. *Quantum-Safe Standards in ISO/IEC JTC1 SC27*. ETSI Quantum Safe Cryptography Technical Event. 2021.

[Dam90]   I. Damgård. "On the Randomness of Legendre and Jacobi Sequences". In: *CRYPTO'88*. Ed. by S. Goldwasser. Vol. 403. LNCS. Springer, Heidelberg, Aug. 1990, pp. 163–172. DOI: [10.1007/0-387-34799-2_13](10.1007/0-387-34799-2_13).

[DCP+19]   J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, and B.-Y. Yang. *Rainbow*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[DDG+20]   D. Dachman-Soled, L. Ducas, H. Gong, and M. Rossi. "LWE with Side Information: Attacks and Concrete Security Estimation". In: *CRYPTO*. Ed. by D. Micciancio and T. Ristenpart. Vol. 12171. LNCS. Springer, Heidelberg, Aug. 2020, pp. 329–358. DOI: [10.1007/978-3-030-56880-1_12](10.1007/978-3-030-56880-1_12).

[dDO+19]   C. de Saint Guilhem, L. De Meyer, E. Orsini, and N. P. Smart. "BBQ: Using AES in Picnic Signatures". In: *SAC*. Ed. by K. G. Paterson and D. Stebila. Vol. 11959. LNCS. Springer, Heidelberg, Aug. 2019, pp. 669–692. DOI: 10.1007/978-3-030-38471-5_27.

[DG19]   L. De Feo and S. D. Galbraith. "SeaSign: Compact Isogeny Signatures from Class Group Actions". In: *EUROCRYPT*. Ed. by Y. Ishai and V. Rijmen. Vol. 11478. LNCS. Springer, Heidelberg, May 2019, pp. 759–789. DOI: 10.1007/978-3-030-17659-4_26.

[DGJ+19]   J.-P. D'Anvers, Q. Guo, T. Johansson, A. Nilsson, F. Vercauteren, and I. Verbauwhede. "Decryption Failure Attacks on IND-CCA Secure Lattice-Based Schemes". In: *PKC*. Ed. by D. Lin and K. Sako. Vol. 11443. LNCS. Springer, Heidelberg, Apr. 2019, pp. 565–598. DOI: 10.1007/978-3-030-17259-6_19.

[DH76]   W. Diffie and M. E. Hellman. "New Directions in Cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654.

[Die04]   C. Diem. "The XL-Algorithm and a Conjecture from Commutative Algebra". In: *ASIACRYPT*. Ed. by P. J. Lee. Vol. 3329. LNCS. Springer, Heidelberg, Dec. 2004, pp. 323–337. DOI: 10.1007/978-3-540-30539-2_23.

[Din19]   J. Ding. *The latest progress of PQC competition in China*. 7th ETSI QSC/IQC Workshop. https://docbox.etsi.org/Workshop/2019/201911_QSCWorkshop/TECHNICAL_TRACK/02_COLLABORATIVEEFFORTS/DING_CHONGQINGUNIVERSITY.pdf. 2019.

[DKL+20]   L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski. "SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies". In: *ASIACRYPT*. Ed. by S. Moriai and H. Wang. Vol. 12491. LNCS. Springer, Heidelberg, Dec. 2020, pp. 64–93. DOI: 10.1007/978-3-030-64837-4_3.

[DKP+19]   I. Dinur, D. Kales, A. Promitzer, S. Ramacher, and C. Rechberger. "Linear Equivalence of Block Ciphers with Partial Non-Linear Layers: Application to LowMC". In: *EUROCRYPT*. Ed. by Y. Ishai and V. Rijmen. Vol. 11476. LNCS. Springer, Heidelberg, May 2019, pp. 343–372. DOI: 10.1007/978-3-030-17653-2_12.

[DKR+19]   J.-P. D'Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren. *SABER*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[DKS18]   L. De Feo, J. Kieffer, and B. Smith. "Towards Practical Key Exchange from Ordinary Isogeny Graphs". In: *ASIACRYPT*. Ed. by T. Peyrin and S. Galbraith. Vol. 11274. LNCS. Springer, Heidelberg, Dec. 2018, pp. 365–394. DOI: 10.1007/978-3-030-03332-3_14.

[DLP14]   L. Ducas, V. Lyubashevsky, and T. Prest. "Efficient Identity-Based Encryption over NTRU Lattices". In: *ASIACRYPT*. Ed. by P. Sarkar and T. Iwata. Vol. 8874. LNCS. Springer, Heidelberg, Dec. 2014, pp. 22–41. DOI: 10.1007/978-3-662-45608-8_2.

[DLP+12]   J. P. Degabriele, A. Lehmann, K. G. Paterson, N. P. Smart, and M. Strefler. "On the Joint Security of Encryption and Signature in EMV". In: *CT-RSA*. Ed. by O. Dunkelman. Vol. 7178. LNCS. Springer, Heidelberg, 2012, pp. 116–135. DOI: 10.1007/978-3-642-27954-6_8.

[DN12]   L. Ducas and P. Q. Nguyen. "Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures". In: *ASIACRYPT*. Ed. by X. Wang and K. Sako. Vol. 7658. LNCS. Springer, Heidelberg, Dec. 2012, pp. 433–450. DOI: 10.1007/978-3-642-34961-4_27.

[DRV20]   J.-P. D'Anvers, M. Rossi, and F. Virdia. "(One) Failure Is Not an Option: Boot-strapping the Search for Failures in Lattice-Based Encryption Schemes". In: *EU-ROCRYPT*. Ed. by A. Canteaut and Y. Ishai. Vol. 12107. LNCS. Springer, Heidelberg, May 2020, pp. 3–33. DOI: 10.1007/978-3-030-45727-3_1.

[DST19]   T. Debris-Alazard, N. Sendrier, and J.-P. Tillich. "Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes". In: *ASI-ACRYPT*. Ed. by S. D. Galbraith and S. Moriai. Vol. 11921. LNCS. Springer, Heidelberg, Dec. 2019, pp. 21–51. DOI: 10.1007/978-3-030-34578-5_2.

[DT18]   T. Debris-Alazard and J.-P. Tillich. "Two Attacks on Rank Metric Code-Based Schemes: RankSign and an IBE Scheme". In: *ASIACRYPT*. Ed. by T. Peyrin and S. Galbraith. Vol. 11272. LNCS. Springer, Heidelberg, Dec. 2018, pp. 62–92. DOI: 10.1007/978-3-030-03326-2_3.

[DTV+19]   J. D'Anvers, M. Tiepelt, F. Vercauteren, and I. Verbauwhede. "Timing Attacks on Error Correcting Codes in Post-Quantum Schemes". In: *TIS@CCS*. Ed. by B. Bilgin, S. Petkova-Nikova, and V. Rijmen. ACM, 2019, pp. 2–9. DOI: 10.1145/3338467.3358948. URL: https://doi.org/10.1145/3338467.3358948.

[DVV19]   J.-P. D'Anvers, F. Vercauteren, and I. Verbauwhede. "The Impact of Error Dependencies on Ring/Mod-LWE/LWR Based Schemes". In: *Post-Quantum Cryptography - 10th International Conference, PQCrypto*. Ed. by J. Ding and R. Steinwandt. Springer, Heidelberg, 2019, pp. 103–115. DOI: 10.1007/978-3-030-25510-7_6.

[DXL12]   J. Ding, X. Xie, and X. Lin. *A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem*. Cryptology ePrint Archive, Report 2012/688. http://eprint.iacr.org/2012/688. 2012.

[EAMK20]   R. Elkhatib, R. Azarderakhsh, and M. Mozaffari-Kermani. *Efficient and Fast Hardware Architectures for SIKE Round 2 on FPGA*. Cryptology ePrint Archive, Report 2020/611. 2020.

[EFG+17]   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: *ACM CCS*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press, 2017, pp. 1857–1874. DOI: 10.1145/3133956.3134028.

[ElG85]   T. ElGamal. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms". In: *IEEE Transactions on Information Theory* 31 (1985), pp. 469–472.

[ELP+18]   E. Eaton, M. Lequesne, A. Parent, and N. Sendrier. "QC-MDPC: A Timing Attack and a CCA2 KEM". In: *Post-Quantum Cryptography - 9th International Conference, PQCrypto*. Ed. by T. Lange and R. Steinwandt. Springer, Heidelberg, 2018, pp. 47–76. DOI: 10.1007/978-3-319-79063-3_3.

[ETSI20]   E. T. S. I. (ETSI). *ETSI Work Programme 2020-2021 - Connecting with to-morrow*. 7th ETSI QSC/IQC Workshop. https://www.etsi.org/media-library/work-programme-and-annual-reports. 2020.

[fail10]   fail0verflow. "Console Hacking 2010: PS3 Epic Fail". In: *27th Chaos Communications Congress*. 2010.

[Fau02]   J. C. Faugère. "A New Efficient Algorithm for Computing GröBner Bases without Reduction to Zero (F5)". In: *ISSAC*. ISSAC '02. Lille, France: Association for Computing Machinery, 2002, pp. 7583. ISBN: 1581134843. DOI: 10.1145/780506.780516.

[Fed21]   A. Fedorov. *Quantum Communication Activities in Russia*. ETSI Quantum Safe
             Cryptography Technical Event. 2021.

[Feo17]   L. D. Feo. *Mathematics of Isogeny Based Cryptography*. 2017. arXiv: 1711.04062
             [cs.CR].

[FGO+13]   J. Faugère, V. Gauthier-Umaña, A. Otmani, L. Perret, and J. Tillich. "A Dis-
             tinguisher for High-Rate McEliece Cryptosystems". In: *IEEE Trans. Inf. Theory*
             59.10 (2013), pp. 6830–6844.

[FJP14]   L. D. Feo, D. Jao, and J. Plût. "Towards quantum-resistant cryptosystems from
             supersingular elliptic curve isogenies". In: *Journal of Mathematical Cryptology*
             8.3 (2014), pp. 209–247.

[Flu16]   S. Fluhrer. *Cryptanalysis of ring-LWE based key exchange with key share reuse*.
             Cryptology ePrint Archive, Report 2016/085. http://eprint.iacr.org/2016/
             085. 2016.

[FMP+11]   G. Fumaroli, A. Martinelli, E. Prouff, and M. Rivain. "Affine Masking against
             Higher-Order Side Channel Analysis". In: *SAC*. Ed. by A. Biryukov, G. Gong,
             and D. R. Stinson. Vol. 6544. LNCS. Springer, Heidelberg, Aug. 2011, pp. 262–
             280. DOI: 10.1007/978-3-642-19574-7_18.

[FS87]   A. Fiat and A. Shamir. "How to Prove Yourself: Practical Solutions to Identifica-
             tion and Signature Problems". In: *CRYPTO'86*. Ed. by A. M. Odlyzko. Vol. 263.
             LNCS. Springer, Heidelberg, Aug. 1987, pp. 186–194. DOI: 10.1007/3-540-
             47721-7_12.

[GGH97]   O. Goldreich, S. Goldwasser, and S. Halevi. "Public-Key Cryptosystems from
             Lattice Reduction Problems". In: *CRYPTO'97*. Ed. by B. S. Kaliski Jr. Vol. 1294.
             LNCS. Springer, Heidelberg, Aug. 1997, pp. 112–131. DOI: 10.1007/BFb0052231.

[GJN20]   Q. Guo, T. Johansson, and A. Nilsson. "A Key-Recovery Timing Attack on
             Post-quantum Primitives Using the Fujisaki-Okamoto Transformation and Its
             Application on FrodoKEM". In: *CRYPTO*. Ed. by D. Micciancio and T. Ris-
             tenpart. Vol. 12171. LNCS. Springer, Heidelberg, Aug. 2020, pp. 359–386. DOI:
             10.1007/978-3-030-56880-1_13.

[GJS16]   Q. Guo, T. Johansson, and P. Stankovski. "A Key Recovery Attack on MDPC
             with CCA Security Using Decoding Errors". In: *ASIACRYPT*. Ed. by J. H. Cheon
             and T. Takagi. Vol. 10031. LNCS. Springer, Heidelberg, Dec. 2016, pp. 789–815.
             DOI: 10.1007/978-3-662-53887-6_29.

[GJS+01]   C. Gentry, J. Jonsson, J. Stern, and M. Szydlo. "Cryptanalysis of the NTRU
             Signature Scheme (NSS) from Eurocrypt 2001". In: *ASIACRYPT*. Ed. by C.
             Boyd. Vol. 2248. LNCS. Springer, Heidelberg, Dec. 2001, pp. 1–20. DOI: 10.
             1007/3-540-45682-1_1.

[GJY19]   Q. Guo, T. Johansson, and J. Yang. "A Novel CCA Attack Using Decryption
             Errors Against LAC". In: *ASIACRYPT*. Ed. by S. D. Galbraith and S. Moriai.
             Vol. 11921. LNCS. Springer, Heidelberg, Dec. 2019, pp. 82–111. DOI: 10.1007/
             978-3-030-34578-5_4.

[GKR+20]   S. Guo, P. Kamath, A. Rosen, and K. Sotiraki. "Limits on the Efficiency of
             (Ring) LWE Based Non-interactive Key Exchange". In: *PKC*. Ed. by A. Kiayias,
             M. Kohlweiss, P. Wallden, and V. Zikas. Vol. 12110. LNCS. Springer, Heidelberg,
             May 2020, pp. 374–395. DOI: 10.1007/978-3-030-45374-9_13.

[GLP12]   T. Güneysu, V. Lyubashevsky, and T. Pöppelmann. "Practical Lattice-Based
             Cryptography: A Signature Scheme for Embedded Systems". In: *CHES*. Ed. by
             E. Prouff and P. Schaumont. Vol. 7428. LNCS. Springer, Heidelberg, Sept. 2012,
             pp. 530–547. DOI: 10.1007/978-3-642-33027-8_31.

[Gol87]   O. Goldreich. "Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme". In: *CRYPTO'86*. Ed. by A. M. Odlyzko. Vol. 263. LNCS. Springer, Heidelberg, Aug. 1987, pp. 104–110. DOI: 10.1007/3-540-47721-7_8.

[GPS+16]   S. D. Galbraith, C. Petit, B. Shani, and Y. B. Ti. "On the Security of Supersingular Isogeny Cryptosystems". In: *ASIACRYPT*. Ed. by J. H. Cheon and T. Takagi. Vol. 10031. LNCS. Springer, Heidelberg, Dec. 2016, pp. 63–91. DOI: 10.1007/978-3-662-53887-6_3.

[GPS+18]   S. Galbraith, L. Panny, B. Smith, and F. Vercauteren. *Quantum Equivalence of the DLP and CDHP for Group Actions*. Cryptology ePrint Archive, Report 2018/1199. https://eprint.iacr.org/2018/1199. 2018.

[GPT91]   E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. "Ideals over a Non-Commutative Ring and thier Applications in Cryptology". In: *EUROCRYPT'91*. Ed. by D. W. Davies. Vol. 547. LNCS. Springer, Heidelberg, Apr. 1991, pp. 482–489. DOI: 10.1007/3-540-46416-6_41.

[GPV08]   C. Gentry, C. Peikert, and V. Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions". In: *40th ACM STOC*. Ed. by R. E. Ladner and C. Dwork. ACM Press, May 2008, pp. 197–206. DOI: 10.1145/1374376.1374407.

[Gro96]   L. K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *28th ACM STOC*. ACM Press, May 1996, pp. 212–219. DOI: 10.1145/237814.237866.

[GRR+16]   L. Grassi, C. Rechberger, D. Rotaru, P. Scholl, and N. P. Smart. "MPC-Friendly Symmetric Key Primitives". In: *ACM CCS*. Ed. by E. R. Weippl, S. Katzenbeisser, C. Kruegel, A. C. Myers, and S. Halevi. ACM Press, Oct. 2016, pp. 430–443. DOI: 10.1145/2976749.2978332.

[GRS+14]   P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor. "RankSign: An Efficient Signature Algorithm Based on the Rank Metric". In: *Post-Quantum Cryptography - 6th International Workshop, PQCrypto*. Ed. by M. Mosca. Springer, Heidelberg, Oct. 2014, pp. 88–107. DOI: 10.1007/978-3-319-11659-4_6.

[GSE20]   T. Gellersen, O. Seker, and T. Eisenbarth. *Differential Power Analysis of the Picnic Signature Scheme*. Cryptology ePrint Archive, Report 2020/267. https://eprint.iacr.org/2020/267. 2020.

[Ham19]   M. Hamburg. *Three Bears*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[HBD+19]   A. Hulsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, and J.-P. Aumasson. *SPHINCS+*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[HCY20]   W.-L. Huang, J.-P. Chen, and B.-Y. Yang. "Power Analysis on NTRU Prime". In: *IACR TCHES* 2020.1 (2020). ISSN: 2569-2925.

[HGS99]   C. Hall, I. Goldberg, and B. Schneier. "Reaction Attacks against several Public-Key Cryptosystems". In: *ICICS 99*. Ed. by V. Varadharajan and Y. Mu. Vol. 1726. LNCS. Springer, Heidelberg, Nov. 1999, pp. 2–12.

[HHK17]   D. Hofheinz, K. Hövelmanns, and E. Kiltz. "A Modular Analysis of the Fujisaki-Okamoto Transformation". In: *TCC*. Ed. by Y. Kalai and L. Reyzin. Vol. 10677. LNCS. Springer, Heidelberg, Nov. 2017, pp. 341–371. DOI: 10.1007/978-3-319-70500-2_12.

[HHP+03]   J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. H. Silverman, and W. Whyte. "NTRUSIGN: Digital Signatures Using the NTRU Lattice". In: *CT-RSA*. Ed. by M. Joye. Vol. 2612. LNCS. Springer, Heidelberg, Apr. 2003, pp. 122–140. DOI: 10.1007/3-540-36563-X_9.

[HKK+21]   K. Hashimoto, S. Katsumata, K. Kwiatkowski, and T. Prest. *An Efficient and Generic Construction for Signal's Handshake (X3DH): Post-Quantum, State Leakage Secure, and Deniable.* PKC. 2021.

[HMO+19]   J. Howe, M. Martinoli, E. Oswald, and F. Regazzoni. "Optimised Lattice-Based Key Encapsulation in Hardware". In: *NIST's Second PQC Standardization Conference* (2019).

[HNP+03]   N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer, and W. Whyte. "The Impact of Decryption Failures on the Security of NTRU Encryption". In: *CRYPTO*. Ed. by D. Boneh. Vol. 2729. LNCS. Springer, Heidelberg, Aug. 2003, pp. 226–246. DOI: 10.1007/978-3-540-45146-4_14.

[HNS+20]   A. Hülsing, K.-C. Ning, P. Schwabe, F. Weber, and P. R. Zimmermann. *Post-quantum WireGuard.* Cryptology ePrint Archive, Report 2020/379. https://eprint.iacr.org/2020/379. 2020.

[HOK+18]   J. Howe, T. Oder, M. Krausz, and T. Güneysu. "Standard Lattice-Based Key Encapsulation on Embedded Devices". In: *IACR TCHES* 2018.3 (2018). https://tches.iacr.org/index.php/TCHES/article/view/7279, pp. 372–393. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i3.372-393.

[HPR+20]   J. Howe, T. Prest, T. Ricosset, and M. Rossi. "Isochronous Gaussian Sampling: From Inception to Implementation". In: *Post-Quantum Cryptography - 11th International Conference, PQCrypto.* Ed. by J. Ding and J.-P. Tillich. Springer, Heidelberg, 2020, pp. 53–71. DOI: 10.1007/978-3-030-44223-1_5.

[HPR+21]   A.-L. Horlemann, S. Puchinger, J. Renner, T. Schamberger, and A. Wachter-Zeh. *Information-Set Decoding with Hints.* Cryptology ePrint Archive, Report 2021/279. https://eprint.iacr.org/2021/279. 2021.

[HPS01]   J. Hoffstein, J. Pipher, and J. H. Silverman. "NSS: An NTRU Lattice-Based Signature Scheme". In: *EUROCRYPT*. Ed. by B. Pfitzmann. Vol. 2045. LNCS. Springer, Heidelberg, May 2001, pp. 211–228. DOI: 10.1007/3-540-44987-6_14.

[HPS98]   J. Hoffstein, J. Pipher, and J. H. Silverman. "NTRU: A Ring-Based Public Key Cryptosystem". In: *ANTS*. Ed. by J. Buhler. Vol. 1423. Lecture Notes in Computer Science. Springer, 1998, pp. 267–288. ISBN: 3-540-64657-4. DOI: 10.1007/BFb0054868.

[Hül13]   A. Hülsing. "W-OTS+ - Shorter Signatures for Hash-Based Signature Schemes". In: *AFRICACRYPT 13*. Ed. by A. Youssef, A. Nitaj, and A. E. Hassanien. Vol. 7918. LNCS. Springer, Heidelberg, June 2013, pp. 173–188. DOI: 10.1007/978-3-642-38553-7_10.

[IKO+07]   Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. "Zero-knowledge from secure multiparty computation". In: *39th ACM STOC*. Ed. by D. S. Johnson and U. Feige. ACM Press, June 2007, pp. 21–30. DOI: 10.1145/1250790.1250794.

[JAC+19]   D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, and G. Pereira. *SIKE.* Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[JD11]   D. Jao and L. De Feo. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". In: *Post-Quantum Cryptography - 4th Inter-*

national Workshop, PQCrypto. Ed. by B.-Y. Yang. Springer, Heidelberg, 2011, pp. 19–34. DOI: 10.1007/978-3-642-25405-5_2.

[JNR+20]   S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia. "Implementing Grover Oracles for Quantum Key Search on AES and LowMC". In: *EUROCRYPT.* Ed. by A. Canteaut and Y. Ishai. Vol. 12106. LNCS. Springer, Heidelberg, May 2020, pp. 280–310. DOI: 10.1007/978-3-030-45724-2_10.

[JS19]   S. Jaques and J. M. Schanck. "Quantum Cryptanalysis in the RAM Model: Claw-Finding Attacks on SIKE". In: *CRYPTO.* Ed. by A. Boldyreva and D. Micciancio. Vol. 11692. LNCS. Springer, Heidelberg, Aug. 2019, pp. 32–61. DOI: 10.1007/978-3-030-26948-7_2.

[JV17]   A. Joux and V. Vitse. *A crossbred algorithm for solving Boolean polynomial systems.* Cryptology ePrint Archive, Report 2017/372. http://eprint.iacr.org/2017/372. 2017.

[KAE+20]   B. Koziel, A. Ackie, R. El Khatib, R. Azarderakhsh, and M. M. Kermani. "SIKE'd Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* (2020), pp. 1–13.

[KKW18]   J. Katz, V. Kolesnikov, and X. Wang. "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures". In: *ACM CCS.* Ed. by D. Lie, M. Mannan, M. Backes, and X. Wang. ACM Press, Oct. 2018, pp. 525–537. DOI: 10.1145/3243734.3243805.

[KPP20]   M. J. Kannwischer, P. Pessl, and R. Primas. "Single-Trace Attacks on Keccak". In: *IACR TCHES* 2020.3 (2020). https://tches.iacr.org/index.php/TCHES/article/view/8590, pp. 243–268. ISSN: 2569-2925. DOI: 10.13154/tches.v2020.i3.243-268.

[KRR+20]   D. Kales, S. Ramacher, C. Rechberger, R. Walch, and M. Werner. "Efficient FPGA Implementations of LowMC and Picnic". In: *CT-RSA.* Ed. by S. Jarecki. Vol. 12006. LNCS. Springer, Heidelberg, Feb. 2020, pp. 417–441. DOI: 10.1007/978-3-030-40186-3_18.

[KRS+19]   M. J. Kannwischer, J. Rijneveld, P. Schwabe, and K. Stoffelen. *pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4.* Cryptology ePrint Archive, Report 2019/844. https://eprint.iacr.org/2019/844. 2019.

[Kup05]   G. Kuperberg. "A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem". In: *SIAM J. Comput.* 35.1 (2005), pp. 170–188. DOI: 10.1137/S0097539703436345.

[Kup13]   G. Kuperberg. "Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem". In: *TQC.* Ed. by S. Severini and F. G. S. L. Brandão. Vol. 22. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2013, pp. 20–34. DOI: 10.4230/LIPIcs.TQC.2013.20.

[KW16]   H. Krawczyk and H. Wee. "The OPTLS Protocol and TLS 1.3". In: *2016 IEEE European Symposium on Security and Privacy (EuroS P).* 2016, pp. 81–96. DOI: 10.1109/EuroSP.2016.18.

[KZ20]   D. Kales and G. Zaverucha. *An Attack on Some Signature Schemes Constructed From Five-Pass Identification Schemes.* Cryptology ePrint Archive, Report 2020/837. https://eprint.iacr.org/2020/837. 2020.

[Lam79]   L. Lamport. *Constructing Digital Signatures from a One-way Function.* Technical Report SRI-CSL-98. SRI International Computer Science Laboratory, Oct. 1979.

[LDK+19]   V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, and D. Stehlé. *CRYSTALS-DILITHIUM.* Tech. rep. available at https://csrc.nist.

gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[LIM20]   F. Liu, T. Isobe, and W. Meier. *Cryptanalysis of Full LowMC and LowMC-M with Algebraic Techniques.* Cryptology ePrint Archive, Report 2020/1034. https://eprint.iacr.org/2020/1034. 2020.

[LLZ⁺18]   X. Lu, Y. Liu, Z. Zhang, D. Jia, H. Xue, J. He, B. Li, and K. Wang. *LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus.* Cryptology ePrint Archive, Report 2018/1009. https://eprint.iacr.org/2018/1009. 2018.

[LMP15]   T. Laarhoven, M. Mosca, and J. van de Pol. "Finding shortest lattice vectors faster using quantum search". In: *Des. Codes Cryptogr.* 77.2-3 (2015), pp. 375–400. DOI: 10.1007/s10623-015-0067-5. URL: https://doi.org/10.1007/s10623-015-0067-5.

[LNP⁺20]   N. Lahr, R. Niederhagen, R. Petri, and S. Samardjiska. "Side Channel Information Set Decoding Using Iterative Chunking - Plaintext Recovery from the "Classic McEliece" Hardware Reference Implementation". In: *ASIACRYPT*. Ed. by S. Moriai and H. Wang. Vol. 12491. LNCS. Springer, Heidelberg, Dec. 2020, pp. 881–910. DOI: 10.1007/978-3-030-64837-4_29.

[LPR10]   V. Lyubashevsky, C. Peikert, and O. Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *EUROCRYPT*. Ed. by H. Gilbert. Vol. 6110. LNCS. Springer, Heidelberg, 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1.

[LS15]   A. Langlois and D. Stehlé. "Worst-case to average-case reductions for module lattices". In: *Des. Codes Cryptogr.* 75.3 (2015), pp. 565–599. DOI: 10.1007/s10623-014-9938-4. URL: https://doi.org/10.1007/s10623-014-9938-4.

[Lyu09]   V. Lyubashevsky. "Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures". In: *ASIACRYPT*. Ed. by M. Matsui. Vol. 5912. LNCS. Springer, Heidelberg, Dec. 2009, pp. 598–616. DOI: 10.1007/978-3-642-10366-7_35.

[Mar20]   A. Marotzke. "A Constant Time Full Hardware Implementation of Streamlined NTRU Prime". In: *International Conference on Smart Card Research and Advanced Applications.* Springer. 2020, pp. 3–17.

[McE78]   R. J. McEliece. "A Public-Key Cryptosystem Based on Algebraic Coding Theory". In: *JPL DSN Progress Report* 44 (May 1978).

[Mer90]   R. C. Merkle. "A Certified Digital Signature". In: *CRYPTO'89*. Ed. by G. Brassard. Vol. 435. LNCS. Springer, Heidelberg, Aug. 1990, pp. 218–238. DOI: 10.1007/0-387-34805-0_21.

[MGT⁺19]   V. Migliore, B. Gérard, M. Tibouchi, and P.-A. Fouque. "Masking Dilithium - Efficient Implementation and Side-Channel Evaluation". In: *ACNS 19*. Ed. by R. H. Deng, V. Gauthier-Umaña, M. Ochoa, and M. Yung. Vol. 11464. LNCS. Springer, Heidelberg, June 2019, pp. 344–362. DOI: 10.1007/978-3-030-21568-2_17.

[MIS20]   K. Mus, S. Islam, and B. Sunar. "QuantumHammer: A Practical Hybrid Attack on the LUOV Signature Scheme". In: *ACM CCS 20*. Ed. by J. Ligatti, X. Ou, J. Katz, and G. Vigna. ACM Press, Nov. 2020, pp. 1071–1084. DOI: 10.1145/3372297.3417272.

[MLR⁺20]   P. M. C. Massolino, P. Longa, J. Renes, and L. Batina. "A Compact and Scalable Hardware/Software Co-design of SIKE". In: *IACR TCHES* 2020.2 (2020). https://tches.iacr.org/index.php/TCHES/article/view/8551, pp. 245–271. ISSN: 2569-2925. DOI: 10.13154/tches.v2020.i2.245-271.

[MP12]   D. Micciancio and C. Peikert. "Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller". In: *EUROCRYPT*. Ed. by D. Pointcheval and T. Johansson. Vol. 7237. LNCS. Springer, Heidelberg, Apr. 2012, pp. 700–718. DOI: 10.1007/978-3-642-29011-4_41.

[NAB+19]   M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. *FrodoKEM*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[NCSC20]   N. C. S. C. (NCSC). *Quantum-Safe Cryptography*. https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography. (accessed August 31, 2020).

[NIS16]   NIST. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf. 2016.

[NR06]   P. Q. Nguyen and O. Regev. "Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures". In: *EUROCRYPT*. Ed. by S. Vaudenay. Vol. 4004. LNCS. Springer, Heidelberg, 2006, pp. 271–288. DOI: 10.1007/11761679_17.

[NSA20]   N. S. A. (NSA). *Post-Quantum Cybersecurity Resources*. https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/. (accessed August 31, 2020).

[OM07]   E. Oswald and S. Mangard. "Template Attacks on Masking - Resistance Is Futile". In: *CT-RSA*. Ed. by M. Abe. Vol. 4377. LNCS. Springer, Heidelberg, Feb. 2007, pp. 243–256. DOI: 10.1007/11967668_16.

[OSP+18]   T. Oder, T. Schneider, T. Pöppelmann, and T. Güneysu. "Practical CCA2-Secure Masked Ring-LWE Implementations". In: *IACR TCHES* 2018.1 (2018). https://tches.iacr.org/index.php/TCHES/article/view/836, pp. 142–174. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i1.142-174.

[PBY17]   P. Pessl, L. G. Bruinderink, and Y. Yarom. "To BLISS-B or not to be: Attacking strongSwan's Implementation of Post-Quantum Signatures". In: *ACM CCS*. Ed. by B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu. ACM Press, 2017, pp. 1843–1855. DOI: 10.1145/3133956.3134023.

[Pec19]   M. Pecan. *Report from ETSI Cyber Working Group for QuantumSafe Cryptography*. 7th ETSI QSC/IQC Workshop. https://docbox.etsi.org/Workshop/2019/201911_QSCWorkshop/TECHNICAL_TRACK/02_COLLABORATIVEEFFORTS/ETSICYBERQSC_PECEN.pdf. 2019.

[Pei14]   C. Peikert. "Lattice Cryptography for the Internet". In: *Post-Quantum Cryptography - 6th International Workshop, PQCrypto*. Ed. by M. Mosca. Springer, Heidelberg, Oct. 2014, pp. 197–219. DOI: 10.1007/978-3-319-11659-4_12.

[Pei15]   C. Peikert. *A Decade of Lattice Cryptography*. Cryptology ePrint Archive, Report 2015/939. http://eprint.iacr.org/2015/939. 2015.

[Pei16]   C. Peikert. "How (Not) to Instantiate Ring-LWE". In: *SCN 16*. Ed. by V. Zikas and R. De Prisco. Vol. 9841. LNCS. Springer, Heidelberg, 2016, pp. 411–430. DOI: 10.1007/978-3-319-44618-9_22.

[Pei20]   C. Peikert. "He Gives C-Sieves on the CSIDH". In: *EUROCRYPT*. Ed. by A. Canteaut and Y. Ishai. Vol. 12106. LNCS. Springer, Heidelberg, May 2020, pp. 463–492. DOI: 10.1007/978-3-030-45724-2_16.

[Per01]   A. Perrig. "The BiBa One-Time Signature and Broadcast Authentication Protocol". In: *ACM CCS*. Ed. by M. K. Reiter and P. Samarati. ACM Press, Nov. 2001, pp. 28–37. DOI: 10.1145/501983.501988.

[PFH+19]   T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. *FALCON*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[Pol18]   R. L. V. Polanco. "Cold Boot Attacks on Post-Quantum Schemes". PhD thesis. Royal Holloway, University of London, 2018.

[Por19]   T. Pornin. *New Efficient, Constant-Time Implementations of Falcon*. Cryptology ePrint Archive, Report 2019/893. https://eprint.iacr.org/2019/893. 2019.

[PP19]   C. Peikert and Z. Pepin. "Algebraically Structured LWE, Revisited". In: *TCC*. Ed. by D. Hofheinz and A. Rosen. Vol. 11891. LNCS. Springer, Heidelberg, Dec. 2019, pp. 1–23. DOI: 10.1007/978-3-030-36030-6_1.

[Pra62]   E. Prange. "The use of information sets in decoding cyclic codes". In: *IRE Trans. Inf. Theory* 8.5 (1962), pp. 5–9. DOI: 10.1109/TIT.1962.1057777.

[PS96]   D. Pointcheval and J. Stern. "Security Proofs for Signature Schemes". In: *EUROCRYPT'96*. Ed. by U. M. Maurer. Vol. 1070. LNCS. Springer, Heidelberg, May 1996, pp. 387–398. DOI: 10.1007/3-540-68339-9_33.

[PSK+18]   A. Park, K.-A. Shim, N. Koo, and D.-G. Han. "Side-Channel Attacks on Post-Quantum Signature Schemes based on Multivariate Quadratic Equations". In: *IACR TCHES* 2018.3 (2018). https://tches.iacr.org/index.php/TCHES/article/view/7284, pp. 500–523. ISSN: 2569-2925. DOI: 10.13154/tches.v2018.i3.500-523.

[PV17]   K. G. Paterson and R. Villanueva-Polanco. "Cold Boot Attacks on NTRU". In: *INDOCRYPT*. Ed. by A. Patra and N. P. Smart. Vol. 10698. LNCS. Springer, Heidelberg, Dec. 2017, pp. 107–125.

[RB20]   S. S. Roy and A. Basso. "High-speed Instruction-set Coprocessor for Lattice-based Key Encapsulation Mechanism: Saber in Hardware". In: *IACR TCHES* 2020.4 (2020). https://tches.iacr.org/index.php/TCHES/article/view/8690, pp. 443–466. ISSN: 2569-2925. DOI: 10.13154/tches.v2020.i4.443-466.

[RBG20]   J. Richter-Brockmann and T. Güneysu. *Folding BIKE: Scalable Hardware Implementation for Reconfigurable Devices*. Cryptology ePrint Archive, Report 2020/897. https://eprint.iacr.org/2020/897. 2020.

[Reg05]   O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *37th ACM STOC*. Ed. by H. N. Gabow and R. Fagin. ACM Press, May 2005, pp. 84–93. DOI: 10.1145/1060590.1060603.

[RHH+17]   M. Rossi, M. Hamburg, M. Hutter, and M. E. Marson. "A Side-Channel Assisted Cryptanalytic Attack Against QcBits". In: *CHES*. Ed. by W. Fischer and N. Homma. Vol. 10529. LNCS. Springer, Heidelberg, Sept. 2017, pp. 3–23. DOI: 10.1007/978-3-319-66787-4_1.

[RJH+19]   P. Ravi, M. P. Jhanwar, J. Howe, A. Chattopadhyay, and S. Bhasin. "Exploiting determinism in lattice-based signatures: practical fault attacks on pqm4 implementations of NIST candidates". In: *AsiaCCS*. 2019, pp. 427–440.

[RMJ+21]   S. Ricci, L. Malina, P. Jedlicka, D. Smekal, J. Hajny, P. Cibik, and P. Dobias. *Implementing CRYSTALS-Dilithium Signature Scheme on FPGAs*. Cryptology ePrint Archive, Report 2021/108. https://eprint.iacr.org/2021/108. 2021.

[RR02]   L. Reyzin and N. Reyzin. "Better than BiBa: Short one-time signatures with fast signing and verifying". In: *Information Security and Privacy 2002*. Vol. 2384. LNCS. Springer, 2002, pp. 1–47.

[RS06]   A. Rostovtsev and A. Stolbunov. *Public-Key Cryptosystem Based On Isogenies*. Cryptology ePrint Archive, Report 2006/145. http://eprint.iacr.org/2006/145. 2006.

[RSA78]   R. L. Rivest, A. Shamir, and L. M. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the Association for Computing Machinery* 21.2 (1978), pp. 120–126.

[SAB+19]   P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, and D. Stehlé. *CRYSTALS-KYBER*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[SBB+18]   N. Samwel, L. Batina, G. Bertoni, J. Daemen, and R. Susella. "Breaking Ed25519 in WolfSSL". In: *CT-RSA*. Ed. by N. P. Smart. Vol. 10808. LNCS. Springer, Heidelberg, Apr. 2018, pp. 1–20. DOI: 10.1007/978-3-319-76953-0_1.

[Sch90]   C.-P. Schnorr. "Efficient Identification and Signatures for Smart Cards". In: *CRYPTO'89*. Ed. by G. Brassard. Vol. 435. LNCS. Springer, Heidelberg, Aug. 1990, pp. 239–252. DOI: 10.1007/0-387-34805-0_22.

[SCH+19]   S. Samardjiska, M.-S. Chen, A. Hulsing, J. Rijneveld, and P. Schwabe. *MQDSS*. Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[SE94]   C. Schnorr and M. Euchner. "Lattice basis reduction: Improved practical algorithms and solving subset sum problems". In: *Math. Program.* 66 (1994), pp. 181–199. DOI: 10.1007/BF01581144. URL: https://doi.org/10.1007/BF01581144.

[Sha90]   A. Shamir. "An Efficient Identification Scheme Based on Permuted Kernels (Extended Abstract) (Rump Session)". In: *CRYPTO'89*. Ed. by G. Brassard. Vol. 435. LNCS. Springer, Heidelberg, Aug. 1990, pp. 606–609. DOI: 10.1007/0-387-34805-0_54.

[SHB21]   I. A. Seres, M. Horváth, and P. Burcsi. *The Legendre Pseudorandom Function as a Multivariate Quadratic Cryptosystem: Security and Applications*. Cryptology ePrint Archive, Report 2021/182. https://eprint.iacr.org/2021/182. 2021.

[Sho94]   P. W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *35th FOCS*. IEEE Computer Society Press, Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[SKC+19]   B.-Y. Sim, J. Kwon, K. Y. Choi, J. Cho, A. Park, and D.-G. Han. "Novel Side-Channel Attacks on Quasi-Cyclic Code-Based Cryptography". In: *IACR TCHES* 2019.4 (2019). https://tches.iacr.org/index.php/TCHES/article/view/8349, pp. 180–212. ISSN: 2569-2925. DOI: 10.13154/tches.v2019.i4.180-212.

[SKD20]   D. Sikeridis, P. Kampanakis, and M. Devetsikiotis. *Post-Quantum Authentication in TLS 1.3: A Performance Study*. Cryptology ePrint Archive, Report 2020/071. https://eprint.iacr.org/2020/071. 2020.

[SSH11a]   K. Sakumoto, T. Shirai, and H. Hiwatari. "On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack". In: *Post-Quantum Cryptography - 4th International Workshop, PQCrypto*. Ed. by B.-Y. Yang. Springer, Heidelberg, 2011, pp. 68–82. DOI: 10.1007/978-3-642-25405-5_5.

[SSH11b]   K. Sakumoto, T. Shirai, and H. Hiwatari. "Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials". In: *CRYPTO*. Ed. by P. Ro-

gaway. Vol. 6841. LNCS. Springer, Heidelberg, Aug. 2011, pp. 706–723. DOI: 10.1007/978-3-642-22792-9_40.

[SSP+19]   S. Samardjiska, P. Santini, E. Persichetti, and G. Banegas. "A Reaction Attack Against Cryptosystems Based on LRPC Codes". In: *LATINCRYPT*. Ed. by P. Schwabe and N. Thériault. Vol. 11774. LNCS. Springer, Heidelberg, 2019, pp. 197–216. DOI: 10.1007/978-3-030-30530-7_10.

[SSW20]   P. Schwabe, D. Stebila, and T. Wiggers. *Post-quantum TLS without handshake signatures*. Cryptology ePrint Archive, Report 2020/534. https://eprint.iacr.org/2020/534. 2020.

[Ste94]   J. Stern. "A New Identification Scheme Based on Syndrome Decoding". In: *CRYPTO'93*. Ed. by D. R. Stinson. Vol. 773. LNCS. Springer, Heidelberg, Aug. 1994, pp. 13–21. DOI: 10.1007/3-540-48329-2_2.

[Ste96]   J. Stern. "A new paradigm for public key identification". In: *IEEE Trans. Inf. Theory* 42.6 (1996), pp. 1757–1768. DOI: 10.1109/18.556672. URL: https://doi.org/10.1109/18.556672.

[Str10]   F. Strenzke. "A Timing Attack against the Secret Permutation in the McEliece PKC". In: *The Third International Workshop on Post-Quantum Cryptography, PQCRYPTO*. Ed. by N. Sendrier. Springer, Heidelberg, May 2010, pp. 95–107. DOI: 10.1007/978-3-642-12929-2_8.

[Str13]   F. Strenzke. "Timing Attacks against the Syndrome Inversion in Code-Based Cryptosystems". In: *Post-Quantum Cryptography - 5th International Workshop, PQCrypto*. Ed. by P. Gaborit. Springer, Heidelberg, June 2013, pp. 217–230. DOI: 10.1007/978-3-642-38616-9_15.

[Sul19]   N. Sullivan. *IETF protocols and the Crypto Forum Research Group (CFRG)*. 7th ETSI QSC/IQC Workshop. https://docbox.etsi.org/Workshop/2019/201911_QSCWorkshop/TECHNICAL_TRACK/02_COLLABORATIVEEFFORTS/IETF_SULLIVAN.pdf. 2019.

[Szy04]   M. Szydlo. "Merkle Tree Traversal in Log Space and Time". In: *EUROCRYPT*. Ed. by C. Cachin and J. Camenisch. Vol. 3027. LNCS. Springer, Heidelberg, May 2004, pp. 541–554. DOI: 10.1007/978-3-540-24676-3_32.

[TS16]   R. C. Torres and N. Sendrier. "Analysis of Information Set Decoding for a Sublinear Error Weight". In: *Post-Quantum Cryptography - 7th International Workshop, PQCrypto*. Ed. by T. Takagi. Springer, Heidelberg, 2016, pp. 144–161. DOI: 10.1007/978-3-319-29360-8_10.

[Ver19]   K. Verhulst. "Power Analysis and Masking of Saber". MA thesis. Belgium: KU Leuven, 2019.

[Vér96]   P. Véron. "Improved identification schemes based on error-correcting codes". In: *Appl. Algebra Eng. Commun. Comput.* 8.1 (1996), pp. 57–69. DOI: 10.1007/s002000050053. URL: https://doi.org/10.1007/s002000050053.

[vW99]   P. C. van Oorschot and M. J. Wiener. "Parallel Collision Search with Cryptanalytic Applications". In: *Journal of Cryptology* 12.1 (Jan. 1999), pp. 1–28. DOI: 10.1007/PL00003816.

[Wei20]   A. Weibel. *Round 2 Hybrid Post-Quantum TLS Benchmarks*. AWS Security Blog. https://aws.amazon.com/fr/blogs/security/round-2-hybrid-post-quantum-tls-benchmarks/. 2020.

[Xia21]   H. Xiang. *Analysis of the Chinese PQC Competition*. ETSI Quantum Safe Cryptography Technical Event. 2021.

[XL21]   Y. Xing and S. Li. "A Compact Hardware Implementation of CCA-Secure Key Exchange Mechanism CRYSTALS-KYBER on FPGA". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021), pp. 328–356.

[YC04]   B. Yang and J. Chen. "All in the XL Family: Theory and Practice". In: *ICISC*. Vol. 3506. Lecture Notes in Computer Science. Springer, 2004, pp. 67–86.

[YF14]   Y. Yarom and K. Falkner. "FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack". In: *USENIX Security*. Ed. by K. Fu and J. Jung. USENIX Association, Aug. 2014, pp. 719–732.

[ZCD+19]   G. Zaverucha, M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, J. Katz, X. Wang, and V. Kolesnikov. *Picnic.* Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[ZCH+19]   Z. Zhang, C. Chen, J. Hoffstein, W. Whyte, J. M. Schanck, A. Hulsing, J. Rijneveld, P. Schwabe, and O. Danba. *NTRUEncrypt.* Tech. rep. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions. National Institute of Standards and Technology, 2019.

[Zha15]   M. Zhandry. "A note on the quantum collision and set equality problems". In: *Quantum Inf. Comput.* 15.7&8 (2015), pp. 557–567.

[ZYF+20]   J. Zhang, Y. Yu, S. Fan, Z. Zhang, and K. Yang. "Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: KEMs and Signatures of Smaller Sizes". In: *PKC*. Ed. by A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas. Vol. 12111. LNCS. Springer, Heidelberg, May 2020, pp. 37–65. DOI: 10.1007/978-3-030-45388-6_2.