A Survey on Exotic Signatures for Post-Quantum Blockchain: Challenges & Research Directions

MAXIME BUSER, Monash University, Australia
RAFAEL DOWSLEY, Monash University, Australia
MUHAMMED F. ESGIN, Monash University, Australia and CSIRO's Data61, Australia
CLÉMENTINE GRITTI, University of Canterbury, New Zealand
SHABNAM KASRA KERMANSHAHI, RMIT University, Australia
VERONIKA KUCHTA, The University of Queensland, Australia
JASON T. LEGROW, Virginia Polytechnic Institute and State University, United States of America
JOSEPH K. LIU, Monash University, Australia
RAPHAËL C.-W. PHAN, Monash University, Malaysia
AMIN SAKZAD, Monash University, Australia
RON STEINFELD, Monash University, Australia
JIANGSHAN YU, Monash University, Australia

Blockchain technology provides efficient and secure solutions to various online activities by utilizing a wide range of cryptographic tools. In this paper, we survey the existing literature on post-quantum secure digital signatures that possess *exotic* advanced features and which are crucial cryptographic tools used in the blockchain ecosystem for (i) account management, (ii) consensus efficiency, (iii) empowering scriptless blockchain, and (iv) privacy. The exotic signatures that we particularly focus on in this work are the following: multi-/aggregate, threshold, adaptor, blind and ring signatures. Herein the term exotic refers to signatures with properties which are not just beyond the norm for signatures e.g. unforgeability, but also imbue new forms of functionalities. Our treatment of such exotic signatures includes discussions on existing challenges and future research directions in the post-quantum space. We hope that this article will help to foster further research to make post-quantum cryptography more accessible so that blockchain systems can be made ready in advance of the approaching quantum threats.

CCS Concepts: • **Security and privacy** → **Digital signatures**;

Additional Key Words and Phrases: Post-quantum cryptography, Digital signatures, Blockchain applications

1 INTRODUCTION

Cryptographic algorithms play a key role in blockchain systems to guarantee security, preserve privacy, and improve system performance. Digital signatures, in particular, are one of the key cryptographic primitives for blockchains. For example, Bitcoin [120] deploys the Elliptic Curve Digital Signature Algorithm (ECDSA) to manage coin ownership, so that funds can only be spent by their rightful owners. In particular, a classic signature scheme consists of a public verification key and a private signing key. A Bitcoin address is a 160-bit hash derived deterministically from the ECDSA verification key. Anyone who possesses the corresponding ECDSA signing key has the right to spend the fund represented by the Bitcoin address. A transaction to transfer funds from one (or more) Bitcoin address to other Bitcoin addresses is authorised if all inputs (i.e., Bitcoin addresses of the to-be-spent funds) are signed by using the corresponding signing keys.

2022. XXXX-XXXX/2022/9-ART1
https://doi.org/

With the advancement of blockchains, signatures with special features and functionalities beyond the conventional unforgeability (i.e., *exotic* signatures) have also been leveraged to tackle various issues therein. In fact, there exists a rich literature in using different signature schemes in digital cash before the birth of the blockchain, such as using blind signatures to prevent the signer (i.e., the payee) from being linked to its transactions [42]. Other signature schemes, such as adaptor, multi-, aggregate, threshold, and ring signatures, also play important roles in the blockchain. They empower blockchains with additional features in four main aspects, namely account management, consensus efficiency, empowering scriptless blockchains, and user privacy.

For account management, Bitcoin natively supports multi-signature addresses (with $\mathrm{OP}_{\mathrm{CHECKMULTISIG}}$) via its Non-Turing complete script language [23], to enable jointly owned asset management. A multi-signature address specifies a list of n ECDSA public keys and a threshold $t \leq n$, where the holders of at least t corresponding secret keys are each required to provide a signature to validate the transaction spending the jointly owned coin. While using multi-signature to manage jointly owned assets provides accountability, i.e., the set of signers is made transparent on blockchain, it has its own limit. First, with Bitcoin, the number n of keys has a hardcoded limit, making it non-scalable. In addition, it also incurs more transactions fees due to the larger size of a transaction (containing t signatures). Last, this is not privacy-friendly and may not be suitable for privacy-aware applications. Threshold signature schemes have been proposed to improve jointly owned asset management, where the ability to construct a single signature is distributed to n participants, such that producing a signature requires the involvement of t participants. This addresses the weaknesses of multi-signature transactions and has been implemented in several services, such as Binance, Wanchain, and Fusion.

For consensus efficiency, traditional Byzantine Fault Tolerant (BFT) protocols, such as PBFT [38], use an all-to-all message pattern to commit a decision block. To reduce the communication complexity from $O(n^2)$ to $O(n)$, aggregated or threshold signatures have been leveraged in several blockchain consensus protocols, such as SBFT [77], HotStuff [154], and Damysus [55].

Layer 2 protocols are one of the promising techniques to scale blockchains. In particular, layer 2 protocols, such as payment channels, aim to improve the throughput of blockchains by only recording a summary of a potentially large number of transactions into the blockchain. Taking payment channel as an example, two users establish a payment channel on a blockchain by committing pre-defined collaterals (i.e., coins) on the blockchain, and start to update the balance of the channel between the two users according to the agreed payments. Upon the channel closure, they only need to record the final state of the balance to represent all intermediate payments on the blockchain. Layer 2 protocols normally require the support of script language, making it challenging for scriptless blockchains (such as Monero or ZCash) to adopt the technique. Adaptor signatures have been considered to enable layer 2 protocols on scriptless blockchains [7, 117].

Exotic signatures have also been leveraged to protect blockchain privacy. The two main types of signatures for blockchain privacy are blind signature and ring signature. The use of blind signature has been proposed to improve Bitcoin privacy by constructing a coin mixing service, such as BlindCoin [147], to hide the payment links. CryptoNote [49] was proposed to provide transaction untraceability in blockchain-based cryptocurrencies. Unlike in Bitcoin where an observer of the blockchain can learn the trace of all coins, CryptoNote hides the trace of coins by using linkable ring signature [122]. In particular, linkable ring signature helps to hide the real coin to spend into a number of other coins, called mix-ins, leading to a better privacy guarantee. To date, Monero is the most famous privacy-preserving cryptocurrency with a market cap of 2.6 Billion USD[1].

[1] https://coinmarketcap.com/currencies/monero/, accessed 31-January-2022

While the vital role of cryptographic primitives is well recognised, the advancement of quantum computing raises a growing concern on the resilience of deployed cryptographic algorithms against quantum adversaries, as existing computational hardness assumptions may not hold anymore [11]. For example, Shor's algorithm makes it possible to solve the problems of large integer factorisation and discrete logarithm [142]. The recent announcements of achieving "quantum supremacy" by Google [6] and IBM [127] further strengthens the urge to have post-quantum secure blockchains.

Contribution. A systematic analysis on the landscape of post-quantum secure cryptographic constructions for exotic signatures is desired but missing from the literature. This paper fills the gap by providing a survey on post-quantum (PQ) exotic signatures (as of Aug, 2021) needed by blockchain systems. Considering all results related to exotic signatures is too much to cover in a single paper. Therefore, we limit the scope of the paper based on the following. First, to restrict the number of different signature types we discuss, we focus on the exotic signatures that have an existing major blockchain application, and not those that may *potentially* be useful in the blockchain setting. Since the blockchain application space spans a wide range of real-life settings, it is likely that any signature-like scheme may potentially find a blockchain application, but it is not possible to cover all such schemes in a single paper. Second, since we are motivated by a real-life application (i.e., blockchain), we focus on the most practically efficient results and do not discuss the more theoretical or practically less efficient results. Moreover, post-quantum ordinary signatures have already reached a certain maturity and there has already been works such as [44] that survey them. Therefore, we also do not discuss particular post-quantum ordinary signature proposals in this work.

When considering post-quantum cryptographic protocols it is natural to ask what quantum capabilities to consider for the adversary. Naturally we must allow the adversary the ability to run quantum algorithms, and beyond this, some works allow quantum *interactive* capabilities—in particular, we may consider quantum access to random oracles (the "quantum random oracle model" [26]) or to oracles representing honest parties (*e.g.*, the EUF-qCMA model [29] allows the adversary quantum access to a signing oracle). In this paper, we will not consider the quantum random oracle model or quantum interactions with signing oracles. Since we are considering only classical protocols, there is no real-world scenario in which an adversary would have quantum access to signature generation, so this restriction is quite reasonable. The quantum random oracle model, on the other hand, would be reasonable to consider—however, the field of post-quantum exotic signatures is rather new, and has simply not matured to the point that the quantum random oracle model has been sufficiently considered in the literature. Thus we leave this consideration for future work.

There are some (planned) efforts by major blockchain applications to support post-quantum cryptographic tools. For example, Ethereum 2.0 upgrade[2] is expected to support some quantum-safe cryptographic tools. Moreover, Algorand has recently introduced *state proofs*[3], where a post-quantum signature scheme (based on lattice problems) is used. Beyond these, we are not aware of a large-scale adoption of PQ tools in the blockchain setting and hope our work will pave the way towards a wider adoption of PQ cryptography for blockchain applications.

The rest of the paper is structured as follows. In Section 2, we discuss the main security assumptions that are believed to be quantum-safe. Particularly, we discuss assumptions based on hash functions, lattices, isogenies, codes, and multivariate polynomials. Then, we provide an overview on the role of different types of commonly deployed exotic signatures in blockchain in Section 3.

[2] See https://blog.ethereum.org/2015/12/24/understanding-serenity-part-i-abstraction/ (accessed on Aug 9, 2022).

[3] See https://developer.algorand.org/docs/get-details/algorand_consensus/#state-proof-keys (accessed on Aug 9, 2022).

In Section 4, we first overview the general zero-knowledge proof paradigms used to construct a large subset of the post-quantum exotic signatures we discuss in this work. Our goal here is not to discuss particular proof systems, but rather to overview the common building stones in order not to repeat the same discussions for different signature types. For example, "Fiat-Shamir with Aborts" paradigm (discussed in Section 4) in the context of lattice-based zero-knowledge proofs is used to construct threshold, adaptor and ring signatures. Then, Section 4 continues to our main discussion on different types of PQ exotic signatures, including multisignature and aggregate signature (Section 4.1), threshold signature (Section 4.2), adaptor signature (Section 4.3), and blind signature and ring signature (Section 4.4).

2 POST-QUANTUM SECURITY ASSUMPTIONS

While most of the currently deployed cryptographic schemes rely on the two main classical security assumptions, namely integer factorisation problem or discrete logarithm problem, quantum computers will make such schemes obsolete. The well-known Shor's and Grover's algorithm run on a quantum computer will be able to solve the two above-mentioned security assumptions in polynomial time and therefore break public-key cryptography relying on these assumptions. In contrast to the pre-quantum cryptographic schemes, their post-quantum counterparts rely on mathematical hardness problems which are believed to remain hard even with presence of a quantum computer. The main such post-quantum hardness assumptions will be presented in the subsequent sections. A set of very recent works (after our literature review) have shown the insecurity of some assumptions discussed in this section. For historical reasons, we still describe these assumptions and mark them by $^{\oslash}$ in Table 1 to indicate that they are (asymptotically or practically) broken.

2.1 Hash-based assumptions

Hash-based or symmetric key-based cryptography is one of the candidates to design quantum-safe signature schemes. One of the main features of hash-based cryptography is that the security of the schemes relies solely on the collision resistance of a hash function. Even if a used hash-function becomes insecure, it can be replaced by another secure hash-function without the need to use any other mathematical hardness assumption. One of the first hash-based digital signature was introduced by Merkle in 1989 [114]. An earlier work by Lamport [94] in 1979 presented a one-time signature which can be constructed from any secure hash-function. This work represents an important component in many follow up constructions of hash-based signature schemes.
A hash function $\mathcal{H}$ is a function:

$$\mathcal{H} : \{0,1\}^* \to \{0,1\}^n, D \leftarrow \mathcal{H}(m), \tag{1}$$

that maps an arbitrary-length message m to an n-bit hash value denoted as the digest D. A hash function is expected to satisfy the three properties:

- Preimage Resistance: knowing the digest D, it is computationally infeasible to find an input m s.t. $\mathcal{H}(m) = D$.
- Collision Resistance: Given two inputs $m_1 \neq m_2$, then $\mathcal{H}(m_1) = \mathcal{H}(m_2)$ happens with a negligible probability.
- Second Preimage Resistance: Knowing an input m, it is computationally infeasible to find $m' \neq m$ s.t. $\mathcal{H}(m') = \mathcal{H}(m)$.

A symmetric encryption scheme is defined by a tuple of three algorithm $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$

- KeyGen: This generates a secret key $\mathsf{sk} \in \{0,1\}^n$
- Enc: This takes as inputs a message m and the secret key sk and outputs a ciphertext ct.

- Dec: This takes as inputs a ciphertext and the secret key sk and outputs the corresponding plaintext.

Symmetric encryption schemes are able to satisfy the property of existential unforgeability under chosen message. The first important element to know is that its security is only affected by the Grover's algorithm and not by the Shor's algorithm. Grover's algorithm can recover a secret key or the input of a hash function in $\sqrt{n}$ quantum queries, where n is the size of the secret key or size of the hash outputs. This means that to counter this quantum Grover algorithm, hash-based primitives simply double the size of the secret keys or the size of the digests.

2.2 Lattice-based assumptions

Lattice-based cryptography is a promising candidate for quantum-safe cryptography as their security proofs are based on worst-case hardness and the corresponding constructions enjoy efficient implementations. In his seminal work, Ajtai [1] showed a connection between worst-case and average-case hardness and the suitability of lattices in cryptography. In this section we provide some of the main notions and definitions of lattice-based cryptography. A n dimensional lattice is a set of integer linear combinations of basis vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \in \mathbb{R}^n$:

$$\mathcal{L}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n) = \left\{ \sum_{i=1}^{n} x_i \boldsymbol{b}_i | x_i \in \mathbb{Z} \right\}.$$

The set of basis vectors in denoted by $\boldsymbol{B}$, i.e. $\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$. The most basic geometric quantity about a lattice is its minimum aka. Minkovski's first minimum. For an n-dimensional lattice $\boldsymbol{L}$ it's minimum $\lambda(\mathcal{L})$ is the length of the shortest non-zero vector of $\mathcal{L}$, i.e. $\lambda(\mathcal{L}) = \min \left(\|\boldsymbol{b}\| : \boldsymbol{b} \in \mathcal{L} \setminus 0 \right)$. The most well-known lattice-based hardness problems introduced by Ajtai [1] are the following:

Shortest Vector Problem (SVP): Given a basis $\boldsymbol{B}$, find the shortest $\boldsymbol{v} \in \mathcal{L}(\boldsymbol{B})$, where $\boldsymbol{v} \neq 0$.

γ-Shortest Vector Problem (γ-SVP): Given a basis $\boldsymbol{B}$ for an n-dimensional lattice $\mathcal{L}$, find a vector $\boldsymbol{v} \in \mathcal{L}$ with $0 < \|\boldsymbol{v}\| \leq \gamma\lambda(\mathcal{L})$.

Note: For $\gamma > 2^{O(n)}$ the γ-SVP problem is easy to solve by using the LLL algorithm [97] in polynomial time. However, for $\gamma < O(1)$ the problem is NP hard and thus very unlikely to be solved in polynomial time.

Closest Vector Problem (CVP): Given a basis $\boldsymbol{B}$, and a target vector $\boldsymbol{t}$, find the lattice point $\boldsymbol{v} \in \mathcal{L}(\boldsymbol{B})$ that is closest to $\boldsymbol{t}$.

Shortest Independent Vectors Problem (SIVP): Given a basis $\boldsymbol{B}$, find n linearly independent lattice vectors $S = \{s_1, \ldots, s_n\}$ which minimise the norm $\|S\| = \max_i \|s_i\| \leq \beta$, where $i \in [1, n]$ and β is an upper bound of the Euclidean norm.

In 1997, Ajtai [1] introduced the Short Integer Solution problem which served as the base for one-way and collision-resistant hash functions.

Short Integer Solution (SIS) Problem [1]: Given m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$ which form the columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ the problem is to find a non-zero integer vector $\mathbf{v} \in \mathbb{Z}^m$ of Euclidean norm $\|\mathbf{v}\| \leq \beta$ for a positive real β, such that $\mathbf{A}\mathbf{v} = \mathbf{0} \mod q$.

Many of the lattice-based constructions we address in this paper are based on the conjectured hardness of the Learning With Errors (LWE) problem, which was introduced by Regev [134] in 2005. It is defined given a probability distribution χ on $\mathbb{Z}_q$, normally taken to be a normal distribution with standard deviation σ:

Learning With Errors (LWE) Problem [134]: Given parameters q, n, m, α, a matrix $\boldsymbol{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ and $\boldsymbol{y} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e} \mod q$, where $\boldsymbol{e} \hookleftarrow \chi_{\alpha q}^m$ with standard deviation αq and $\boldsymbol{s} \hookleftarrow U(\mathbb{Z}_q^n)$, find $\mathbf{s}$.

Corresponding to the above stated Search LWE problem there exists also a Decision LWE problem where the goal is to distinguish $\boldsymbol{y}$ as computed above from a random $\boldsymbol{y} \hookleftarrow U(\mathbb{Z}_q^n)$.

The LWE problem is believed to be very hard with the best known algorithms solving the problem in time that is exponential in the lattice dimension n. We remark that SIS and LWE problems are average case approximation variants of SVP and CVP for the class of q-ary lattices defined over $\mathbb{Z}_q$. Practical lattice-based cryptographic algorithms often use algebraically structured variants of the SIS and LWE problems defined over polynomial rings such as $R_q = \mathbb{Z}_q[X]/(X^N + 1)$, with $N = 2^k$, which can be exploited to reduce communication/storage and computational costs. In particular, the R-SIS problem was introduced and its hardness studied in [104, 116, 129] and the R-LWE problem was introduced and its hardness studied in [106, 143]. Both ring problems are commonly used structured variants of SIS and LWE, where $\mathbb{Z}_q$ in the unstructured variants is replaced by R_q. More flexibility in lattice dimension is offered by the general *module* variants of those problems: M-LWE introduced in [32] and M-SIS introduced in [95]; the hardness of both problems was studied in [95]. The module problems in fact generalize their unstructured and ring variants, including the latter as special cases: the module problems are defined with respect to a matrix $\mathbf{A} \in R_q^{m\times n}$ and the cases $n = 1$ and $N = 1$ correspond to the ring and unstructured variants, respectively.

2.3 Isogeny-based assumptions

Isogeny-based protocols are built on the assumption that, given two elliptic curves, it is generally difficult to find an isogeny of a specific form (which depends on the protocol being considered) between them. Isogeny-based exotic signature protocols are built on essentially two kinds of problems: those which resemble the "computational supersingular isogeny problem with torsion point information," [88] and those which resemble "computational group action inversion" [40] for the action of the ideal class group. In this section we briefly introduce the fundamental algebraic-geometric definitions and these computational problems.

An elliptic curve E in Montgomery form defined over a field k is the set of $\overline{k}$-solutions to an equation

$$E/k\colon y^2 = x^3 + Ax^2 + x$$

for some $A \in k \setminus \{-2, 2\}$, along with a distinguished point ∞. The constant A is called the Montgomery coefficient, and we let E_A denote the curve with Montgomery coefficient A. An elliptic curve is a group under the chord-and-tangent law, with ∞ acting as the group identity. We define the set of k-rational points of E_A to be $E_A(k) = \{(x, y) \in E_A \ : \ x, y \in k\}$. In fact, $E_A(k)$ is a subgroup of E_A. For any integer N, we let $E_A[N] = \{P \in E_A \ : \ NP = \infty\}$ denote the set of N-torsion points of E_A. It is well-known that as long as N is coprime to $\operatorname{char} k$ we have $E_A[N] \cong \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$.

Every elliptic curve is either ordinary or supersingular. There are many equivalent characterizations of these notions; in isogeny-based cryptography we work over finite fields $k = GF(p)$ or $k = GF(p^2)$, and in this setting we have

$$E_A[p^n] \cong \begin{cases} \{0\} & \text{if } E_A \text{ is supersingular} \\ \mathbb{Z}/p^n\mathbb{Z} & \text{if } E_A \text{ is ordinary} \end{cases}$$

for all $n \in \mathbb{N}$. Isogeny-based cryptography almost exclusively uses supersingular curves, since for supersingular curves we have considerable control over the group structure of the subgroup of k-rational points, as discussed in [88, Section 4] and [40, Section 3].

An isogeny $\psi\colon E_A \to E_B$ between elliptic curves is a non-constant rational map which is also a group homomorphism. The degree of an isogeny is simply its degree as a rational map. We say that an isogeny is k-rational if the coefficients of the polynomials in its coordinate maps can be taken to be in k.

With these definitions, we can define the **Computational supersingular isogeny problem with torsion point information (SSI-T)** problem: Let N, N' be coprime integers, and let $\psi \colon E_A \longrightarrow E_B$ be an isogeny of degree N. Given N, N', E_A, E_B, and $\psi(P), \psi(Q)$, where $\{P, Q\}$ is a generating set for $E_A[N']$, find ψ.

A recent series of works due to Castryck and Decru [39], Maino and Martindale [109], and Robert [136] demonstrates that the SSI-T problem can, in fact, be solved in polynomial time; this renders all exotic signatures built on SSI-T and related problems insecure. In particular, the two blind signatures we discuss in Section 4.4 are not secure, though we briefly discuss them for historical reasons.

Isogeny-based protocols based on the **Group Action Inversion** problem are immune to the Castryck-Decru, Maino-Martindale, and Robert attacks; we discuss that problem here. Given an elliptic curve E_A, its endomorphism ring $\mathrm{End}(E_A)$ is the set of all isogenies $\psi \colon E_A \longrightarrow E_A$, along with the constant map ψ_0 which sends each point of E_A to ∞; the ring operations are pointwise addition and function composition. When E_A is defined over $GF(p)$, we define the subring $\mathrm{End}_p(E_A)$ to be the ring of all $GF(p)$-rational endomorphisms of E_A, again along with ψ_0. When E_A is supersingular and defined over $GF(p)$, it is known that $\mathrm{End}_p(E_A)$ is isomorphic to an order O in an imaginary quadratic field; moreover, the ideal class group $\mathrm{cl}(O)$ of this order acts freely and transitively by complex multiplication on the set $\mathcal{E}\ell\ell(O)$ of elliptic curves E' which have $\mathrm{End}_p(E') \cong O$—for details on the definition of this action, see [40, Section 3].

The other major problem in isogeny-based cryptography—often called **group action inversion (GAIP)**—is to invert complex multiplication: that is, given E_A, E_B which satisfy $\mathrm{End}_p(E_A) \cong O \cong \mathrm{End}_p(E_B)$, to find an ideal class $[\mathfrak{a}] \in \mathrm{cl}(O)$ such that $E_B = [\mathfrak{a}] * E_A$. Some protocols consider a **multi-target (MT)** variant of the problem: given $E_{A_1}, E_{A_2}, \ldots, E_{A_n}$ whose endomorphism rings are pairwise isomoprhic, find $[\mathfrak{a}], k_1, k_2$ such that $E_{A_{k_2}} = [\mathfrak{a}] * E_{A_{k_1}}$. At present, these problems underlie all secure isogeny-based exotic signature protocols.

2.4 Code-based assumptions

Code-based cryptographic schemes deploy an error-correction code (ECC) in their algorithm. The security analysis of code-based cryptosystems assumes that the attacker has no access to the algebraic structure of the underlying ECC. Therefore, correcting errors is only possible if one knows a parity check (generator) matrix. Let C denote a linear code of length n and dimension k. Let $r = n - k$ be the codimension of C and H a parity matrix of this code. A syndrome mapping relatively to the parity matrix H is defined as

$$S_H : \{0,1\}^n \longrightarrow \{0,1\}^r,\ \boldsymbol{y} \mapsto \boldsymbol{y}H^{tr}.$$

Next, let $\boldsymbol{s} \in \{0,1\}^r$ denote a syndrome which defines a set of words of $\{0,1\}^n$ as follows:

$$S_H^{-1}(\boldsymbol{s}) = \{\boldsymbol{y} \in \{0,1\}^n | \boldsymbol{y}H^{tr} = \boldsymbol{s}\}.$$

Security of code-based cryptosystems relies on decoding problems which either address the Hamming distance of a codeword $\boldsymbol{x} \in C$ to a word $\boldsymbol{y}$, or look for the minimal Hamming weight of an error $\boldsymbol{e}$ lying either in the coset $\boldsymbol{y} + C$ or in $S_H^{-1}(\boldsymbol{s})$. These problems are not in NP, because it is difficult to check whether $\boldsymbol{e}$ is really of minimal weight in the coset. Therefore, we focus on slightly different decoding problems which were defined in [17]:

Computational Syndrome Decoding. Given a $r \times n$ matrix H, a word $\boldsymbol{s} \in \{0,1\}^r$ and a positive integer $w > 0$, find a word $\boldsymbol{e} \in S_H^{-1}(\boldsymbol{s})$ of Hamming weight at most w.

It is worth to mention that the corresponding decision problem is NP-complete.

Codeword Finding. Given a binary $r \times n$ matrix H and a positive integer $w > 0$, find a non-zero word of Hamming weight at most w in $S_H^{-1}(\mathbf{0})$.

Complete Decoding. Given a binary $r \times n$ matrix H and a word $\boldsymbol{s} \in \{0,1\}^r$, find a word of Hamming weight at most $d_0(n,r)$ in $S_H^{-1}(\boldsymbol{s})$.

2.5 MQ-assumptions

The first Multivariate Public-Key Cryptography (MPKC) as we know it today was introduced in 1988 by Matsumoto and Tsutomu [112]. MPKC is based on the existence of trapdoor one-way functions which is defined in the form of a multivariate quadratic polynomial map over a finite field. The public key of such a cryptosystem is given as a set of quadratic polynomials $\mathcal{P} = \big(p_1(w_1,\ldots,w_n),\ldots,p_m(w_1,\ldots,w_n)\big)$. Each of the p_i's is defined as the following quadratic polynomial:

$$p_i(w_1,\ldots,w_n) := \sum_k P_{ki}w_k + \sum_k Q_{ki}w_k^2 + \sum_{k>\ell} R_{k\ell i}w_k w_\ell$$

where all coefficients and variables are in $\mathbb{F}_q$.
The hardness problem introduced in [112] that all multivariate public-key cryptographic schemes rely on is called the MQ (multivariate quadratic) problem which is defined as follows:

MQ Problem: Given multivariate quadratic polynomials $p_i(\boldsymbol{x}), \boldsymbol{x} = (x_1,\ldots,x_n)$, where all coefficients and variables are in the finite field $\mathbb{F}_q$, the MQ problem is to solve the system $p_1(\boldsymbol{x}) = \cdots = p_m(\boldsymbol{x}) = 0$.

Rainbow signature scheme [58] is one of the oldest and well-studied multivariate signature schemes that made it to the third round of NIST Post-Quantum Cryptography standardization process. A recent work by Beullens [18] showed how to practically break Rainbow. As a result, the multivariate blind signatures and ring signatures we discuss in Sections 4.2 and 4.4 are not secure anymore, because they fall short to guarantee the required post-quantum security due to the underlying insecure Rainbow signature scheme. However, we give a brief description of these scheme for historical reasons.

3 OVERVIEW: EXOTIC SIGNATURES FOR BLOCKCHAIN

This section presents a brief overview on the need of signature schemes with special features in blockchain, which establishes the necessary background to understand the roles of advanced cryptographic signatures in blockchain and introduces also the roadmap (see Figure 1).

3.1 Account Management: Multi- & Aggregate Signature

A multisignature is a digital signature scheme which allows a group of users to jointly sign a message. The identities of all signers of a multisignature are transparent and verifiable. It is usually desired to have a single signature representing the collection of distinct signatures on the same message, as this reduces both the size of the jointly signed message and the time to verify its validity. Such multisignature schemes, where distinct signatures on the same message can be aggregated, are called aggregate signature. Given a multisignature, the identities of group members who produced it are known to the verifier.

This concept is particularly useful for ownership management in the blockchain, such as maintaining a joint account where the authorisation from multiple users is required to validate a transaction, increasing wallet security where compromising a single signing key does not lead to the compromise of the wallet [5].

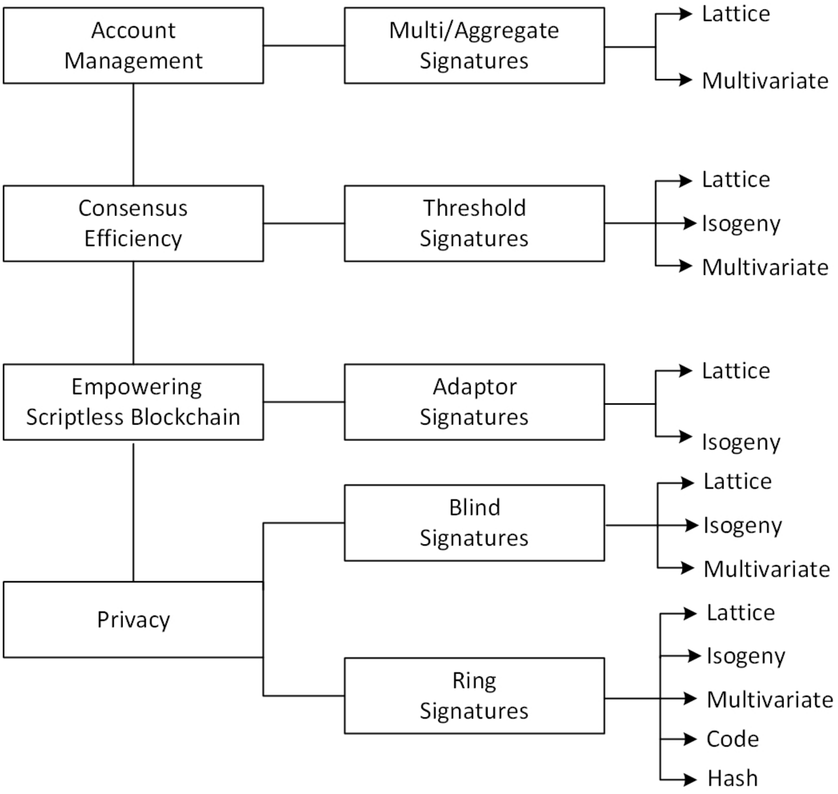

Fig. 1. Roadmap of studied exotic signature schemes.

3.2 Consensus Efficiency: Threshold Signature

(t, n)-Threshold signatures enable a pre-defined minimum number t of signers to generate a valid signature on behalf of a group of size n. The identity of all involved signers is hidden. This primitive enables better efficiency for the Byzantine Fault-Tolerant (BFT)-style consensus.

In particular, miners in blockchain systems reach an agreement on the validity and ordering of transactions through a consensus mechanism [121]. In addition to the permissionless blockchain consensus algorithms (such as proof-of-work and proof-of-stake), BFT-style consensus algorithms are also a popular choice [36, 48, 157] as they provide instant finality and better throughput [150]. However, BFT protocols require participants (aka. replicas) to collect and verify a pre-defined minimum number of signed votes from distinct replicas [111]. In most of the BFT protocols, at least one replica needs to forward the collected distinct signatures to others, where this can be made more efficient by leveraging a threshold signature.

3.3 Empowering Scriptless Blockchain: Adaptor Signature

Adaptor signature schemes allow a party to pre-sign a message, in a way that anyone can turn it into a valid signature if a secret witness of the pre-signed message is known. This has been used to empower scriptless blockchains with offchain payments and atomic swaps.

Layer 2 solutions support offchain payments, where a payer and a payee can process payment without the need to record their transactions online [79]. With offchain payment solutions, such as payment channel or state channel, the channel state is updated through new offchain transactions and a mechanism for state revocation is required to avoid state duplication. While state revocation can be achieved through blockchain scripts, it is challenging for scriptless blockchains. The use of adaptor signatures [63] has been explored to enable state revocation with scriptless blockchains [7, 117].

Atomic swap protocols [81] enable parties to exchange assets across different blockchains. Atomic swap protocols require assets to be locked before the exchange is successful. However, similar to the payment channel network, such locking normally requires the support of a script language. The use of an adaptor signature enables atomic swap protocols to be executed over scriptless blockchains [132].

3.4 Privacy: Blind Signature and Ring Signature

As blockchains provide a transparent archive of all transactions, privacy is also a main concern. Blind signatures [42] are proposed for protecting the transaction privacy in the digital cash application before the birth of the blockchain, and also in the blockchain-based cryptocurrencies [153]. With a blind signature scheme, the message is blinded before it is signed. The resulting blind signature can be verified by anyone who has the knowledge of the original unblinded message.

A Linkable Ring Signature (LRS) [100] is a more popular primitive for protecting user privacy in cryptocurrencies [122, 149]. An LRS enables a signer to hide herself among a group of entities, with an additional constraint that if the signer creates two distinct signatures by using the same key, then the identity of the signer will be revealed. This primitive is leveraged in cryptocurrencies to protect transaction untraceability, which guarantees that it is impossible to trace any coin back to another transaction. Monero, which improves upon the CryptoNote-style blockchains [149], is a notable example built upon the LRS primitive. It deploys the Ring Confidential Transactions (RingCT) protocol, where the LRS is used for protecting untraceability and an additional commitment scheme with range proof is used for hiding the transaction amount [122]. However, prior research shows that even when assuming a secure RingCT protocol, the transaction untraceability still cannot be achieved when considering side channel information and user behaviours [37, 43, 93, 119, 156, 158].

4 POST-QUANTUM SCHEMES FOR BLOCKCHAIN

This section provides an analysis of the recent and advanced post-quantum cryptographic primitives, with a focus on zero-knowledge proofs and special flavours of digital signatures, we call *exotic signatures*. Figure 1 provides a roadmap of the primitives we present in this paper and their connection. Our main focus is on the exotic signature schemes such as adaptor, blind, multi-/aggregate, threshold and ring signatures. We analyse the post-quantum constructions of the above mentioned signatures and emphasize the challenges and drawbacks in the existing lattice-, isogeny-, hash-, code-based and multivariate schemes. It is worth mentioning that several signature schemes can be constructed from zero-knowledge protocols. Therefore, there is a direct connection between the zero-knowledge proofs and exotic signatures as we can see in Figure 1. Lastly, we present the post-quantum constructions of ring confidential transactions (RingCT) which can be constructed from ring signatures. This fact establishes a connection between the exotic signatures and RingCT showed in Figure 1. The analysis of these exotic primitives makes our work distinct from the previous results [68] as their focus is mainly placed on encryption schemes and conventional signature schemes.

Important Zero-Knowledge Paradigms Underlying Efficient Exotic Signatures

Zero-Knowledge Proofs (ZKPs), initially introduced by Goldwasser *et al.* [78], describe a paradoxical nature of NP proof systems where a prover convinces a verifier about some statement without revealing anything else apart from the claim that the statement is correct. Being such a powerful tool, it is no surprise that ZKPs can be used to construct various signature schemes. Therefore, we next discuss the general ZKP paradigms used as a building block for post-quantum signature-like schemes we discuss in this work.

Lattice-based approach. There is a very rich literature in designing lattice-based ZKPs. Those relevant for *practical* applications (such as blockchain protocols) mainly follow the "Fiat-Shamir with Aborts" (FSwA) paradigm [102, 103]. This approach is an adaptation of the Schnorr proof system [140] to the lattice setting with an additional rejection sampling technique. In particular, the overall proof often follows (or at least includes) the 3-move commit-challenge-response structure, where (i) in the *commit* phase, the prover commits to some masking value(s) and transfers the commitment(s) to the verifier, (ii) in the *challenge* phase, the verifier sends a random challenge (sampled from a certain distribution) to the prover, and (iii) in the *response* phase, the prover reveals the masked openings that are used to validate the proof. Many signature-like lattice-based schemes follow (in part) the above paradigm, but adjust it to the specific requirements of the concrete construction.

Hash-based approach. Symmetric-based ZKPs use a one-way function $F : \{0,1\}^n \longrightarrow \{0,1\}^n$ like block ciphers or hash functions, which can be represented as a binary or arythemtic circuit. They prove the knowledge of a secret input x with the help of the public output y ($F(x) = y$). There exist different approach to prove the knowledge of the input x. One approach introduced by Ishai *et al.* [85] is called MPC-in-the-head which consists of simulating a multi-party computation of the function F between a number of parties to prove the knowledge of x. The work of ZKBoo [76] and ZKB++ [41]. Both schemes compute F with an MPC protocol between three parties and then reveal the views of only two of them in the proof. Katz *et al.* introduced the ZKP system KKW [92], which improves ZKB++ when it comes to proof size. KWW increases the number of parties for the MPC-in-the-head parts, which results in a decrease of the proof size. The proof contains the view of all parties except one. ZBK++ and KKW are at the heart of the security of the digital signature Picnic [41] submitted to the NIST standardisation process. An optimised version of KKW is presented in [91]. The proof size depends directly on the number of multiplications ("AND" gates) in the circuit F, therefore, ZKB++ and KKW use the non-standard block cipher LowMC [2], which has a low multiplicative complexity. The works [54],[12] use (MPC-in-the-head), but employ the standard AES as a one-way function F. Low-degree testing [14] is an alternative to MPC-in-the-head to construct symmetric-based ZKPs and is implement in ZKPs such as Ligero++ [22], ZK-STARK [13] and Aurora [14]. The results presented in [22] and [14] show that this later technique could be more promising than MPC-in-the-head.

Isogeny-based approach. Isogeny-based ZKPs can be broadly divided into two classes: those which prove knowledge of a solution to an SSI-T instance, and those which prove knowledge of a solution to a GAIP or MT-GAIP instance. These protocols are described in detail in [88] (in the SIDH-like setting) and [20] (in the CSIDH-like setting). The underlying hard problem of finding such an isogeny is called the *supersingular isogeny problem* (SSI).

The primary application of these isogeny-based ZKPs—especially in the blockchain-relevant context—is to construct isogeny-based digital signatures by applying the Fiat-Shamir transform [69] or the Unruh transform [146], such as Yoo *et al.*'s scheme [155], SeaSign [52] and CSI-FiSh [20]. Extensions of these simple ZKP protocols are used to develop the special flavors presented in Sec. 4.

Code-based approach. The first code-based ZKP construction was proposed by Stern [144], which was based on the syndrome decoding (SD) problem. It was showed how to use this ZKP as a basis for the zero-knowledge identification scheme. In a subsequent work [87], the authors proposed a ZKP based on the Exact Learning Parity with Noise (xLPN) problem, which is a special case of the LPN problem. We note that their ZKP construction represents a special case of a Sigma protocol where the soundness error is larger than 1/2. The total complexity of the protocol in [87] is $\Theta(\sum C_i \ell \log \ell)$, where C_i are the layers of the used circuit C and ℓ is the length of the underlying LPN problem. A special case of code-based ZKPs was introduced in [35], which provides a zero-knowledge protocol for the correct evaluation of a code-based pseudorandom function (PRF). Such proof system allows the prover to convince the verifier that a given output y is correctly computed by a code-based PRF using a secret key k and an input x. The communication complexity of this ZKP depends on the input dimension t of code-based PRF. For $t = 128$ and $t = 256$ the communication complexity ranges between approximately 700 MB and 1500 MB, respectively, which justifies the use of this ZKP only in prove-on-demand application scenarios.

Multivariate approach. The first zero-knowledge protocol based on multivariate quadratic polynomials was proposed in [139]. The construction follows the cut-and-choose approach, where the secret the prover wants to prove is split into shares and after verifier's choice the prover proves the correctness of some of the shares. Mathematical properties such as modular exponentiation $g \mapsto g^x \bmod p$ and a linear function $x \mapsto Mx$ are used in this approach. For instance, when sharing a secret $s = s_1 + s_2$ the map of this secret can be written as $g^s = g^{s_1}g^{s_2}$ and $Ms = Ms_1 + Ms_2$. However these properties are not given in the multivariate quadratic (MQ) function $(x_1, \ldots, x_n) \mapsto (y_1, \ldots, y_n)$ where $y_k = \sum_{i,j} a_{k,i,j}x_i x_j + \sum_i b_{k,i}x_i$. This can be fixed by using the bilinearity property of the polar form of the MQ function. The security of the construction relies on the conjectured intractability of the MQ problem assuming the existence of a non-interactive commitment scheme which is statistically-hiding and computationally-binding.

4.1 Account Management: Multi- & Aggregate Signature

The construct of multi-signature was first articulated by Itakura and Nakamura [86] where a coalition of signers generate a signature σ together over a message m. Given the set of public keys of all signers and the message m, σ can be verified publicly. A straightforward approach is to generate a signature over m per each individual signer and then concatenate all of them. This trivial approach is not practical as the size of the multi-signature grows linearly with the number of signers. Thus, ideally the size of the signature in a multi-signature protocol should be similar to a single-signer scheme. In Bitcoin, some transactions' outputs require multiple signatures to be spent. This transactions are often called as m-of-n multisignature transactions where the trivial approach of building a multi-signature scheme as mentioned above is used. Currently Bitcoin implementation uses ECDSA signatures [152] to authenticate transactions. However, ECDSA is complex to be used in multiparty fashion [74, 99], hence multisignature schemes supporting key aggregation [113] as well as efficient threshold signature protocols for ECDSA [74, 99] have been proposed to address this issue. In general, a multisignature scheme with key aggregation differs from the original digital signature scheme by an interactive signing protocol and an additional algorithm KAgg which aggregates the public key of the signers into a single public key. At the end of the Sign protocol the output is a single signature σ on a message m. Similar functionality as in multisignatures can be achieved by an aggregate signature scheme which was introduced in [28]. However, the main difference to the multisignature is given by a non-interactive signing algorithm which is run by each of the n signers S_i individually on a different message m_i and all individual signatures σ_i are *publicly aggregated* into σ.

Lattice-based approach. El Bansarkhani and Sturm [62] construct a lattice-based multisignature derived from the GLP signature [80], a variant of the Lyubashevsky-Schnorr Fiat-Shamir with rejection sampling signature [103] based on the P-LWE (aka. Ring-LWE) and Ring-SIS lattice problems (we note though, that recent work pointed out that this protocol's security proof has a gap, which implies its provable security relies on a non-standard variant of the Ring-LWE problem). The scheme has a 3-round multi-signing protocol, in which the commitments and responses of each signer in the protocol are compressed by summation, exploiting the homomorphic property of P-LWE and P-SIS problem for verification. Each of N cosigners may reject their responses in the rejection sampling step, which leads to re-starting the full protocol for all signers - this requires the rejection probability of each signer to be N times smaller than in the one-signer GLP signature, for the same overall signing acceptance probability. The signature length is $O(\log N)$ asymptotically for large N, while for smaller N there is a linear component in N that grows by 2λ bits per signer for security parameter λ-bit. Concrete signature lengths in [62] are 4.7 KB for $N = 5$ and 4.9 KB for $N = 10$ at 120-bit security level (compared to 1.1 KB for the $N = 1$ GLP signature at 100-bit security level [80]). However, there is no compression mechanism for the co-signer public keys. Recent work [51] pointed out a gap in the security proof of the multisignature in [62], which implies its provable security relies on a non-standard variant of the Ring-LWE problem. The paper [51] also gives two modified multisignature schemes that fix this problem and have a security proof from standard MLWE/MSIS assumptions at the cost of lower efficiency and longer signature length: a three-round signing protocol that adds an additional randomised homomorphic commitment computation in signing and verification, and a two-round signing protocol which also embeds a trapdoor in the homomorphic commitment scheme. The paper [71] gives a variant of the scheme [62] with a security proof in the quantum random oracle model and additional parameter constraints, but similarly to [62], its security proof also relies on an (explicitly stated) non-standard 'rejected MLWE' assumption. Finally, paper [108] gives a variant of [62] with a lower signing rejection probability and shorter signatures but, as pointed out in [51] its security proof also appears to require (an even stronger) non-standard 'rejected MLWE' assumption.

Doroz *et al.* [59] construct aggregate signature schemes MMSAT and MMSATK derived from the one-signer PASS signature [84]. Security is based on a more structured variant of the PLWE/RingLWE and Ring-SIS problems introduced in [84] called Partial Fourier Recovery Problem (aka. Vandermonde-LWE and Vandermonde-SIS). In this problem the random matrix underlying the LWE/SIS problems is replaced by a partial Vandermonde (aka. partial NTT) transform matrix over the underlying polynomial ring. The schemes assume a non-interactive signing protocol where each of N cosigners signs independently using the PASS scheme. In MMSAT, N signatures are aggregated using a short linear combination of responses from the original PASS Fiat-Shamir signatures, with short linear combination coefficients determined by a hashing process. The aggregate signature length is further reduced using a linear map T to compress the commitments, resulting in an overall $O(\log N) + 2\lambda N$. The MMSATK scheme additionally allows aggregation of the N signer public keys by compressing each key using a linear map; the resulting aggregated key length is still linear in N but with a much smaller proportionality constant, reported as ≈ 157 bytes per signer at a 128-bit security level (compared to 4.3 KB per signer for PASS). Concrete aggregated signature size of 36 bytes at 128-bit security level is reported in [59]. However, it was recently pointed out [31] that the compressing linear map T used in MMSAT and MMSATK implies that the security of these aggregate signatures relies on the hardness of a problem we call *T-Vandermonde-SIS*, a variant of Vandermonde-SIS but with significantly reduced security against lattice attacks with the parameter choices in [59]. Consequently, only the 'response' part of the signature can be securely aggregated, not the 'commitment' part. Due to a similar issue, the aggregatable signature from M-LWE and M-SIS problems constructed in [31] also does not produce substantially shorter signatures than concatenated regular signatures.

Multivariate approach. The first sequential aggregate signature (SAS) scheme based on multivariate quadratic polynomials was proposed in [10]. The construction deploys multiple signers, where each of them signs a different message and all signatures are sequentially aggregated into a single signature which benefits from a shorter size than a simple concatenation of the individual signatures. The construction of an SAS scheme is instantiated from a HFEv- signature scheme introduced in [124], where the resulted SAS length only slightly extends the signature length of the standard HFEv- [125]. This construction enables high compression rates and therefore achieves very short sizes of the signature. For instance, in presence of 20 signer and a 80-bit security level, the signature size is about 254 bits. It is remarkable that the compression length for a 120-bits security level is even higher than in the 80-bit scenario. However, the main disadvantage in the case of 120-bits security level is the considerably larger size of the public keys. The security of SAS is based on the hardness of the MQ problem which for a given set of multivariate quadratic polynomials requires to find a vector $\vec{x}$ such that all polynomials evaluate to zero in this vector $\vec{x}$. In terms of the signature size, multivariate SAS construction in [10] proves to be more suitable than other SAS constructions from lattice-based cryptography.

Discussion. Currently there are no known hash-based, isogeny-based nor code-based construction of multisignatures or aggregate signatures.

Among the lattice-based multisignature constructions, the scheme of [62] gives short signatures but relies on non-standard variants of lattice problems. For more security confidence, we would recommend the scheme of [51] which relies on standard polynomial (ring) SIS and LWE lattice problems; the multisignature length scales logarithmically with the number of signers similar to [62], although its concrete signature lengths are not evaluated. Both those lattice multisignature schemes do not support key aggregation. It is an open problem to construct lattice-based aggregate signatures (i.e. supporting public aggregation) that are substantially shorter than concatenated regular signatures and support key aggregation. The multivariate construction of [10] is based on a known HFEv- variant of the MQ problem and gives the shortest aggregate signatures only slightly longer than standard HFEv- signatures, but requires sequential aggregation, does not support key aggregation, and has quite large public keys. See Table 1 for a summary.

The main application of multi- and aggregate signature in blockchains is user account management, where authorising payments requires multiple users to sign on the same message in their individual apps (such as mobile wallet). Given the use case, the current best length (in the order of bytes) and computation time (a few milliseconds or even less) are considered acceptable in the deployment.

4.2 Consensus Efficiency: Threshold Signature

A k-out-of-N threshold signature scheme—first introduced by Desmedt and Frankel [57]—is a variant of a digital signature scheme in which signing authority is split among N users in such a way that any k of them can construct signatures, while any group of $k - 1$ of fewer users cannot. The idea is built upon earlier works of Blakley [24] and Shamir [141], which introduced *(threshold) secret sharing schemes*: schemes in which a secret can be split among N users in such a way that any k of them can recover that secret while any $k - 1$ or fewer of them have no information whatsoever about the secret (in the sense that those shares could correspond to any possible value of the secret). The correctness and security definitions for threshold signatures are mostly the same as for ordinary digital signature schemes; the main difference is that in the definition of unforgeability, we require that no $k - 1$ or fewer colluding malicious users can produce a signature on a message they have not seen signed before—see [75] for the complete details.

Lattice-based approach. Cozzo and Smart [46] investigated threshold variants of the NIST PQC signature schemes, constructed using a combination of secure multiparty computation (MPC) techniques with linear secret sharing to allow the signers to jointly compute a sharing of the signature. However, for the Falcon, Dilithium and qTesla lattice-based signature schemes, this results in signing protocols involving multiple rounds of communication with relatively slow signing run-times. An earlier theoretical approach in [16] gives threshold signing protocols for GPV-type trapdoor lattice-based signatures, but relies on inefficient generic MPC techniques for offline and key generation Gaussian sampling. Another theoretical approach by Boneh *et al.* [27] introduced threshold signatures built from threshold Fully Homomorphic Encryption (FHE) techniques. In this approach, the public key contains an FHE encryption of the signing key, and the FHE decryption key shared among the signers; the signing protocol involves each signer performing a homomorphic evaluation of the signing circuit followed by a partial decryption with its share of the FHE decryption key. When instantiated with lattice-based signatures and FHE schemes, a major efficiency bottleneck in [27] arises from the need to 'smudge' the partial decryptions with noise magnitude exponentially large in the security parameter λ, which leads to long partial signatures of length $\widetilde{O}(\lambda^3)$.

Isogeny-based approach. De Feo and Meyer [53] constructed the first isogeny-based threshold signature in 2019. Like many other isogeny-based signature schemes, this scheme is based on CSI-FiSh [20]. The key ideas of the scheme are that the structure of a hard homogeneous space [45] with cyclic group action allows to: (a) Construct a straightforward distributed group action computation protocol; (b) Apply the ZKP construction as in [20, Section 5], and; (c) Use Harn's "secret sharing in the exponents" construction [82] to split the proof of knowledge authority in a k-out-of-N fashion.

Applying the Fiat-Shamir transform to the resulting k-out-of-N threshold proof of knowledge protocol yields the desired threshold signature. Despite being based on robust and versatile classical primitives, the lack of ring structure in the exponent stands in the way of realizing certain desirable properties, such as the ability to detect malicious participants (as in [75], for instance), the ability to do away with the trusted dealer, as in [126], or the ability to use a central "combiner" to construct a signature, rather than requiring parties to operate sequentially online. As well, the scheme is limited by the ability of parameter generation since at present, the best-known algorithm to generate parameter sets for CSI-FiSh-like protocols takes exponential classical time. However, parameter generation can be done efficiently on a quantum computer, making such schemes potentially useful in the "post-post-quantum" setting. Finally, to prove the security of their scheme, the authors use a theorem of Gennaro *et al.* [75], which requires that their underlying threshold secret sharing scheme based on the hardness of *power decisional Diffie-Hellman group action problem* (Power DDH) be simulatable.

In 2020 Cozzo and Smart proposed Sashimi [47], an isogeny-based threshold signature scheme which achieves security against active adversaries. Like the protocol of De Feo and Meyer this scheme also requires the structure of $\mathrm{cl}(\mathcal{O})$ to be known, and so can only presently be instantiated for the CSIDH-512 parameter set. The protocol essentially follows the first two steps of the protocol of De Feo and Meyer, with added ZKPs of the kind described in Section 4 to ensure that participants are constructing the intermediate curves honestly; it is these ZKPs that give the scheme active security. Both schemes require $O(k)$ rounds of communication for thresholds of size k.

Multivariate approach. The most practical among the interactive threshold protocols designed by Cozzo and Smart [46] using general secure multiparty computation (MPC) techniques is a threshold signing protocol for the LUOV multivariate-based signature scheme [21] from the NIST PQC process. The interactive LUOV signing protocol of [46] for 3 parties runs in 6 communication rounds and is estimated in [46] to take about 1.3 seconds to generate a signature, assuming typical LAN communication latency, for a 231 bits quantum security level parameter set.

Discussion. We note that there are no code-based constructions of standard threshold signatures. A lattice-based threshold signature by Boneh *et al.* [27] is less efficient due to large smudging errors.

Recently, two isogeny-based threshold signature schemes were proposed; De Feo-Meyer and Sashimi. They have similar design of making CSI-FiSh into a threshold scheme. In both, the signature is produced more towards a ring signature fashion, with each signer required to accept and receive a message. The main simplification in Sashimi is that a Replicated Secret Sharing Scheme is used. That is, the resulting sharing (for a given qualified set) is treated as a full threshold sharing. The MQ-based LUOV threshold signing protocol [46] has potential practicality issues due to the interactive 6-round signing process. For our recommendation, see Table 1.

Threshold signatures are widely considered as a good way to reduce the network overhead (w.r.t. the number of bits to transfer). For example, a leader in a consensus scheme (such as Hotstuff [154] and Damysus [55]) would need to collect and broadcast a quorum of votes/signatures, where the numbers of bits to transfer of $O(N)$ complexity. However, the deployment barrier for using threshold signatures is mainly the time it takes to generate a signature (which includes steps to generate and disseminate signature shares to reconstruct a full signature).

4.3 Empowering Scriptless Blockchain: Adaptor Signature

Adaptor signatures are a relatively new concept introduced initially as *scriptless scripts* by Poelstra [133]. They extend a digital signature such that first a “pre-signature” based on some condition is generated. Then, whoever is in possession of a witness for the condition can adapt the pre-signature to create a full signature. Upon completion of the full signature, a secret value (in particular, a witness to the condition) is revealed. The conditions are defined by a hard relation on a public *statement* and a secret *witness* such as the knowledge of a discrete log secret or a preimage of a hash function. The complete signature is simply an ordinary signature output that can be verified as the original signature scheme. As a result, an ordinary signature is created at the end of the two party interaction in the adaptor signature. In particular for the blockchain application, the miners simply verify the ordinary signature without realizing it may be an adaptor signature output. At the same time, the two parties involved in the adaptor signature generation can embed a condition that is not limited by the blockchain’s scripting language.

There are mainly three advantages of adaptor signatures: (i) on-chain cost reduction, (ii) improved fungibility of transactions, and (iii) provision of extra capabilities beyond the blockchain’s scripting language. More specifically, as adaptor signature interaction happens off-chain and thus the condition is not published on-chain separately, there is no additional on-chain storage and verification costs. This fungibility property is used, for example, to obscure payment channel network transactions among regular transactions [110]. Finally, adaptor signatures bring about enhanced functionalities to blockchains with a limited scripting language. These advantages have been utilised in various applications such as atomic swaps [132], payment channel networks [7, 110], and discrete log contracts [60].

Table 1. Summary of state-of-the-art post-quantum exotic signature schemes.

Type	Scheme	PQ Type	Security Assumption[4]	Quantum Security	Sign./Ver. (ms) Time at 3GHz	Signature Length (KB)	Asymptotic Complexity
Multi- and Aggregate Signatures[5]	[62]	Lattice	R-SIS & R-LWE [6]	120 bits	0.84/0.15	0.49 ($N = 10$)	$O(\log N)$
	[51]	Lattice	M-SIS & M-LWE	128 bits	N/E	N/E	$O(\log N)$
	~~MMSAT~~ [59]	Lattice	T-Vand.-SIS$^{\oslash}$ & -LWE	128 bits	N/E	0.036 ($N = 10^3$)	$O(N)$
	MQSAS [10]	MQ	HFEv- MQ	120 bits	4.18/N/E	0.004 ($N = 10$)	$O(N)$
Threshold Signatures[7]	Falcon MPC [46]	Lattice	NTRU & R-SIS	108 bits	>5700/0.03	0.67	$O(1)$
	De Feo-Meyer [53]	Isogeny	Power DDH	60 bits	722/722	0.560	$O(1)$
	Sashimi [47]	Isogeny	Power DDH	60 bits	5.66×10^5/280	1.77	$O(k)$
	LUOV MPC [46]	MQ	LUOV MQ	231 bits	1300 [8]/22	3.1	$O(1)$
Adaptor Signatures	LAS [63]	Lattice	M-SIS & M-LWE	128 bits	0.22/0.08 [9]	1.58 [10]	N/A[11]
	O-IAS [145]	Isogeny	GAIP	60 bits	86.7/93.3	19.0 (Pre-sig.) 0.956 (Sig.)	N/A
Blind Signatures	[83]	Lattice	R-SIS	128 bits	N/E[12]	7730	N/A
	~~UBSS~~ [107]	Isogeny	DSSP$^{\oslash}$ & 1MSSCDH$^{\oslash}$	N/E[13]	N/E	N/E	N/A
	~~DVBS~~ [138]	Isogeny	Decisional SSI-T$^{\oslash}$	128 bits	N/E	$\approx$ 1.75	N/A
	CFS [25]	Code	Decisional SD	82 bits	N/E	3100	N/A
	RankSign [25]	Code	Decisional SD	100 bits	N/E	200	N/A
	~~[131]~~	MQ	Rainbow$^{\oslash}$	128 bits	19/5505	28.5	N/A
Ring Signatures[14]	DualRing-LB [159]	Lattice	M-SIS & M-LWE	128 bits	3/1 [15]	5 [16]	$O(N)$
	MatRing [64, 66, 67]	Lattice	M-SIS & M-LWE	128 bits	10/3	11	$O(\log^{1.7} N)$
	SMILE [105]	Lattice	M-SIS & M-LWE	128 bits	N/E	16	$O(\log N)$
	Calamari [19]	Isogeny	Decisional CSIDH	60 bits	$\approx 10^6$	7	$O(\log N)$
	[92]	Hash	MPC-in-the-head	128 bits	2000/2000 [17]	178 [18]	$O(\log N)$
	[56]	Hash	MPC-in-the-head	128 bits	N/E	2125	$O(\log N)$
	[160]	Code	SD	63.3 bits	N/E	0.208 ($N = 10$)	N/A
	[50][19]	Code	GD/GPBD	80 bits	N/E	0.587 ($N = 10, \ell = 9$) [20]	N/A
	[33][21]	Code	GSD	128 bits	N/E	397 ($N = 10$) [22]	N/A
	~~Ringrainbow~~ [118][23]	MQ	Rainbow$^{\oslash}$	128 bits	N/E	0.83 ($N = 10$)	N/A
	[130][24]	MQ	MQ-Problem	80 bits	N/E	324 ($N = 10$)	N/A

[4] Those marked with $^{\oslash}$ indicate the assumptions that have recently been broken (asymptotically or practically). This renders the corresponding schemes insecure, which is indicated by striking through the scheme's name or citation.

[5] The aggregate signature lengths are per signer at the indicated number N of signers.

[6] Due to a gap in the security proof of [62] pointed out in [51], provable security relies on a non-standard variant of MLWE.

[7] Metrics are reported for thresholds of size 2 unless otherwise indicated. Asympt. complexity reported is a function of the threshold k.

[8] This estimate is for a 6-round interactive secure computation 3-party signing protocol ($k = 3$) based on typical LAN latency.

[9] We estimate the runtimes of LAS as 2× of those of Dilithium [61].

[10] This is an estimate size under Bai-Galbraith [9] and Dilithium [61] compression techniques. Also note that Dilithium parameters are more conservative and at a higher security level than those of LAS.

[11] 'N/A' means 'not applicable'.

[12] 'N/E' means 'not evaluated by the authors' and we are unable to estimate.

[13] The 1MSSCDH assumption is broken in [115]. However, a flaw in the securty proof of [107] means that the break does not necessarily imply a polynomial-time attack on UBSS. Its security level is currently unknown.

[14] Metrics are reported for rings of size $N = 32$ unless otherwise stated.

[15] We estimate the runtimes of DualRing-LB as one-thirds of those of MatRing. [159] claims DualRing-LB is 5× faster than MatRing.

[16] It may be possible to reduce the signature length of DualRing-LB using Bai-Galbraith [9] and Dilithium [61] compression techniques.

[17] This signing/verifying time has been given for a ring of size $N = 128$.

[18] This signature size have been approximated thanks to the formula given in [92].

[19] The scheme in [50] is a *threshold* ring signature.

[20] In [50] the signature size is given as $675N - 228\ell$.

[21] The scheme in [33] is a *linkable* ring signature.

[22] In [33] the signature size is provided as 317800N.

[23] Since in the first construction [151] the authors did not provide any efficiency analysis, we provide here the parameters for the later construction [118] which is a *linkable* ring signature scheme.

[24] The scheme in [130] is a *threshold* ring signature.

As formalised in [7], an adaptor signature has four algorithms (AS.PreSign, AS.PreVerify, AS.Adapt, AS.Ext), where the first one is used to create a pre-signature using the signer's secret key, the message and the public statement; and the second is its public verification algorithm. We then have AS.Adapt function, which completes a pre-signature to a full signature using a secret witness. Finally, AS.Ext algorithm takes a pair of (signature, pre-signature) on the same statement and outputs a witness for the statement. As defined in [7], there are three main properties of an adaptor signature: (i) unforgeability, (ii) pre-signature adaptability and (iii) witness extractability. The unforgeability of an adaptor signature is very similar to that of an ordinary signature, but gives the adversary access to a pre-signature on the target message. Even in this case, the adversary is expected to fail in forging an adaptor signature output. In pre-signature adaptability, we expect any user to be able to adapt a valid pre-signature $\hat{\sigma}$ as long as the user knows a witness to the statement used to generate the pre-signature $\hat{\sigma}$. Finally, witness extractability informally requires that a valid witness can be extracted from any given valid pre-signature/signature pair.

Lattice-based approach. The first post-quantum adaptor signature, named LAS, was proposed by Esgin *et al.* in [63]. This builds on the Dilithium signature scheme [61], a third round signature candidate in NIST's Post-Quantum Cryptography standardisation process. Both Dilithium and LAS rely on the two well known computational lattice problems, namely Module-SIS and Module-LWE. The efficiency of LAS is similar to that of Dilithium.

In [63], the authors first extend the formal model for adaptor signature to handle the so-called "knowledge gap" in lattice-based ZKPs. In particular, the proposal in [63] only satisfies *weak* pre-signature adaptability, which means that *extracted* witnesses are not guaranteed to be successful in adapting other pre-signatures. This limitation leads to a more careful analysis of the application of LAS in the blockchain application settings. Nevertheless, the authors of [63] show how to overcome these challenges without incurring additional on-chain costs.

Isogeny-based approach. The only presently-known isogeny-based adaptor signature is IAS (and its optimised variant O-IAS), proposed in 2020 by Tairi et al. [145]. The scheme, like many other isogeny-based signature schemes, is adapted from CSI-FiSh, which itself is obtained from applying the Fiat-Shamir transform [69] to an isogeny-based Schnorr-like identification protocol [140] as discussed in Section 4. In contrast to prior Schnorr-based adaptor signatures [7], the lack of group structure on $\mathcal{E}\ell\ell_p(\mathcal{O})$ prevents a straightforward construction in this setting. The authors overcome this obstruction by introducing additional ZKPs to the protocol which essentially allow participants to verify that the signer is behaving correctly by extending the protocol in [20, Section 5] to prove that certain tuples (E_1, E_1', E_2, E_2') satisfy $\exists\, [\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ s.t. $E_i' = [\mathfrak{a}] * E_i$ for $i = 1, 2$.

Discussion. To the best of our knowledge, LAS and IAS are the only currently-proposed post-quantum adaptor signatures, and their differences are emblematic of the differences between lattice-based and isogeny-based protocols in general. At similar security levels one expects LAS to have much faster signing and verification times, but larger signatures and pre-signatures—for concrete values for specific parameter sets, see Table 1. With the application of well-known compression techniques in the lattice setting to LAS, the gap in signature size gets smaller, though they remain larger than in IAS. The security of LAS is based on the very well-known and extensively-studied M-SIS and M-LWE problems, and so we are relatively confident in its claimed security level. For IAS, security is based on GAIP for the specific case of $\mathrm{cl}(\mathcal{O})$ acting on $\mathcal{E}\ell\ell_p(\mathcal{O})$; the difficulty of this problem for specific CSIDH primes p is still being studied, though it is generally agreed that CSIDH-512 does not offer the 128 bits of quantum security required for NIST level 1; the current state-of-the-art estimates indicate that this parameter set offers only 60 bits of quantum security [128]. This problem is exacerbated by the difficulty of computing the group structure of cl(O), which is required for CSI-FiSh [20] and, consequently, for [145]. In light of these facts, we recommend LAS over IAS, unless signature size is of utmost importance and the relatively low 60-bit security level provided by CSIDH-512 is adequate for the application.

One of the main applications of adaptor signatures is enabling layer 2 protocols, such as payment channel, on scriptless blcockhains. Given that payment channel parties (the payer and the payee) only need to interact with each other off-chain, given their frequency of payments, the current computing time is acceptable. However, the size of signatures that are recorded on the chain should be as small as possible to reduce the size of transactions and blockchains. Given the fact that LAS produces signatures as small as a similar ordinary lattice signature such as Dilithium [61], we find LAS to be an acceptable solution for post-quantum blockchain.

4.4 Privacy: Blind Signature and Ring Signature

4.4.1 Blind signatures. Blind signatures—introduced by Chaum in 1983 for use in untraceable payment systems [42]—are a variant of digital signatures in which a message m chosen by the signature *requester* can be signed by the signer who knows the secret key, without revealing the message to the signer. There are a number of formalisms that encode the intuition of a blind signature scheme; we describe the formalism which appears in, for instance, [3, Definition 1]. In this setting, KeyGen and Verify are as in a digital signature, while Sign is now an *interactive protocol* between a requester (who knows m) and the signer (who knows sk). At the end of the Sign protocol, the requester should have a signature σ on m, while the signer should come away not knowing anything about m. Just as in an ordinary digital signature we have a notion of correctness and unforgeability, which are essentially unchanged. For a blind signature scheme, we also require the *blindness* property, which should encode the signer's lack of knowledge of m; notably, we want this lack of knowledge to extend to cases when the signer is allowed to choose the secret key/public key pair, even when she knows that the message comes from a small collection of messages that she herself has chosen before the interaction.

In [3], blindness is formalised based on an indistinguishability game. An adversary $\mathcal{A}$ (acting as a signer) chooses a secret key/public key pair $(\mathrm{sk}, \mathrm{pk})$ and two messages m_0, m_1, and then interacts with two requesters: one who requests a signature on m_0, and one who requests a signature on m_1. These interactions occur in a random order; once the interactions are done, $\mathcal{A}$ must guess in which order they interacted with the requesters. There are a few closely-related "levels" of blindness, depending on the running time and success probability $\mathcal{A}$ can be allowed to have; formally, we say that the scheme has:

- *Computational blindness* if a PPT adversary cannot win the blindness game with probability non-negligibly greater than $\frac{1}{2}$;
- *Statistical blindness* if an $\mathcal{A}$ whose running time is unbounded cannot win the blindness game with probability non-negligibly greater than $\frac{1}{2}$, and;
- *Perfect blindness* if an $\mathcal{A}$ whose running time is unbounded cannot win the blindness game with probability different from $\frac{1}{2}$.

Blind signatures are used to provide unlinkability and anonymity of transactions in blockchain. For instance, BlindCoin [148] uses blind signatures to hide the mapping between a user's input and output addresses from the mix.

Lattice-based approach. The first lattice-based blind signature was constructed by Rückert [137]. The construction was based on the famous SIS-based Lyubashevsky's identification scheme [102]. At one hand, the Gaussian rejection sampling [103] plays a central role in BLAZE [3] as it is used instead of uniform distribution to achieve smaller sizes. On the other hand, BLAZE is not one-more unforgeable and this deficiency is been addressed in BLAZE+ [4], which reduces the correctness error (inherent in lattice constructions) by a novel approach that allows performing multiple in parallel rejection samplings. This hugely reduces the communication complexity.

Other lattice-based blind signatures with other features also appeared in the literature including [30, 96, 123]. All the above schemes rely on an analysis by Rückert [137] to argue that a collision can be found with non-negligible probability when rewinding. However, such an analysis found to be faulty in [83] implying all of the aforementioned schemes have a subtle flaw in their security proofs. The authors of [83] then proposed a new three-round lattice-based blind signature scheme, whose security can be proved, in the random oracle model, from the standard SIS assumption. Their scheme is only blind in the weaker honest signer model [90] as compared to the malicious signer model [70].

There has been another line of research on constructing lattice-based blind signatures based on preimage sampleable trapdoor functions [73, 98, 161]. All these schemes are also shown to be insecure by [4] as well.

Isogeny-based approach. In contrast with all other isogeny-based protocols in this work, isogeny-based blind signatures use the full supersingular isogeny graph, rather than the complex multiplication graph. There are two constructions: the first - UBSS - given in [107], builds upon the undeniable signature scheme of [89], and unfortunately inherits a flaw in its security proof from [89], given in [115]. Because the security of this protocol is in question, we do not discuss it further here.

The second construction, given in [138], improves upon the construction of [107] in two main ways: (1) It is not vulnerable to the attack of [115], and; (2) It is a designated verifier signature scheme, rather than an undeniable signature scheme. More intuitively, point (2) means that signature verification in the protocol of [138] does not require an interactive protocol involving the signer, though signatures are still *non-transferable*; that is, they can only be verified by a designated party (the *designated verifier*). This protocol requires parties to compute isogenies of four coprime degrees: one prime power degree for hashing messages, blinding/unblinding, signing, and verifying. Generally speaking, in SIDH-like protocols the size of the underlying prime field increases with the number of prime power isogenies required. In this protocol, achieving λ bits of security (both for unforgeability and blindness) requires a prime of at least 7λ bits, which is relatively large (compared with SIDH [88] and SIKE [8], which require primes of only 4λ bits to achieve λ bits of security).

Code-based approach. The first and to the best of our knowledge the only code-based construction of a blind signature has been proposed in [25]. The construction uses a concatenation of Stern-like ZKPs [144] which enables an authentication protocol for concatenated matrices. The blind signature based on the Hamming metric and is obtained by applying the Fiat-Shamir heuristic to the authentication protocol. The security of the construction relies on the security of a trapdoor function for the computational syndrome decoding problem (CSD) problem and the soundness of the underlying ZKP. While for the Hamming metric this trapdoor function is given by the CFS signature and for the Rank metric it is given by the RankSign protocol [72]. The authors provide the parameters for rank metric and for Hamming metric, which are practical for the first metric but less practical for the latter one. In term of the signature size, the instantiation with the Hamming metric is outperformed by the instantiation for the rank metric by multiple times.

Multivariate approach. The first multivariate construction has been proposed in [131]. The blind signature is obtained by a transformation of Rainbow, a multivariate quadratic (MQ) signature scheme and a post-quantum candidate to the NIST competition. The transformation is achieved by combining the MQ signature scheme with the MQ-based zero-knowledge identification protocol from [139]. In terms of security, the scheme achieves the usual blindness property and the universal one-more unforgeability. Regarding the efficiency, the most costly part for the user is the execution of the public key generation procedure of Rainbow signature scheme.

Discussion. Although the incorrect provable lattice-based blind signatures BLAZE [3] and BLAZE+ [4] and their parents [137] can offer practical key and signature sizes (in the order of only a few kilobytes or in some cases less than 1 KB), the only correct-proof lattice based blind signatures [83] have either signatures sizes on the order of megabytes or large keys due to homomorphic nature of the construction, respectively. Hence, an outstanding open problem is to construct a practical (in terms of key and signature sizes) and secure (in the malicious signer model) lattice-based blind signature from standard assumptions. The MQ-based scheme of [131] guarantees the usual blindness security property and the universal one-more unforgeability. Regarding the efficiency, the most costly part for the user is the execution of the public key generation procedure of Rainbow signature scheme. Compared to the existing lattice-based construction [137], this MQ-based construction benefits from a shorter signature size on one side but on the other side it required larger public keys than in [137]. For a 100 bits of security, [131] gives shorter signature sizes 17.6 KB but larger pk size 54.6 KB compared to 200 KB and 15 KB, respectively for the shortest code-based blind signature RankSign [72]. Our final recommendation is to use [131], which enjoys reasonable key and signature sizes and is based on well-understood multivariate assumptions. For further performance metrics and the effect of recent attacks on these blind signature proposals, see Table 1.

Given that a number of isogeny-based and multivariate blind signatures have been rendered insecure due to recent attacks and that the remaining ones are quite inefficient, we believe there is a lot of further progress to be done in the area of post-quantum blind signatures. Particularly for blockchain application, one would expect to have significant efficiency improvements before they can be acceptable for deployment.

4.4.2 Ring signatures. Ring signatures were first introduced in 2001 by Rivest, Shamir and Tauman [135], initially to allow authoritative but anonymous secret leaking, but have found other applications to the blockchain. The rigorous formal definitions were established in [15].

An ordinary ring signature scheme has much the same structure and security requirements as a ordinary digital signature. The main syntactic difference between the two is that, in a ring signature scheme, the Sign and Verify functions take as input a collection of users R, called a *ring*. A signer can sign on behalf of any ring that includes her public key. Any third party can verify that a signature was generated by a ring member on behalf of the ring, but the verification process will not reveal any information about which ring member produced the signature.

Correctness of ring signatures is analogous to that of ordinary digital signatures. Their unforgeability is more complicated, since they are required to be unforgeable in the face of *insider corruption.* Informally, we say that a ring signature is *unforgeable with respect to insider corruption* if an efficient adversary cannot forge a signature on behalf of a ring R^*, even with access to a signing oracle of each user not in R^*.

Ring signatures must satisfy the additional property of *anonymity (against full key exposure)* which requires that an efficient adversary $\mathcal{A}$ cannot tell which of two users $\mathsf{pk}_{i_0}, \mathsf{pk}_{i_1}$ in a ring R produced a given signature σ on a message m on behalf of R, even if $\mathcal{A}$ is given access to each user's secret key, and even if $\mathcal{A}$ is allowed to choose R, m, i_0, and i_1. This security definition includes two intuitively important scenarios: (1) *Insider collusion:* No collection of users can determine which ring member produced a given signature on behalf of the ring; (2) *Key exposure:* If a user's private key is revealed, signatures produced by that user cannot be deanonymised.

Linkable ring signatures are a variant of ring signatures introduced in 2004 by Liu *et al.* [100]. They enhance ring signatures by adding a new functionality—*linking*—which allows anybody to determine whether two signatures were produced by the same user, without revealing that user.

This functionality is instantiated as a function Link which takes in two signatures and outputs a bit b indicating whether the signatures were produced by the same user.

This new functionality introduces new correctness and security requirements, i.e., *linkage correctness*: if two signatures σ_0 and σ_1 are generated by the same user, then $\mathsf{Link}(\sigma_0, \sigma_1) = 1$; and further three properties:

- *Linkability*: Among any $N + 1$ signatures, each signed on behalf of rings which are subsets of a fixed ring of N users, there must be a linking pair of signatures;
- *Linkable anonymity:* Given two public keys $\mathsf{pk}_0, \mathsf{pk}_1$ whose corresponding private keys are $\mathsf{sk}_0, \mathsf{sk}_1$, resp., and two disjoint lists S_0, S_1 of ring signatures, which contain pk_0 and pk_1, such that either all those signatures in S_0 were constructed using sk_0 and all those in S_1 were constructed using s_1, or *vice versa*, no efficient adversary can determine which is the case, and;
- *Non-frameability against insider collusion:* No efficient adversary can produce a new valid signature which links to any honestly-constructed signature σ, even with access to the secret key of each user.

In the literature, one often distinguishes: (i) logarithmic ring signature, where the signature size scales polylogarithmically in the ring size N, and (ii) linear ring signature, where the signature size is $O(N)$.

Lattice-based approach. Until recently, lattice-based ring signature proposals were far from practical. Then, in 2019, Esgin *et al.* [65] introduced a substantially more efficient ring signature construction based on Module-SIS and Module-LWE problems and initiated the path towards practically efficient lattice-based ring signatures. This construction also has the advantage of being of polylogarithmic size. The blueprint idea in [65] has been greatly improved upon in subsequent works [64, 66, 67], where the signature size was reduced by orders of magnitude in comparison to the state of the art prior to [65]. The shortest proposal in this family is obtained by instantiating the ring signature in [64] using the techniques in [66, 67], which allow to set parameters significantly more efficiently. We call the state-of-the-art proposal resulting from this series of works as $\mathsf{MatRing}$ signature. This proposal also easily extends to the *linkable* setting as shown in [66, 67].

Recently, Beullens *et al.* [19] and Lyubashevsky *et al.* [105] proposed new approaches to construct ring signatures with instantiations based on Module-SIS and Module-LWE problems. Overall, all schemes in [19, 64, 65, 67, 105] scale polylogarithmically in signature size, but Falafl [19] and the proposal in [105] scale more efficiently in *asymptotic* signature size. The practical advantage of the latter two proposals' concrete signature sizes, however, is only observed for large ring sizes of about 1000 (and even much larger ring sizes for Falafl). In Table 1, we consider $\mathsf{MatRing}$ and [105] as either one leads to the most practically efficient scheme for any ring size.

There are also some efficient linear-size ring signature proposals: Raptor by Lu *et al.* [101] and DualRing-LB by Yeun *et al.* [159]. Despite being linear-sized, DualRing-LB signature sizes scale slowly thanks to its novel approach, which requires a single ZKP response and N challenges for a ring size of N users. The advantage comes from the fact that the size of a challenge (at most 32 bytes) is significantly smaller than the size of a ZKP response (a few kilobytes) in the lattice setting. From the security perspective, although Raptor relies on a stronger "NTRU-like" security assumption, DualRing-LB is based on standard Module-SIS and Module-LWE assumptions. DualRing-LB produces very short signatures for small to medium size rings (see Table 1).

Some of the aforementioned works on constructing ring signatures also extend their proposals to build a RingCT protocol (employed by Monero), where the ring signature is a core ingredient. A RingCT protocol [122] allows a *payer/spender* to transfer assets on blockchain to a *payee/recipient* while preserving privacy, i.e., while hiding sensitive information such as payer/payee identities and transaction amount from third parties. The payer anonymity is achieved by the use of a linkable ring signature and further advanced ZKPs are employed to construct a full RingCT protocol. Due their strong connection to ring signatures, we briefly mention these works below.

The work of Esgin *et al.* [67] introduced the first practical post-quantum RingCT protocol, named MatRiCT. More recently, MatRiCT was significantly improved upon by Esgin, Steinfeld and Zhao in [66]. The recent protocol, named MatRiCT$^+$ [66], requires significantly less communication and computation, and has the important feature that the proof length scales only logarithmically in the number of input accounts while MatRiCT (as well as other prior post-quantum proposals) scales linearly in that. Concurrently with MatRiCT$^+$, Lyubashevsky, Nguyen and Seiler [105] instantiated the MatRiCT framework using different approaches to realise the underlying proofs. For the most common Monero transactions (with two inputs/outputs and ring size of $N = 11$), MatRiCT$^+$ and the proposal in [105] require very similar communication while MatRiCT$^+$ scales much more efficiently to larger number of inputs (which is the second most common setting in Monero).

Hash-based approach. [92] has outlined how to build a ring signature from their proposed zero-knowledge protocol based on symmetric primitives (more details will be discussed in Section 4). The idea is to based on the (normal) signature proposed in their paper. Key generation chooses a uniform secret key $k \in \{0,1\}^\kappa$ for some security parameter κ and the corresponding public key will be $y = \mathsf{PRF}_k(0^\kappa)$ for some pseudorandom function PRF. Given a ring $R = \{y_i\}_{i=1}^N$ of N public keys, let C be the circuit that takes as input a secret key k and outputs 1 iff $\mathsf{PRF}_k(0^\kappa) = y_i$ for some $i \in [1, N]$. A ring signature will then be an NIZKPoK of an input k_i such that $C(k_i) = 1$. The size of the signature (that is, the size of the circuit C in this case) is linear with N, the number of users in R.

In order to shorten the signature size to logarithmic in N, [92] further suggested to use a Merkle tree and put all the public keys y_i as leaves (for simplicity, they assume $N = 2^q$ for some integer q). The proof further takes an auxiliary value path which outputs 1 if path is a valid Merkle proof (with respect to root) for the value y at leaf i. A signature is an NIZKPoK of an input for which C evaluates to 1. In this case, the size is only $\log(N)$.

Isogeny-based constructions. The only isogeny-based (linkable) ring signature to date is Calamari [19]. At its core is a sigma protocol Π which allows a prover to prove knowledge of the solution to one *out of* N instances $E_1 = [\mathfrak{a}_1] * E_0, E_2 = [\mathfrak{a}_2] * X_0, \ldots, E_N = [\mathfrak{a}_N] * E_0$ of the GAIP with respect to the same base E_0, without revealing the index j^* of the known solution. The signature scheme is constructed by applying the Fiat-Shamir transform [69].

To make this into a linkable ring signature, the authors propose to add a tag $T = [\mathfrak{a}_i] \star T_0$ to each signature, where $\star$ is an action of the group G on some set $\mathcal{T}$ (different from and "compatible with," in a precise sense, the action $*$), and T_0 is a fixed public value. When signing, the signer then produces a proof of knowledge of the element $[\mathfrak{a}]$ such that $[\mathfrak{a}] * E_0 = E_j$ for some j, and such that $[\mathfrak{a}] \star T_0 = T$. Since T_0 is fixed, to test whether two signatures $\sigma_1 = (\hat{\sigma}_1, T_1)$ and $\sigma_2 = (\hat{\sigma}_2, T_2)$ were generated by the same individual, it suffices to check that $T_1 = T_2$.

Beyond the basics of the scheme we describe here, Calamari makes a number of optimisations to reduce signature sizes. Calamari signatures are extremely small and scale logarithmically with ring size; for two-member ring signatures are 3.5 KB, and are 23 KB long for rings of size 2^{21}. However, signing is orders of magnitude slower than for the comparable lattice-based ring signature Falafl, requiring from 10^{11} to more than 10^{13} cycles for signing, compared to Falafl's 10^8 to 10^{10} cycles (depending on ring size). As well, this relatively efficient version of Calamari can only be instantiated when the group structure of $\mathrm{cl}(\mathcal{O})$ is known explicitly; at present, this restricts us to the CSIDH-512 parameter set (or smaller), which offers only 60 bits of quantum security [128].

Code-based approach. The first code-based ring signature has been proposed in [160]. In terms of security the signature is secure under the syndrome decoding problem. The authors achieve a signature size of $144 + 126N$, where N is the number of ring members for a security level of about $2^{63.3}$. A special flavour of ring signatures, a ℓ-out-of-N threshold ring signature has been introduced in [50]. It allows a set of ℓ ring members to sign a message without revealing the identities of the members, with a ring size of N. The security of the scheme is given in the reductionist security model and the construction is secure under the hardness of Bounded Distance Decoding (BDD) problem and Goppa Code Distinguishing (GCD) problem. While the signature size is small the main drawback of this construction is the large size of public keys and the slow signing procedure. The first code-based linkable ring signature has been proposed in [33]. It is achieved from a Stern-like protocol which is transformed into a ring signature by applying the Fiat-Shamir transform. The signature size in [33] is $39N$ kBytes, where N is the number of signers in the ring. A recent construction of a ring signature [34] achieves also the additional property of traceability which allows to identify the user who signs two different messages with respect to the same ring. The security of this construction is based on the hardness of the syndrom decoding problem. The signature size is $240N$ kBytes, which might be too large for many applications.

Multivariate approach. The first multivariate quadratic polynomials-based ring signature was introduced in [151]. The scheme achieves completeness and anonymity against full key exposure. A more efficient construction has been proposed in [118]. In [130] the authors provided the first multivariate threshold ring signature scheme which is an extension of the multivariate identification scheme [139]. Even though the construction in [130] requires more rounds to achieve given levels of security, the main advantage of the scheme is the shorter signature size than those obtained by other post-quantum approaches. The construction also achieves provable security which is rare in multivariate cryptography.

Discussion. Ring signatures have certain inherent limitations such as requiring $O(N)$ signing/verification times and $O(N)$ storage/communication of public keys. Such linear barriers prevent their real-life use with large values of N despite the appealing feature of a higher anonymity level for increasing N. This is, for example, one of the main reasons why Monero cryptocurrency uses a small ring size of $N = 11$. As a result, in terms of blockchain applications, the main desideratum appears to be optimizing the performance for small N.

While the most efficient lattice-based and hash-based constructions scale polylogarithmically in the ring size N, code-based constructions can only achieve a linear signature size, which is the main drawback of code-based constructions. Finding new techniques to reduce the key and signature sizes of code-based signatures is an open problem and offers directions for future research. Isogeny-based schemes scale logarithmically with ring size but are slower than their lattice-based counterparts. Multivariate constructions claim to achieve better efficiency than any other post-quantum ring signature constructions. For detailed evaluation of these results, see Table 1.

The computational speed of existing lattice-based ring signature proposals in the order of milliseconds is well within the requirements of major ring signature applications in the blockchain setting, such as RingCT protocol used in Monero. In terms of the signature size, there is of course a significant increase compared to pre-quantum proposals, however this overhead appears to be a common cost to be paid when upgrading to post-quantum security. A goal for future work in this area could be to minimize the signature as well as public key lengths as much as possible.

5 CONCLUSION

This work surveys the extensive literature on post-quantum cryptographic schemes crucial for blockchains. We particularly focus on exotic signatures achieving advanced functionalities, which enable empowering features for blockchain. For each presented exotic signature, we have included all known construction techniques based on different quantum-safe assumptions (including lattice-based, code-based, hash-based, multivariate-polynomial-based and isogeny-based assumptions) and a discussion on existing challenges and future research directions for each one in the post-quantum space. We have also compared these exotic signatures in terms of the promised quantum security levels, signature generation and verification times, signature size, and the promised asymptotic complexity. We hope our work can help to promote further research on and adoption of post-quantum cryptography in the blockchain space.

REFERENCES

[1] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 99–108, New York, NY, USA, 1996. Association for Computing Machinery.

[2] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen, and M. Zohner. Ciphers for MPC and FHE. In E. Oswald and M. Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015, Proceedings, Part I*, volume 9056 of *LNCS*, pages 430–454. Springer, 2015.

[3] N. Alkeilani Alkadri, R. El Bansarkhani, and J. Buchmann. Blaze: Practical lattice-based blind signatures for privacy-preserving applications. In J. Bonneau and N. Heninger, editors, *Financial Cryptography and Data Security*, pages 484–502, Cham, 2020. Springer International Publishing.

[4] N. Alkeilani Alkadri, R. El Bansarkhani, and J. Buchmann. On lattice-based interactive protocols: An approach with less or no aborts. In J. K. Liu and H. Cui, editors, *Information Security and Privacy*, pages 41–61, Cham, 2020. Springer International Publishing.

[5] G. Andresen. BIP 0011: M-of-N Standard Transactions, 2011. https://en.bitcoin.it/wiki/BIP_0011.

[6] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[7] L. Aumayr, O. Ersoy, A. Erwig, S. Faust, K. Hostáková, M. Maffei, P. Moreno-Sanchez, and S. Riahi. Generalized bitcoin-compatible channels. *IACR Cryptol. ePrint Arch.*, 2020:476, 2020.

[8] R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Hutchinson, A. Jalali, K. Karabina, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, and D. Urbanik. Supersingular isogeny key encapsulation. Technical report, 2017.

[9] S. Bai and S. D. Galbraith. An improved compression technique for signatures based on learning with errors. In *CT-RSA*, volume 8366 of *LNCS*, pages 28–47. Springer, 2014.

[10] R. E. Bansarkhani, M. S. E. Mohamed, and A. Petzoldt. MQSAS - A multivariate sequential aggregate signature scheme. In M. Bishop and A. C. A. Nascimento, editors, *Information Security - ISC 2016, Proceedings*, volume 9866 of *LNCS*, pages 426–439. Springer, 2016.

[11] I. Barmes and B. Bosch. Quantum computers and the bitcoin blockchain. https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-the-bitcoin-blockchain.html.

[12] C. Baum, C. D. de Saint Guilhem, D. Kales, E. Orsini, P. Scholl, and G. Zaverucha. Banquet: Short and fast signatures from AES. In J. A. Garay, editor, *Public-Key Cryptography - PKC 2021 - Proceedings, Part I*, volume 12710 of *Lecture Notes in Computer Science*, pages 266–297. Springer, 2021.

[13] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptol. ePrint Arch.*, 2018:46, 2018.

[14] E. Ben-Sasson, A. Chiesa, M. Riabzev, N. Spooner, M. Virza, and N. P. Ward. Aurora: Transparent succinct arguments for R1CS. In Y. Ishai and V. Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019, Proceedings, Part I*, volume 11476 of *LNCS*, pages 103–128. Springer, 2019.

[15] A. Bender, J. Katz, and R. Morselli. Ring signatures: Stronger definitions, and constructions without random oracles. In *TCC*, volume 3876 of *LNCS*, pages 60–79. Springer, 2006.

[16] R. Bendlin, S. Krehbiel, and C. Peikert. How to share a lattice trapdoor: Threshold protocols for signatures and (H)IBE. In *ACNS*, volume 7954 of *Lecture Notes in Computer Science*, pages 218–236. Springer, 2013.

[17] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Trans. Inf. Theory*, 24(3):384–386, 1978.

[18] W. Beullens. Breaking rainbow takes a weekend on a laptop. *IACR Cryptol. ePrint Arch.*, page 214, 2022. (to appear at CRYPTO 2022).

[19] W. Beullens, S. Katsumata, and F. Pintore. Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In S. Moriai and H. Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 464–492, Cham,

2020. Springer International Publishing.

[20] W. Beullens, T. Kleinjung, and F. Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In S. D. Galbraith and S. Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 227–247, Cham, 2019. Springer International Publishing.

[21] W. Beullens, B. Preneel, A. Szepieniec, and F. Vercauteren. Luov: Signature scheme proposal for nist pqc project. *Submission to the NIST's post-quantum cryptography standardization process*, 2019.

[22] R. Bhadauria, Z. Fang, C. Hazay, M. Venkitasubramaniam, T. Xie, and Y. Zhang. Ligero++: a new optimized sublinear iop. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 2025–2038, 2020.

[23] Bitcoin Wiki. Script, 2022. [Online; accessed 31-January-2022].

[24] G. R. Blakley. Safeguarding cryptographic keys. In *Managing Requirements Knowledge, International Workshop on*, page 313, Los Alamitos, CA, USA, jun 1979. IEEE Computer Society.

[25] O. Blazy, P. Gaborit, J. Schrek, and N. Sendrier. A code-based blind signature. In *2017 IEEE International Symposium on Information Theory, ISIT 2017, Aachen, Germany, June 25-30, 2017*, pages 2718–2722. IEEE, 2017.

[26] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry. Random oracles in a quantum world. In D. H. Lee and X. Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, pages 41–69, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[27] D. Boneh, R. Gennaro, S. Goldfeder, A. Jain, S. Kim, P. M. R. Rasmussen, and A. Sahai. Threshold cryptosystems from threshold fully homomorphic encryption. In *Advances in Cryptology - CRYPTO 2018 - Proceedings, Part I*, pages 565–596, 2018.

[28] D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In E. Biham, editor, *Advances in Cryptology - EUROCRYPT 2003, Proceedings*, volume 2656 of *LNCS*, pages 416–432. Springer, 2003.

[29] D. Boneh and M. Zhandry. Quantum-secure message authentication codes. In T. Johansson and P. Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 592–608, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[30] S. Bouaziz-Ermann, S. Canard, G. Eberhart, G. Kaim, A. Roux-Langlois, and J. Traoré. Lattice-based (partially) blind signature without restart. Cryptology ePrint Archive, Report 2020/260, 2020. https://eprint.iacr.org/2020/260.

[31] K. Boudgoust and A. Roux-Langlois. Non-interactive half-aggregate signatures based on module lattices - a first attempt. Cryptology ePrint Archive, Paper 2021/263, 2021. https://eprint.iacr.org/2021/263.

[32] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Trans. Comput. Theory*, 6(3):13:1–13:36, 2014.

[33] P. Branco and P. Mateus. A code-based linkable ring signature scheme. In J. Baek, W. Susilo, and J. Kim, editors, *Provable Security - ProvSec 2018, Proceedings*, volume 11192 of *LNCS*, pages 203–219. Springer, 2018.

[34] P. Branco and P. Mateus. A traceable ring signature scheme based on coding theory. In J. Ding and R. Steinwandt, editors, *Post-Quantum Cryptography - 2019 Revised Selected Papers*, volume 11505 of *LNCS*, pages 387–403. Springer, 2019.

[35] C. Brunetta, B. Liang, and A. Mitrokotsa. Code-based zero knowledge PRF arguments. In Z. Lin, C. Papamanthou, and M. Polychronakis, editors, *Information Security - 22nd International Conference, ISC 2019, Proceedings*, volume 11723 of *LNCS*, pages 171–189. Springer, 2019.

[36] C. Cachin and M. Vukolic. Blockchain consensus protocols in the wild (keynote talk). In A. W. Richa, editor, *DISC2017*, volume 91 of *LIPIcs*, pages 1:1–1:16. Schloss Dagstuhl - Leibniz-Zentrum fur Informatik, 2017.

[37] T. Cao, J. Yu, J. Decouchant, X. Luo, and P. Veríssimo. Exploring the monero peer-to-peer network. In J. Bonneau and N. Heninger, editors, *Financial Cryptography and Data Security - FC, 2020 Revised Selected Papers*, volume 12059 of *LNCS*, pages 578–594. Springer, 2020.

[38] M. Castro and B. Liskov. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Trans. Comput. Syst.*, 20(4):398–461, 2002.

[39] W. Castryck and T. Decru. An efficient key recovery attack on sidh (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022.

[40] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. Csidh: An efficient post-quantum commutative group action. In T. Peyrin and S. Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427. Springer International Publishing, 2018.

[41] 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 *Proceedings of the 2017 acm sigsac conference on computer and communications security*, pages 1825–1842, 2017.

[42] D. Chaum. Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology: Proceedings of CRYPTO '82*, pages 199–203. Plenum Press, New York, 1982.

[43] J. O. M. Chervinski, D. Kreutz, and J. Yu. Floodxmr: Low-cost transaction flooding attack with monero's bulletproof protocol. *IACR Cryptol. ePrint Arch.*, 2019:455, 2019.

[44] N. D. Chiano, R. Longo, A. Meneghetti, and G. Santilli. A survey on NIST PQ signatures. *CoRR*, abs/2107.11082, 2021.

[45] J.-M. Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. https://eprint.iacr.org/2006/291.

[46] D. Cozzo and N. P. Smart. Sharing the LUOV: threshold post-quantum signatures. In *Cryptography and Coding - 17th IMA International Conference, IMACC, Proceedings*, pages 128–153, 2019.

[47] D. Cozzo and N. P. Smart. Sashimi: Cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol. In J. Ding and J.-P. Tillich, editors, *Post-Quantum Cryptography*, pages 169–186, Cham, 2020. Springer International Publishing.

[48] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. E. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer. On scaling decentralized blockchains - (A position paper). In J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. S. Wallach, M. Brenner, and K. Rohloff, editors, *FC2016*, volume 9604 of *LNCS*, pages 106–125. Springer, 2016.

[49] Cryptonote currencies, 2018.

[50] L. Dallot and D. Vergnaud. Provably secure code-based threshold ring signatures. In M. G. Parker, editor, *Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009. Proceedings*, volume 5921 of *LNCS*, pages 222–235. Springer, 2009.

[51] I. Damgård, C. Orlandi, A. Takahashi, and M. Tibouchi. Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices. In *PKC 2021, Part I*, pages 99–130, 2021.

[52] L. De Feo and S. D. Galbraith. Seasign: Compact isogeny signatures from class group actions. In Y. Ishai and V. Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 759–789, Cham, 2019. Springer International Publishing.

[53] L. De Feo and M. Meyer. Threshold schemes from isogeny assumptions. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *Public-Key Cryptography – PKC 2020*, pages 187–212, Cham, 2020. Springer International Publishing.

[54] C. D. de Saint Guilhem, L. De Meyer, E. Orsini, and N. P. Smart. Bbq: using aes in picnic signatures. In *International Conference on Selected Areas in Cryptography*, pages 669–692. Springer, 2019.

[55] J. Decouchant, D. Kozhaya, V. Rahli, and J. Yu. Damysus: Streamlined bft consensus leveraging trusted components. In *European Conference on Computer Systems (EuroSys)*, 2022.

[56] D. Derler, S. Ramacher, and D. Slamanig. Post-quantum zero-knowledge proofs for accumulators with applications to ring signatures from symmetric-key primitives. In *International Conference on Post-Quantum Cryptography*, pages 419–440. Springer, 2018.

[57] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In J. Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 457–469, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

[58] J. Ding and D. Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *ACNS*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175, 2005.

[59] Y. Doröz, J. Hoffstein, J. H. Silverman, and B. Sunar. MMSAT: A scheme for multimessage multiuser signature aggregation. *IACR Cryptol. ePrint Arch.*, 2020:520, 2020.

[60] T. Dryja. Discrete log contracts. https://adiabat.github.io/dlc.pdf.

[61] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé. Crystals–Dilithium: Digital signatures from module lattices. In *CHES*, volume 2018-1, 2018. https://eprint.iacr.org/2017/633.pdf.

[62] R. El Bansarkhani and J. Sturm. An efficient lattice-based multisignature scheme with applications to bitcoins. In *International Conference on Cryptology and Network Security*, pages 140–155. Springer, 2016.

[63] M. F. Esgin, O. Ersoy, and Z. Erkin. Post-quantum adaptor signatures and payment channel networks. In *ESORICS (2)*, volume 12309 of *LNCS*, pages 378–397. Springer, 2020.

[64] M. F. Esgin, R. Steinfeld, J. K. Liu, and D. Liu. Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications. In *CRYPTO (1)*, volume 11692 of *LNCS*, pages 115–146. Springer, 2019. (Full version at ia.cr/2019/445).

[65] M. F. Esgin, R. Steinfeld, A. Sakzad, J. K. Liu, and D. Liu. Short lattice-based one-out-of-many proofs and applications to ring signatures. In *ACNS*, LNCS, pages 67–88. Springer, 2019. (Full version at ia.cr/2018/773).

[66] M. F. Esgin, R. Steinfeld, and R. K. Zhao. MatRiCT^{+}: More efficient post-quantum private blockchain payments. In *IEEE Symposium on Security and Privacy*, pages 1281–1298. IEEE, 2022. (Full version at ia.cr/2021/545).

[67] M. F. Esgin, R. K. Zhao, R. Steinfeld, J. K. Liu, and D. Liu. MatRiCT: Efficient, scalable and post-quantum blockchain confidential transactions protocol. In *ACM CCS 2019, Proceedings*, pages 567–584. ACM, 2019. (Full version at ia.cr/2019/1287).

[68] T. M. Fernández-Caramés and P. Fraga-Lamas. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, 8:21091–21116, 2020.

[69] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, *Advances in Cryptology — CRYPTO' 86*, pages 186–194, Berlin, Heidelberg, 1987. Springer Berlin

Heidelberg.

[70] M. Fischlin. Round-optimal composable blind signatures in the common reference string model. In C. Dwork, editor, *Advances in Cryptology - CRYPTO 2006*, pages 60–77, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[71] M. Fukumitsu and S. Hasegawa. A lattice-based provably secure multisignature scheme in quantum random oracle model. In *ProvSec 2020*, pages 45–64, 2020.

[72] P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor. Ranksign: An efficient signature algorithm based on the rank metric. In M. Mosca, editor, *Post-Quantum Cryptography - PQCrypto 2014, Proceedings*, volume 8772 of *LNCS*, pages 88–107. Springer, 2014.

[73] W. Gao, Y. Hu, B. Wang, and J. Xie. Identity-based blind signature from lattices in standard model. In K. Chen, D. Lin, and M. Yung, editors, *Information Security and Cryptology*, pages 205–218, Cham, 2017. Springer International Publishing.

[74] R. Gennaro, S. Goldfeder, and A. Narayanan. Threshold-optimal DSA/ECDSA signatures and an application to bitcoin wallet security. In *ACNS 2016, Proceedings*, pages 156–174. Springer, 2016.

[75] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust threshold dss signatures. *Information and Computation*, 164(1):54–84, 2001.

[76] I. Giacomelli, J. Madsen, and C. Orlandi. Zkboo: Faster zero-knowledge for boolean circuits. In *25th {usenix} security symposium ({usenix} security 16)*, pages 1069–1083, 2016.

[77] G. Golan-Gueta, I. Abraham, S. Grossman, D. Malkhi, B. Pinkas, M. K. Reiter, D. Seredinschi, O. Tamir, and A. Tomescu. SBFT: A scalable and decentralized trust infrastructure. In *49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2019, Portland, OR, USA, June 24-27, 2019*, pages 568–580. IEEE, 2019.

[78] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In R. Sedgewick, editor, *ACM STOC, 1985, Proceedings*, pages 291–304. ACM, 1985.

[79] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais. Sok: Layer-two blockchain protocols. In J. Bonneau and N. Heninger, editors, *Financial Cryptography and Data Security - FC 2020 Revised Selected Papers*, volume 12059 of *Lecture Notes in Computer Science*, pages 201–226. Springer, 2020.

[80] T. Güneysu, V. Lyubashevsky, and T. Pöppelmann. Practical lattice-based cryptography: A signature scheme for embedded systems. In *Cryptographic Hardware and Embedded Systems - CHES 2012, Proceedings*, pages 530–547, 2012.

[81] R. Han, H. Lin, and J. Yu. On the optionality and fairness of atomic swaps. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019*, pages 62–75. ACM, 2019.

[82] L. Harn. Group-oriented (t, n) threshold digital signature scheme and digital multisignature. *IEE Proceedings - Computers and Digital Techniques*, 141:307–313(6), September 1994.

[83] E. Hauck, E. Kiltz, J. Loss, and N. K. Nguyen. Lattice-based blind signatures, revisited. In D. Micciancio and T. Ristenpart, editors, *Advances in Cryptology – CRYPTO 2020*, pages 500–529, Cham, 2020. Springer International Publishing.

[84] J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, and W. Whyte. Practical signatures from the partial fourier recovery problem. In *Applied Cryptography and Network Security - ACNS 2014. Proceedings*, pages 476–493, 2014.

[85] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai. Zero-knowledge proofs from secure multiparty computation. *SIAM Journal on Computing*, 39(3):1121–1152, 2009.

[86] K. Itakura and K. Nakamura. A public-key cryptosystem suitable for digital multisignatures. *NEC Research & Development*, 71:1–8, 1983.

[87] A. Jain, S. Krenn, K. Pietrzak, and A. Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In X. Wang and K. Sako, editors, *Advances in Cryptology - ASIACRYPT 2012, Proceedings*, volume 7658 of *LNCS*, pages 663–680. Springer, 2012.

[88] D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In B.-Y. Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[89] D. Jao and V. Soukharev. Isogeny-based quantum-resistant undeniable signatures. In M. Mosca, editor, *Post-Quantum Cryptography*, pages 160–179, Cham, 2014. Springer International Publishing.

[90] A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures. In B. S. Kaliski, editor, *Advances in Cryptology — CRYPTO '97*, pages 150–164, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[91] D. Kales and G. Zaverucha. Improving the performance of the picnic signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 154–188, 2020.

[92] J. Katz, V. Kolesnikov, and X. Wang. Improved non-interactive zero knowledge with applications to post-quantum signatures. In *ACM SIGSAC CCS 2018, Proceedings*, pages 525–537, 2018.

[93] A. Kumar, C. Fischer, S. Tople, and P. Saxena. A traceability analysis of Monero's blockchain. In *ESORICS*, pages 153–173, 2017.

[94] L. Lamport. Constructing digital signatures from a one-way function. Technical report, Citeseer, 1979.

[95] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 75(3):565–599, 2015.

[96] H. Q. Le, W. Susilo, T. X. Khuc, M. K. Bui, and D. H. Duong. A blind signature from module latices. In *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8, 2019.

[97] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534.

[98] C. Liang, C. Yongquan, T. Xueming, H. Dongping, and W. Xin. Hierarchical id-based blind signature from lattices. In *2011 Seventh International Conference on Computational Intelligence and Security*, pages 803–807, 2011.

[99] Y. Lindell. Fast secure two-party ECDSA signing. In *Advances in Cryptology - CRYPTO 2017, Proceedings, Part II*, LNCS, pages 613–644. Springer, 2017.

[100] J. K. Liu, V. K. Wei, and D. S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups. In H. Wang, J. Pieprzyk, and V. Varadharajan, editors, *Information Security and Privacy*, pages 325–335, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[101] X. Lu, M. H. Au, and Z. Zhang. Raptor: A practical lattice-based (linkable) ring signature. In *ACNS*, volume 11464 of *LNCS*, pages 110–130. Springer, 2019.

[102] V. Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In *ASIACRYPT*, pages 598–616. Springer, 2009.

[103] V. Lyubashevsky. Lattice signatures without trapdoors. In *Advances in Cryptology - EUROCRYPT 2012, Proceedings*, LNCS, pages 738–755, 2012.

[104] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 144–155. Springer, 2006.

[105] V. Lyubashevsky, N. K. Nguyen, and G. Seiler. SMILE: Set membership from ideal lattices with applications to ring signatures and confidential transactions. Cryptology ePrint Archive, Report 2021/564, 2021. ia.cr/2021/564 (to appear at Crypto 2021).

[106] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.

[107] S. M. S. and V. Chandrasekaran. Isogeny-based quantum-resistant undeniable blind signature scheme. *International Journal of Network Security*, 20:9–18, 01 2018.

[108] C. Ma and M. Jiang. Practical lattice-based multisignature schemes for blockchains. *IEEE Access*, 7:179765–179778, 2019.

[109] L. Maino and C. Martindale. An attack on sidh with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026, 2022. https://eprint.iacr.org/2022/1026.

[110] G. Malavolta, P. Moreno-Sanchez, C. Schneidewind, A. Kate, and M. Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability. In *NDSS, 2019*, 2019.

[111] D. Malkhi and M. K. Reiter. Byzantine quorum systems. In *Theory of Computing*, 1997.

[112] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and C. G. Günther, editors, *Advances in Cryptology — EUROCRYPT '88*, pages 419–453, Berlin, Heidelberg, 1988. Springer Berlin Heidelberg.

[113] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille. Simple Schnorr multi-signatures with applications to bitcoin. *Designs, Codes and Cryptography*, 87(9):2139–2164, 2019.

[114] R. C. Merkle. A certified digital signature. In G. Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238. Springer, 1989.

[115] S.-P. Merz, R. Minko, and C. Petit. Another look at some isogeny hardness assumptions. In S. Jarecki, editor, *Topics in Cryptology – CT-RSA 2020*, pages 496–511, Cham, 2020. Springer International Publishing.

[116] D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. *Comput. Complex.*, 16(4):365–411, 2007.

[117] A. Mirzaei, A. Sakzad, J. Yu, and R. Steinfeld. FPPW: A fair and privacy preserving watchtower for bitcoin. In *FC*, 2021.

[118] M. S. E. Mohamed and A. Petzoldt. Ringrainbow - an efficient multivariate ring signature scheme. In M. Joye and A. Nitaj, editors, *Progress in Cryptology - AFRICACRYPT 2017, Proceedings*, volume 10239 of *LNCS*, pages 3–20, 2017.

[119] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin. An empirical analysis of traceability in the Monero blockchain. *PoPETs*, 2018(3):143–163, 2018.

[120] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009.

[121] C. Natoli, J. Yu, V. Gramoli, and P. J. E. Veríssimo. Deconstructing blockchains: A comprehensive survey on consensus, membership and structure. *CoRR*, abs/1908.08316, 2019.

[122] S. Noether. Ring signature confidential transactions for monero. Cryptology ePrint Archive, Report 2015/1098, 2015. ia.cr/2015/1098.

[123] D. Papachristoudis, D. Hristu-Varsakelis, F. Baldimtsi, and G. Stephanides. Leakage-resilient lattice-based partially blind signatures. Cryptology ePrint Archive, Report 2019/1452, 2019. /eprint.iacr.org/2019/1452.

[124] J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In U. M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

[125] J. Patarin, N. T. Courtois, and L. Goubin. Quartz, 128-bit long digital signatures. In D. Naccache, editor, *Topics in Cryptology - CT-RSA 2001, The Cryptographer's Track at RSA 2001, Proceedings*, volume 2020 of *LNCS*, pages 282–297. Springer, 2001.

[126] T. P. Pedersen. A threshold cryptosystem without a trusted party. In D. W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 522–526, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[127] E. Pednault, J. Gunnels, D. Maslov, and J. Gambetta. On "quantum supremacy". https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/.

[128] C. Peikert. He gives c-sieves on the csidh. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 463–492, Cham, 2020. Springer International Publishing.

[129] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *TCC*, volume 3876 of *Lecture Notes in Computer Science*, pages 145–166. Springer, 2006.

[130] A. Petzoldt, S. Bulygin, and J. Buchmann. A multivariate based threshold ring signature scheme. *Appl. Algebra Eng. Commun. Comput.*, 24(3-4):255–275, 2013.

[131] A. Petzoldt, A. Szepieniec, and M. S. E. Mohamed. A practical multivariate blind signature scheme. In A. Kiayias, editor, *Financial Cryptography and Data Security - FC 2017, Revised Selected Papers*, volume 10322 of *LNCS*, pages 437–454. Springer, 2017.

[132] A. Poelstra. Adaptor signatures and atomic swaps from scriptless scripts. https://github.com/ElementsProject/scriptless-scripts/blob/master/md/atomic-swap.md.

[133] A. Poelstra. Scriptless scripts. Presentation Slides. https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2017-05-milan-meetup/slides.pdf.

[134] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93. ACM, 2005.

[135] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 552–565, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[136] D. Robert. Breaking sidh in polynomial time. Cryptology ePrint Archive, Paper 2022/1038, 2022. https://eprint.iacr.org/2022/1038.

[137] M. Rückert. Lattice-based blind signatures. In M. Abe, editor, *Advances in Cryptology - ASIACRYPT 2010, Proceedings*, volume 6477 of *LNCS*, pages 413–430. Springer, 2010.

[138] R. A. Sahu, A. Gini, and A. Pal. Supersingular isogeny-based designated verifier blind signature. Cryptology ePrint Archive, Report 2019/1498, 2019. https://eprint.iacr.org/2019/1498.

[139] K. Sakumoto, T. Shirai, and H. Hiwatari. Public-key identification schemes based on multivariate quadratic polynomials. In P. Rogaway, editor, *Advances in Cryptology - CRYPTO 2011, Proceedings*, volume 6841 of *LNCS*, pages 706–723. Springer, 2011.

[140] C. P. Schnorr. Efficient identification and signatures for smart cards. In G. Brassard, editor, *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 239–252, New York, NY, 1990. Springer New York.

[141] A. Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, Nov. 1979.

[142] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *FOCS 1994*, pages 124–134. IEEE Computer Society, 1994.

[143] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 617–635. Springer, 2009.

[144] J. Stern. A new identification scheme based on syndrome decoding. In D. R. Stinson, editor, *Advances in Cryptology - CRYPTO 1993, Proceedings*, volume 773 of *LNCS*, pages 13–21. Springer, 1993.

[145] E. Tairi, P. Moreno-Sanchez, and M. Maffei. Post-quantum adaptor signature for privacy-preserving off-chain payments. Cryptology ePrint Archive, Report 2020/1345, 2020. https://eprint.iacr.org/2020/1345.

[146] D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In *Advances in Cryptology - EUROCRYPT 2015*, pages 755–784, 04 2015.

[147] L. Valenta and B. Rowan. Blindcoin: Blinded, accountable mixes for bitcoin. In M. Brenner, N. Christin, B. Johnson, and K. Rohloff, editors, *Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers*, volume 8976 of *Lecture Notes in Computer Science*, pages 112–126. Springer, 2015.

[148] L. Valenta and B. Rowan. Blindcoin: Blinded, accountable mixes for bitcoin. In M. Brenner, N. Christin, B. Johnson, and K. Rohloff, editors, *Financial Cryptography and Data Security*, pages 112–126, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[149] N. van Saberhagen. Cryptonote v 1.0, 2012.

[150] M. Vukolic. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In J. Camenisch and D. Kesdogan, editors, *IFIPWG114*, volume 9591 of *LNCS*, pages 112–125. Springer, 2015.

[151] S. Wang, R. Ma, Y. Zhang, and X. Wang. Ring signature scheme based on multivariate public key cryptosystems. *Comput. Math. Appl.*, 62(10):3973–3979, 2011.

[152] A. N. S. X9.62-2005. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA). *ANSI X9*, page 163, 2005.

[153] X. Yi and K. Lam. A new blind ECDSA scheme for bitcoin transaction anonymity. In S. D. Galbraith, G. Russello, W. Susilo, D. Gollmann, E. Kirda, and Z. Liang, editors, *Proceedings of the 2019 ACM, AsiaCCS 2019*, pages 613–620. ACM, 2019.

[154] M. Yin, D. Malkhi, M. K. Reiter, G. Golan-Gueta, and I. Abraham. Hotstuff: BFT consensus with linearity and responsiveness. In *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing*, pages 347–356, 2019.

[155] Y. Yoo, R. Azarderakhsh, A. Jalali, D. Jao, and V. Soukharev. A post-quantum digital signature scheme based on supersingular isogenies. In A. Kiayias, editor, *Financial Cryptography and Data Security*, pages 163–181, Cham, 2017. Springer International Publishing.

[156] J. Yu, M. H. A. Au, and P. J. E. Veríssimo. Re-thinking untraceability in the cryptonote-style blockchain. In *CSF*, pages 94–107. IEEE, 2019.

[157] J. Yu, D. Kozhaya, J. Decouchant, and P. Esteves-Verissimo. Repucoin: Your reputation is your power. *IEEE Transactions on Computers (ToC)*, 2019.

[158] Z. Yu, M. H. Au, J. Yu, R. Yang, Q. Xu, and W. F. Lau. New empirical traceability analysis of cryptonote-style blockchains. In I. Goldberg and T. Moore, editors, *Financial Cryptography and Data Security - FC 2019, Revised Selected Papers*, volume 11598 of *Lecture Notes in Computer Science*, pages 133–149. Springer, 2019.

[159] T. H. Yuen, M. F. Esgin, J. K. Liu, M. H. Au, and Z. Ding. DualRing: Generic construction of ring signatures with efficient instantiations. In *CRYPTO (1)*, volume 12825 of *Lecture Notes in Computer Science*, pages 251–281. Springer, 2021.

[160] D. Zheng, X. Li, and K. Chen. Code-based ring signature scheme. *Int. J. Netw. Secur.*, 5(2):154–157, 2007.

[161] H. Zhu, Y. an Tan, X. Zhang, L. Zhu, C. Zhang, and J. Zheng. A round-optimal lattice-based blind signature scheme for cloud services. *Future Generation Computer Systems*, 73:106–114, 2017.