Supersingular Isogeny-Based Ring Signature*

Maryam Sheikhi Garjan[1], N. Gamze Orhon Kılıç[2], and Murat Cenk[2]

[1] IT University of Copenhagen, Copenhagen, Denmark
{mashe}@itu.dk
[2] Institute of Applied Mathematics,
Middle East Technical University, Ankara, Turkey
{gamze.kilic,mcenk}@metu.edu.tr

Abstract. A ring signature is a digital signature scheme that allows identifying a group of possible signers without revealing the identity of the actual signer. In this paper, we first present a post-quantum sigma protocol for a ring that relies on the supersingular isogeny-based interactive zero-knowledge identification scheme proposed by De Feo, Jao, and Plût in 2014. Then, we construct a ring signature from the proposed sigma protocol for a ring by applying the Fiat-Shamir transform. In order to reduce the size of exchanges, we use Merkle trees and show that the signature size increases logarithmically in the size of the ring. The security proofs and complexity analyses of the proposed protocols are also provided.

Keywords: Post-quantum cryptography · Supersingular isogeny · Ring signatures.

1 Introduction

Rivest, Shamir, and Kalai introduced the *ring signatures* at ASIACRYPT [24] in 2001. A ring signature is a digital signature scheme produced by a member of a *ring* (a group of people), which does not reveal the signer's identity. Ring signatures are very similar to group signatures. However, they differ from group signatures in some points, such that there are no group managers, coordination,

* This work was supported by TÜBİTAK under grant no 120E065. Maryam Sheikhi Garjan was a postdoctoral researcher at Middle East Technical University during a period of this research and would like to thank the Institute of Applied Mathematics Cryptography Department for the hospitality. N. Gamze Orhon Kilic was supported by the Council of Higher Education (YÖK) 100/2000 CoHE Ph.D. Scholarship and would like to thank the Council of Higher Education. A part of this paper was written while Murat Cenk was visiting the University of Waterloo and would like to thank the Department of Combinatorics & Optimization for the hospitality.

setup, and revocation procedures in ring signatures. A signer can select a set of potential signers, including herself, and sign a message with her secret key and other signers' public keys. This scenario does not require the approval of the other signers.

Besides *correctness*, two main features must be satisfied in terms of security by a ring signature: *unforgeability* and *anonymity*. A ring signature scheme is said to have unforgeability if that scheme does not allow anyone to generate a signature on behalf of an honest ring of signers without knowing the secret key of at least one member of the ring. For a given ring signature, anonymity is satisfied if no one can distinguish which member of the ring generated the signature, even with the information of all secret keys of the ring. Furthermore, there is no cooperation or group secret among the ring members in ring signature schemes. Therefore, choosing the ring members can be done in an ad-hoc way.

Whistleblowing was the original motivation of the ring signatures [24], where the leaking person's identity can be hidden by choosing a ring of people who have access to this specific leaked message while convincing the recipient about the authenticity of the leaked message. Recently, ring signatures have found many applications such as cryptocurrency technologies for secure and anonymous transactions and e-voting [20, 29]. For instance, in cryptocurrencies like *Monero*, known as a fungible currency, a user issues a ring signature on the transaction using a ring of public keys in the blockchain and generates a confidential transaction. A signer who generates a ring signature can hide her identity as an actual signer among the ring of public keys by ensuring that her identity is indistinguishable from other ring members' identities.

Since 2001, a huge number of ring signature schemes on various hardness assumptions such as the integer factorization [6, 11, 24], discrete logarithm [1, 15, 16, 20, 21]. and pairing-based [4, 23, 26, 29] have been proposed. The security of the pairing-based ring signatures could be proven without using a random oracle. Furthermore, efficient and short ring signatures that rely on pairing-based cryptography are introduced in [4, 7, 29]. In [1, 16], the signature size increases linearly in the size of the ring, and [23] gives a constant size ring signature, while the signature size in [2, 15] is logarithmic in the number of ring members. The ring signature sizes in [6, 11] based on RSA accumulators is independent of the ring size. Most recently, ring signatures that rely on the post-quantum assumptions like hash-based [10, 18] multivariate [12, 22] and (one-time) lattice-based [3, 5, 13, 19, 28] are introduced.

Recently, Beullens *et al.* presented linkable ring signature schemes in [5], based on logarithmic OR-proof with binary challenges for CSIDH group action and MLWE-based group action. The CSIDH group action is adapted from the Couveignes-Rostovtsev-Stolbunov scheme by substituting supersingular elliptic curves over $\mathbb{F}_p$ for ordinary elliptic curves to improve the efficiency of the scheme. The CSIDH group action is commutative since the subring of $\mathbb{F}_p$-rational endomorphisms is an order in an imaginary quadratic field. The security of the CSIDH-based linkable ring signature is based on the Group Action Inverse Problem (GAIP) and Squaring Decisional CSIDH (sdCSIDH) Problem.

The best-known quantum algorithm to solve GAIP and its variants has subexponential complexity. Nevertheless, there is no ring signature scheme based on supersingular isogenies to the best of our knowledge. The design of the SIDH scheme addressed the security weakness of the isogeny-based schemes by using supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. The endomorphism rings of these curves are non-commutative and therefore provide exponential security. It should be emphasized that SIDH is not similar to CSIDH in security, construction, key size, and performance. For comparison, SIDH has notable advantages over CSIDH by providing high security and computational efficiency.

In this paper, we present a post-quantum version of the sigma protocol for a ring that proves membership in the ring. In our sigma protocol, we apply the OR-proof with binary challenges for a group action proposed in [5] to the SIDH identification protocol given in [9], which does not follow the group action property. We give the proof of the correctness, *2-special soundness*, and *honest-verifier zero-knowledge (HVZK)* properties of the proposed protocol. Moreover, the fast-known quantum attacks against these assumptions are still exponential. Thus, we present a ring signature scheme based on the post-quantum assumptions, i.e., supersingular isogeny problems. The construction proposed in this paper provides a ring signature scheme, where the signature size grows logarithmically in the number of users in the ring. Also, we show that this scheme is correct, anonymous, and existentially unforgeable under an adaptive chosen message attack in the random oracle model.

The rest of the paper is organized as follows: In Section 2, we provide background information required for the proposed schemes in this study. In Section 3, we propose the supersingular isogeny-based sigma protocol, followed by supersingular isogeny-based ring signatures in Section 4. We present the efficiency analyzes in Section 5 and we conclude our paper in Section 6.

2 Background

This section briefly provides some required information related to the elliptic curve isogenies [8, 9, 27], computational problems of supersingular isogenies [9, 17, 25], ring signatures [2, 4, 20], and supersingular isogeny-based zero-knowledge proofs [14, 17, 31].

2.1 Elliptic Curve Isogenies

We consider the elliptic curves defined over a finite field $\mathbb{F}_q$ of characteristic $p > 3$. For an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{F}_q$, the j-invariant of E is denoted by

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

For a given $j \in \mathbb{F}_q$ with $j \neq 0$ and $j \neq 1728$, there is an elliptic curve,

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j},$$

whose j-invariant is j. Two elliptic curves E and E' are isomorphic over $\overline{\mathbb{F}}_q$ if only if they have the same j-invariant. Isomorphism maps between elliptic curves are invertible algebraic maps over algebraic closure $\overline{\mathbb{F}}_q$ and can be efficiently computed.

The n-torsion group of E, denoted by $E[n]$, contains the set of all points $P \in E(\overline{\mathbb{F}}_q)$ such that $nP = \mathcal{O}_E$, where $\mathcal{O}_E$ is the identity element. For n, with $p \nmid n$, we have $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

The elliptic curves defined over a field of characteristic p can be classified according to the structure of their p-torsion group. The elliptic curves with $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$ are called *ordinary* while the curves $E[p] \simeq \mathcal{O}$ are called *supersingular*.

An *isogeny* $\varphi : E \to E'$ is a non-constant morphism from E to E' that preserves the identity element. The *degree of an isogeny* is its degree as a morphism. If φ is separable, then $deg\varphi = \#ker(\varphi)$. The curves E and E' are *isogenous* if there is a separable isogeny between them. Due to Tate's theorem, E and E' are isogenous over $\mathbb{F}_q$ if and only if $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$. The isogeny φ can be explicitly obtained by using Vélu's formulae [30]. An isogeny of degree d is called a d-isogeny. Every isogeny of smooth degree $d > 1$ can be computed as a composition of isogenies of prime degree $d = \prod_{i=1}^{m} \ell_i^{e_i}$ over $\overline{\mathbb{F}}_q$.

An isogeny is a group homomorphism and can be uniquely identified with its kernel (up to isomorphism). Given $G \subseteq E$, there exists a unique curve E_G (up to isomorphism) and a unique separable isogeny (up to automorphism of E) $\varphi_G : E \to E_G \cong E/G$ such that $ker(\varphi_G) = G$. For a given prime ℓ, there exists exactly $\ell + 1$ cyclic subgroups of order ℓ that each defines different ℓ-isogenies. $\Phi_\ell(x, y) \in \mathbb{Z}[x, y]$ is a symmetric modular polynomial of degree $\ell + 1$ in both x and y, and $\Phi_\ell(j_1, j_2) = 0$ if and only if there is an ℓ-isogeny between two elliptic curves with j-invariants j_1 and j_2. Moreover, for a given j, the roots of the univariate equation $\Phi_\ell(x, j) = 0$ are the j-invariants of curves which are ℓ-isogenous to j. For each ℓ-isogeny $\varphi : E \to E'$, there exists a unique *dual* ℓ-isogeny $\widehat{\varphi} : E' \to E$ such that $\widehat{\varphi} o \varphi = [\ell]$ gives the multiplication-by-ℓ map on E and $\varphi o \widehat{\varphi} = [\ell]$ gives the multiplication-by-ℓ map on E'.

An *endomorphism* is an isogeny from E to itself. The set of all endomorphisms of the elliptic curve E, including the zero map, is denoted by $End(E)$. Moreover, it has a ring structure under point-wise addition and composition operations. The $End(E)$ over the algebraic closure field is isomorphic with an order in a quadratic imaginary field or a maximal order in a quaternion algebra. An elliptic curve whose $End(E)$ is an order in a quadratic imaginary field is called *ordinary*. The curve with $End(E)$ as a maximal order in a quaternion algebra is called the *supersingular* elliptic curve. Up to isomorphism, all supersingular elliptic curves over the finite field $\mathbb{F}_q$ of characteristic p can also be defined over $\mathbb{F}_{p^2}$. Indeed, the motivation for using the supersingular isogenies in cryptography is based on the hardness of computing the endomorphism of a randomly chosen supersingular elliptic curve. The best quantum algorithm to solve this problem has $O(p^{1/4})$ running time with only a quadratic improvement over classical algorithms.

2.2 Computational Problems of Supersingular Isogenies

The security of supersingular isogeny-based crypto-systems is based on the following computational problems:

Endomorphism Ring Problem. Let p be a prime number, and E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$, chosen uniformly at random. Computing the endomorphism ring of E is called the endomorphism ring problem.

Let $p = \ell_1^{e_1}\ell_2^{e_2}f \pm 1$ be a prime number where $\ell_1 \neq \ell_2$ are small primes and f is an integer cofactor. Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Fix $\{P_1, Q_1\}$ and $\{P_2, Q_2\}$ as bases of torsion groups $E[\ell_1^{e_1}]$ and $E[\ell_2^{e_2}]$, respectively. We state the following problems that form security assumptions of the supersingular isogeny-based protocols in [9, 17].

Computational Supersingular Isogeny (CSSI) Problem. Let m_1 and m_2 are randomly chosen integers modulo $\ell_1^{e_1}$ such that not both divisible by ℓ_1, and $\varphi : E \to E'$ be an $\ell_1^{e_1}$-isogeny whose kernel generated by $R = [m_1]P_1 + [m_2]Q_1$. For given $\{E', \varphi(P_2), \varphi(Q_2)\}$, CSSI problem is to compute a generator of the kernel φ.

Supersingular Computational Diffie-Hellman (SSCDH) Problem. Let $\varphi : E \to E'$ and $\psi : E \to E''$ be secret isogenies whose kernels are generated by random points $R \in \langle P_1, Q_1\rangle$ and $S \in \langle P_2, Q_2\rangle$, respectively. SSCDH problem is finding the j-invariant of $E/\langle R, S\rangle$ for given $\{E', E'', \varphi(P_2), \varphi(Q_2)\}, \{\psi(P_1), \psi(Q_1)\}$.

Supersingular Decision Diffie-Hellman (SSDDH) Problem. Let $\varphi : E \to E'$ and $\psi : E \to E''$ be isogenies whose kernels are generated by random points $R \in E[\ell_1^{e_1}] = \langle P_1, Q_1\rangle$ and $S \in E[\ell_2^{e_2}] = \langle P_2, Q_2\rangle$, respectively. One of the following tuples is sampled with probability 1/2:

- $(E', E'', \{\varphi(P_2), \varphi(Q_2)\}, \{\psi(P_1), \psi(Q_1)\}, E/\langle R, S\rangle)$,
- $(E', E'', \{\varphi(P_2), \varphi(Q_2)\}, \{\psi(P_1), \psi(Q_1)\}, E/\langle T\rangle)$ where $T \in E[\ell_1^{e_1}\ell_2^{e_2}]$ and is randomly chosen.

The SSDDH problem is to determine from which distribution this tuple is sampled.

Decisional Supersingular Product (DSSP) Problem. Let $\varphi : E \to E'$ be an isogeny whose kernel is generated by a secret point $R \in E[\ell_1^{e_1}] = \langle P_1, Q_1\rangle$. Suppose that $E[\ell_2^{e_2}] = \langle P_2, Q_2\rangle$ and $(E, E', P_2, Q_2, \varphi(P_2), \varphi(Q_2))$ are given. Consider the following distributions of (E, E'):

- (E_1, E_1'), where $E_1 = E/\langle S\rangle$ generated by $S \in E[\ell_2^{e_2}]$ and $E_1' = E'/\langle\varphi(S)\rangle$.

– (E_1, E_1'), where E_1 is a random curve and isogenous to E, and E_1' is generated by a random point $R' \in E_1[\ell_1^{e_1}]$.

DSSP problem is to determine from which distribution the tuple (E_1, E_1') is sampled.

2.3 Ring Signatures

A ring signature scheme for given public parameters $pp(\lambda)$ consists of a triple of *PPT (probabilistic polynomial-time)* algorithms $(\mathsf{Kgen}, \mathsf{Sig}, \mathsf{Ver})$, for generating keys, signing a message, and verifying the ring signature respectively.

– $(pk, sk) \leftarrow \mathsf{Kgen}(pp(\lambda), rand)$: Outputs public and secret keys for a given security parameter (1^λ) and a random number $rand$.
– $\sigma \leftarrow \mathsf{Sig}(sk_r, R, pp, m)$: Let R be a ring containing n signers. Sig takes a message m, a secret key sk_r where $1 \leq r \leq n$ and a set of public keys $R = \{pk_1, \ldots, pk_n\}$ such that $pk_r \in R$, and outputs a signature σ on message m with respect with the ring R.
– $1/0 \leftarrow \mathsf{Ver}(\sigma, R, pp, m)$: Takes a signature σ, message m, and a ring $R = \{pk_1, \ldots, pk_n\}$ as input, outputs 1 for accepting and 0 for rejecting.

A ring signature scheme is required to comply with the properties: correctness, anonymity, and unforgeability.

A ring signature σ is said to satisfy the correctness condition if for every public information $pp(\lambda)$, $n = \mathsf{poly}(\lambda)$, message m, $R \subseteq \{pk_1, pk_2, \ldots, pk_n\}$ where $\mathsf{Kgen}(pp(\lambda), rand_i) = (pk_i, sk_i)$ for every $i \in \{1, 2, \ldots, n\}$, the signature $\sigma = \mathsf{Sig}(sk_r, R, pp, m)$ for $pk_r \in R$, $1 \leq r \leq n$ always holds $Pr[\mathsf{Ver}(\sigma, R, pp, m) = 1] = 1$.

A ring signature σ is called anonymous if for every public parameter $pp(\lambda)$, message m and $n = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has at most negligible advantage in the following game against a challenger: The challenger runs the $\mathsf{Kgen}(pp(\lambda), rand_i) = (pk_i, sk_i)$ for every $i \in \{1, 2, \ldots, n\}$ using random coins $rand_i$, and samples a random bit $b \in \{0, 1\}$. The challenger also provides pp and a set of random coins $\{rand_1, \ldots, rand_n\}$ to $\mathcal{A}$. $\mathcal{A}$, using these random coins, has all the secret keys in the ring. The adversary $\mathcal{A}$ gives a challenge (pk_i, R, m) where $pk_{i_0}, pk_{i_1} \in R$ and $pk_i = pk_{i_0}$ or $pk_i = pk_{i_1}$. The challenger then runs the signing algorithm $\mathsf{Sig}(sk_{i_b}, R, pp, m)$ and outputs σ^* to $\mathcal{A}$. $\mathcal{A}$ wins the game if the $\mathcal{A}$'s guess b^* equals b.

A ring signature σ is called unforgeable under insider corruption if for every public parameter $pp(\lambda)$ and $n = \mathsf{poly}(\lambda)$, any PPT adversary $\mathcal{A}$ has at most a negligible advantage in the following game against a challenger: The challenger runs the $\mathsf{Kgen}(pp(\lambda), rand_i) = (pk_i, sk_i)$ for every $i \in \{1, 2, \ldots, n\}$ using random coins $rand_i$, and gives pp and $pk = \{pk_1, pk_2, \ldots, pk_n\}$ to $\mathcal{A}$. $\mathcal{A}$ can generate signatures for a polynomial number of times. The corruption queries as follows:

– $\mathsf{Squeri}(i, R, m)$: the challenger verifies that $pk_i \in R$ then gives σ corresponding with (sk_i, R, m) to $\mathcal{A}$.

– $\mathsf{Cqueri}(i)$: the challenger gives its corresponding random coin $rand_i$ that generates (pk_i, sk_i) when $\mathcal{A}$ reruns the $\mathsf{Kgen}(pp(\lambda), rand_i)$.

$\mathcal{A}$ outputs (σ^*, R^*, m^*) where $R^* \subseteq pk$ and each $pk_i \in R^*$ has never requested as a corruption query, and $(., R^*, m^*)$ has not been in signing query list. $\mathcal{A}$ wins the game if $\mathsf{Ver}(\sigma^*, R^*, m^*) = 1$. The advantage of $\mathcal{A}$ in the unforgeability game is denoted as $\xi = Pr[\mathcal{A}\ wins]$.

2.4 Supersingular Isogeny-Based Zero-Knowledge Proof

A supersingular isogeny-based zero-knowledge proof of identity is presented in [17]. In this protocol, Peggy (prover) wants to prove to Victor (verifier) that she knows the secret kernel $\langle S \rangle$ of the isogeny $\varphi : E \to E_S$ without revealing it. This protocol is computationally zero-knowledge and works as follows: Let $\ell_p = \ell_1^{e_1}$, $\ell_v = \ell_2^{e_2}$, f be a small integer, p be a prime such that $p = \ell_p \ell_v f \pm 1$, $\{p, E, E_S, E[\ell_v] = \langle P, Q \rangle, \varphi(P), \varphi(Q)\}$ be publicly known, and $S \in E[\ell_p]$ be the secret information. Peggy selects a random cyclic subgroup $V \in E[\ell_v]$, computes isogenies $\psi : E \to E_V$ and $\psi' : E_S \to E_{SV}$, whose kernels are generated by V and $\varphi(V)$, respectively. Peggy then publishes E_V and E_{SV} as commitment. Victor chooses a random challenge $b \in \{0, 1\}$ and sends it to Peggy. Peggy responds with $\{V, \varphi(V)\}$ upon receiving the challenge $b = 0$, or responds with $\psi(S)$ for challenge $b = 1$. Victor accepts if the response generates the isogenies that connect the corresponding curves. For λ-bit security, this interactive process should be run λ times, and Peggy successfully proves her knowledge of the secret kernel S if the verifier accepts the responses of all λ times of interaction. An interactive zero-knowledge proof protocol can be transformed into a non-interactive signature scheme as given in [14, 31].

3 Supersingular Isogeny-Based Sigma Protocol for a Ring

In this section, we propose a supersingular isogeny-based sigma protocol for a ring that forms the basis of the supersingular isogeny-based ring signature scheme given in Section 4. The proposed sigma protocol is derived from the interactive zero-knowledge proof of identity proposed by De Feo, Jao, and Plût [9]. This section presents the proposed sigma protocol in detail, proves its security, and provides a Merkle tree application.

3.1 Sigma Protocol for a Ring

Let R be a ring chosen by Peggy with n members and r be an integer with $1 \leq r \leq n$. Peggy wants to convince Victor that she knows a secret key $\langle S_r \rangle$ that generates one of the public keys (i.e., E_{S_r}) in R, without revealing the secret key and the certain public key in the ring R. A supersingular isogeny-based interactive zero-knowledge proof takes over R as follows:

1. For a security parameter λ, let the public parameters be a prime number $p = \ell_p \ell_v f \pm 1$ where $\ell_p \approx \ell_v$ are smooth numbers, a supersingular elliptic curve $E(\mathbb{F}_{p^2})$, two points P and Q that are the generators of the ℓ_v-torsion group $E[\ell_v]$.
2. Every user in the system has public and secret keys for given security parameter λ. For the i^{th} user, S_i is the secret key and (E_{S_i}, P_i, Q_i) is the public key where $S_i \in E[\ell_p]$, generating the kernel of a secret ℓ_p-isogeny $\alpha_i : E \to E_{S_i}$, and $P_i = \alpha_i(P)$, $Q_i = \alpha_i(Q)$ as the images of ℓ_v-torsion generators $\langle P, Q\rangle$.
3. Peggy picks a ring $R = \{(E_{S_i}, P_i, Q_i)\}_{i=1}^{n}$ of n public keys where the index of her public key in R is r. She chooses a random integer $\omega \in \mathbb{Z}/\ell_v\mathbb{Z}$, then computes $V = P + \omega Q \in E[\ell_v]$ and $\alpha_i(V) = P_i + \omega Q_i$ defining the kernels of the isogenies given in Fig. 1. In this scheme, $\beta : E \to E/\langle V\rangle = E_V$ and $\beta_i : E_{S_i} \to E_{S_i}/\langle \alpha_i(V)\rangle = E_{S_iV}$ are ℓ_v-isogenies defined by V and $\alpha_i(V)$, respectively. Peggy applies a random permutation τ on $\big[j(E_V), j(E_{S_1V}), \ldots, j(E_{S_nV})\big]$ and obtains $X = [j_{i_1}, j_{i_2}, \ldots, j_{i_{n+1}}]$ then sends the commitment X to Victor.

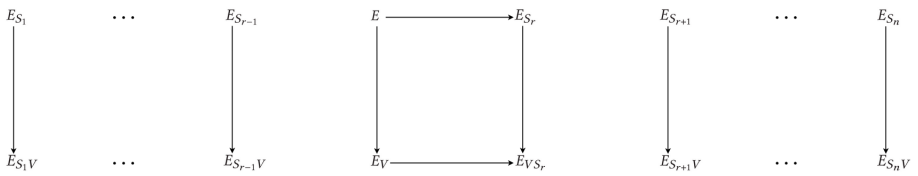

Fig. 1. Supersingular isogeny-based sigma protocol commitment isogenies.

4. Victor sends a challenge $ch \in \{0, 1\}$ to Peggy.
5. Peggy reveals the response $resp$, based on the challenge. If $ch = 1$ then, $resp = (\omega, \tau)$. If $ch = 0$ then $resp = (j(E_V), \beta(S_r))$ where $\langle \beta(S_r)\rangle$ is the kernel of the isogeny $\alpha'_r : E_V \to E_V/\langle \beta(S_r)\rangle = E_{VS_r}$.
6. If $ch = 1$ and $resp = (\omega, \tau)$, Victor verifies whether ω generates the elliptic curve points of order ℓ_v that define the kernels of the isogenies (shown in Fig. 2) $E \to E_{V'}$, and $E_{S_i} \to E_{S_iV'}$, for $1 \le i \le n$, respectively. Victor sets $X' = \big[j(E_{V'}), j(E_{S_1V'}), \ldots, j(E_{S_nV'})\big]$ and applies τ on X'. He accepts if $X' = X$, otherwise rejects. If $ch = 0$, Victor checks whether $\beta(S_r)$ has order ℓ_p and generates the isogeny illustrated in Fig. 3, $E_V \to E_V/\langle \beta(S_r)\rangle = E_{VS'_r}$ and then accepts if $j(E_V), j(E_{VS'_r}) \in X$. He rejects otherwise. Note that $E_{S_rV} \simeq E/\langle S_r, V\rangle \simeq E/\langle S_r\rangle/\langle \alpha_r(V)\rangle \simeq E/\langle V\rangle/\langle \beta(S_r)\rangle$.

The sigma protocol does not leak any information about (E_{S_r}, r). The prover uses a permutation map, which hides the index of the elements in the commitment. Moreover, when the verifier sends $ch = 1$, the prover's response allows the verifier to compute all the commitments, and therefore, there is no leak of anonymity. When the verifier sends the challenge $ch = 0$, the prover's answer is

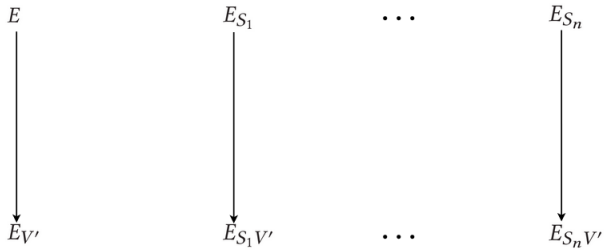

Fig. 2. Supersingular isogeny-based sigma protocol verification isogenies for $ch = 1$.

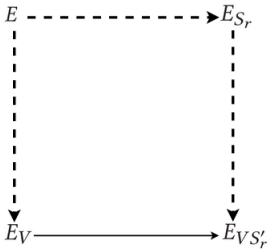

Fig. 3. Supersingular isogeny-based sigma protocol verification isogeny for $ch = 0$.

an isogeny between two arbitrary curves (E_V, E_{S_iV}) in the commitment. Since the verifier does not know the isogeny that connects these two curves to public curves in the ring, the response of this challenge is independent of the knowledge of (E_{S_r}, r).

Theorem 1. *The supersingular isogeny-based sigma protocol for a ring is complete, honest-verifier zero-knowledge (HVZK), and it satisfies 2-special soundness if the supersingular isogeny problems — DSSP and CSSI problems — are computationally hard.*

Proof. It is trivial to check the completeness. We shall prove that the scheme is HVZK, which means that one can simulate a real execution of the identification protocol for a given public key and a challenge without the knowledge of the secret key. To see this, consider the algorithm $\mathsf{Sim}(R, ch) \rightarrow (com, ch, resp)$. For a given R and a challenge ch, Sim works as follows: If $ch = 1$, choose a random integer $\omega' \in \mathbb{Z}/\ell_v\mathbb{Z}$ and compute the corresponding isogeny maps of degree ℓ_v with the public keys in R. X' stores the j-invariants of the image curves. Sim outputs the transcript $(com, ch, resp) = (X', 1, (\omega', \tau'))$. In this case, the output transcript is simulated correctly. If $ch = 0$, choose a curve E' (isogenous to E) and a random point $S' \in E'[\ell_p]$ where $E'' = E'/\langle S' \rangle$. X' holds the j-invariants of E', E'', and $n - 1$ randomly chosen curves isogenous to E. Sim outputs the transcript $(com, ch, resp) = (X', 0, (E', S'))$, however, in this case, X' is not distributed as a real execution. The computational assumption of

DSSP implies that it is computationally hard to distinguish whether a transcript is simulated or is a transcript of a real execution. Therefore the scheme has computational zero-knowledge. 2-Special soundness follows from the following observation: For given two valid transcripts $(com, ch, resp) = (X, 1, (\omega, \tau))$ and $(com, ch', resp') = (X, 0, (E', S'))$ with respect to R, it is possible to extract the secret key. Let $\beta : E \to E' = E/\langle V \rangle$ be the isogeny generated by the kernel $V = P + \omega Q$ and $\alpha' : E' \to E'' = E'/\langle S' \rangle$ be the isogeny generated by S'. With the knowledge of these two transcripts, one can compute $\hat{\beta}(S')$ that generates a secret kernel for one of the curves in the ring. Suppose that $\mathcal{A}$ is an adversary that can correctly respond both $ch = 0$ and $ch = 1$ corresponding with X, then $\mathcal{A}$ can solve an instance of CSSI problem.

Assume that Peggy does not know any S_i that generates one of the public keys in R and tries to cheat Victor that she is a member of R. She can select a random number $\omega \in \mathbb{Z}/\ell_v\mathbb{Z}$ and obtains a commitment X, only with the knowledge of public parameters. In this scenario, if Victor sends $ch = 1$, then Peggy can send a valid response, but if Victor sends $ch = 0$ since she does not know any of the secret keys, she cannot compute a valid kernel $\langle S_i \rangle$ that generates one of the curves in commitment X. Conversely, Peggy can choose a random number $\omega \in \mathbb{Z}/\ell_v\mathbb{Z}$, compute $V = P + \omega Q$ and E_V. Then, she selects random points on E_V to generate a commitment X. If Victor sends $ch = 0$, Peggy's response $j(E_V), \beta(S_i)$ will convince Victor since X includes $E_V/\langle \beta(S_i) \rangle$. If Victor sends $ch = 1$, then Peggy has to send ω, which generates the kernels of the curves in X; however, the commitment does not include the curves generated by the public keys in R. Therefore, Victor does not accept Peggy's response. For both of these scenarios, Peggy can cheat with the probability of $1/2$. So, the sigma protocol should be repeated until Victor is convinced that Peggy is honest.

3.2 Reducing the Size of Commitment Using Merkle Tree

The size of the commitment in Section 3.1 is large. To reduce the size of the commitment, we apply the Merkle tree to the commitment set X in each iteration of the sigma protocol for R. We set a Merkle tree on commitment $X = [j_{i_1}, j_{i_2}, \ldots, j_{i_{n+1}}]$ whose leaf nodes are $\left[H(j_{i_1}), H(j_{i_2}), \ldots, H(j_{i_{n+1}})\right]$ where H is a hash function. Internal nodes further up in the tree are hash values of a concatenation of two hashes (their two children). The root of the Merkle tree (the top hash) contains the hash of the entire tree. In order to prove that $H(j_i)$ is a leaf node of the Merkle tree for a given $Root(X)$, an ordered path that contains the sibling node of $H(j_i)$ and other internal nodes are needed. This path has a logarithmic size in the number of leaf nodes.

As an example, Fig. 4 illustrates the construction of a Merkle tree where $X = [j_{i_1}, j_{i_2}, \ldots, j_{i_8}]$ is the permuted j-invariants of the curves $E_V, E_{S_1V}, \ldots, E_{S_7V}$. One can obtain the path of a single node by following the shortest path from the root node to the specific node. For instance, $Path(j_{i_6}) = (H_5, H_{78}, H_{1234})$.

We slightly modify the sigma protocol for R so that the prover only reveals a Merkle tree root of X as a commitment. The changes in each step of the sigma

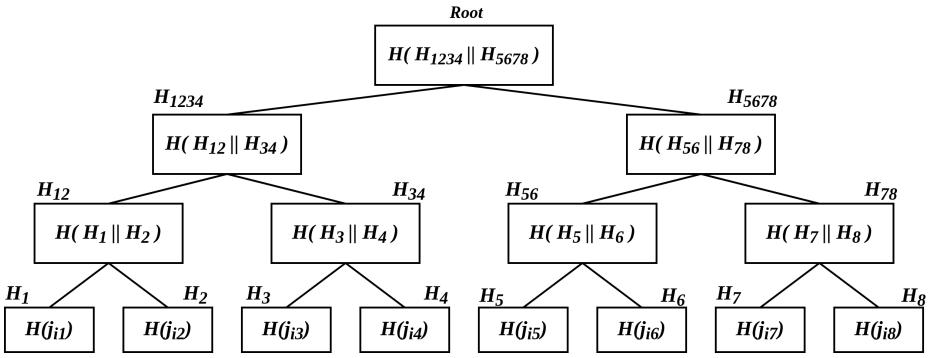

Fig. 4. A Merkle tree constructed for 8 j-invariants.

protocol are as follows: Peggy applies the step 3 of sigma protocol given in Section 3.1, and computes a Merkle tree root of $X = [j_{i_1}, j_{i_2}, \ldots, j_{i_{n+1}}]$. Then, sends $Root(X)$ to Victor. Victor sends a challengel $ch \in \{0, 1\}$ to Peggy. If $ch = 1$, Peggy reveals the response $resp = (\omega, \tau)$. Victor reconstructs the Merkle tree root $X' = \left[j(E_{V'}), j(E_{S_1V'}), \ldots, j(E_{S_nV'})\right]$ generated by ω, then applies τ on X'. He accepts if $Root(X') = Root(X)$. If $ch = 0$, the response is modified as $resp = (j(E_V), \beta(S_r), Path(j(E_{S_rV})))$. Victor first computes $E_{VS'_r}$ from the knowledge $(j(E_V), \beta(S_r))$. Then, by using the given $Path(j(E_{S_rV}))$, the leaf node $H(j(E_{VS'_r}))$ recovers $Root(X')$. Victor accepts it if $Root(X') = Root(X)$.

4 Supersingular Isogeny-Based Ring Signature

In this section, we describe a supersingular isogeny-based ring signature which is obtained by applying Fiat-Shamir transform to the sigma protocol given in Section 3.1.

Let $p = \ell_p \ell_v f \pm 1$ be a prime number for a given security parameter λ, E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$, and H be a hash function with output size $q = O(\lambda)$. The points P and Q are on the curve $E(\mathbb{F}_{p^2})$ such that $E[\ell_v] = \langle P, Q \rangle$. The set of public parameters is $pp = \{p, E, P, Q, H\}$. Supersingular isogeny-based ring signature works as follows:

- $\mathsf{Kgen}(pp)$: For the i^{th} user, the point $S_i \in E[\ell_p]$ which generates the kernel of the secret isogeny $\alpha_i : E \to E_{S_i}$ is the secret key, (E_{S_i}, P_i, Q_i) is the public key where $(P_i, Q_i) = (\alpha_i(P), \alpha_i(Q))$. So, secret and public keys of i^{th} user is $(sk_i, pk_i) = (S_i, (E_{S_i}, P_i, Q_i))$.
- $\mathsf{Sig}(sk, pk, pp, m)$: Let Peggy choose a ring $R = \{(E_{S_i}, P_i, Q_i)\}_{i=1}^n$ with n users. Consider r as Peggy's public key index in R. Peggy generates the ring signature by running the sigma protocol for a ring q times. The k^{th} iteration of the protocol is as follows:
  - Select a random integer $\omega_k \in \mathbb{Z}/\ell_v\mathbb{Z}$, compute $V_k = P + \omega_k Q$ and the corresponding ℓ_v-isogeny $\beta_k : E \to E_{V_k}$.

- By using the public keys $pk_i = (E_{S_i}, P_i, Q_i)$ in R, compute the isogenies $\beta_{k1}, \beta_{k2}, \ldots, \beta_{kn}$ where $\beta_{ki} : E_{S_i} \to E_{S_i V_k}$, generated by $\alpha_i(V_k) = P_i + \omega_k Q_i$ of degree ℓ_v, for $i = 1, 2, \ldots, n$.
- Compute $X_k = \big[j(E_{V_k}), j(E_{S_1 V_k}), j(E_{S_2 V_k}), \ldots, j(E_{S_n V_k})\big]$, apply the permutation τ_k, and set $\sigma_k = Root(X_k)$.

After collecting all σ_k values for $k = 1, \ldots, q$, Peggy computes $h = H(m, \sigma_1, \sigma_2, \ldots, \sigma_q)$ where $m \in \{0,1\}^*$ is the message and $h \in \{0,1\}^q$ is the output of H which holds the challenges of the ring signature. Let z be the verification key and z_k be the k^{th} element of z, for $k = 1, \ldots, q$. If $h_k = 1$, Peggy sets $z_k = (\omega_k, \tau_k)$, otherwise $z_k = (j(E_{V_k}), \beta_k(S_r), Path(j(E_{S_r V_k})))$. The signature is $\sigma = (z, R)$.

– $\mathsf{Ver}(\sigma, pp, m)$: Victor can recover each σ_k by using the information given by z_k, for $1 \le k \le q$. First, he extracts the bits of $h = H(m, \sigma_1, \sigma_2, \ldots, \sigma_q)$ according to the size of z_k, since the size of z_k differs for $ch = 1$ and $ch = 0$. If Victor obtains $z_k = (\omega_k, \tau_k)$ and so $hk = 1$, he computes $V'_k = P + \omega_k Q$, $V'_{ki} = P_i + \omega_k Q_i$ and the isogenies $\beta_k : E \to E_{V'_k}$, $\beta_{ki} : E \to E_{S_i V'_k}$ with the kernels $\langle V'_k \rangle$ and $\langle V'_{ki} \rangle$. Finally, he sets $X'_k = \big[j(E_{V'_k}), j(E_{S_1 V'_k}), j(E_{S_2 V'_k}), \ldots, j(E_{S_n V'_k})\big]$, applies τ_k, and finds $\sigma'_k = Root(X'_k)$. In the case $h_k = 0$, z_k contains a kernel $\beta_k(S_r)$ of an ℓ_p-isogeny and $j(E_{V_k})$, so Victor can compute $E_{V_k} \to E_{V_k S'_r} = E_{V_k}/\langle \beta_k(S_r) \rangle$. $Path(j(E_{S_r V_k}))$ is also included in z_k, thus Victor obtains the root of the corresponding Merkle tree (which also equals to σ'_k) using $j(E_{V_k S'_r})$ and $Path(j(E_{S_r V_k}))$. After collecting each σ'_k, he computes $h' = H(m, \sigma'_1, \sigma'_2, \ldots, \sigma'_q)$ then, compares h and h'. Victor accepts if $h = h'$.

Theorem 2. *The supersingular isogeny-based ring signature is correct, anonymous, and existentially unforgeable under an adaptive chosen message attack in the random oracle model if the problems CSSI and DSSP are computationally hard, and the sigma-protocol for a ring given in Section 3 is correct, 2-special sound, and honest-verifier zero-knowledge.*

Proof. The correctness of the ring signature produced by a signer who knows a secret key in the ring follows from the correctness of the sigma protocol for a ring since we run it in q parallel times, and the commitments are reconstructed from the verification keys of the signature. We prove the anonymity by showing that there exists a simulator Sim that outputs signatures indistinguishable from signatures generated by a signer. Let the adversary challenge be (m, R, S_0, S_1) where the ring R contains two public keys corresponding with the secret keys S_0 and S_1. Using the zero-knowledge simulator Sim, the challenger simulates a signature in the random oracle (where the output challenges are well adjusted with the responses given by Sim) without the knowledge of secret keys S_0 and S_1. Hence, the zero-knowledge property of the ring signature is independent of the knowledge of the secret keys, which preserves the anonymity of the proposed scheme even against the full key exposure. The unforgeability of the supersingular isogeny-based ring signature is shown with the assumption that the adversary $\mathcal{A}$ succeeds in generating a forgery with advantage ξ. Let $\mathcal{B}$ be an algorithm that

runs $\mathcal{A}$ for given public keys and public parameters. $\mathcal{B}$ uses the Sim to generate the queried signatures as in the anonymity case. If $\mathcal{A}$ outputs a forged signature (σ^*, R^*, m^*) where $(., R^*, m^*)$ have never been queried before. $\mathcal{B}$ rewinds $\mathcal{A}$ and reruns it by refreshing the randomness of random oracle to obtain another proof for a particular query of the random oracle that before was made by (σ^*, R^*, m^*). In this case, if $\mathcal{A}$ succeeds, then $\mathcal{B}$ either will find a collision or two transcripts $(com, ch, resp)$ and $(com, ch', resp')$, which results in a secret key in the ring R.

5 Efficiency

This section provides efficiency analyses of the schemes introduced in Section 3 and 4. Note that the method given in *Lemma 2.* of [14] is used for the efficiency analyses.

The best known classical and quantum attacks of supersingular isogeny assumptions of smooth degree $\ell_p \approx \ell_v$ have roughly $O(\sqrt{\ell_p})$ and $O(\sqrt[3]{\ell_p})$ heuristic running times, respectively. Thus, for a given security parameter λ, we have $\log \ell_p = 2\lambda$ for the classical security and $\log \ell_p = 3\lambda$ for the quantum security.

We assume that H is a secure hash function with the output $\{0,1\}^q$ where $q = O(\lambda)$ and the ring R consists of n public keys. Each $pk_i = (j(E_i), x(P_i), x(Q_i)) \in R$ is the public key of a ring member where $j(E_i), x(P_i), x(Q_i) \in \mathbb{F}_{p^2}$. The secret key of the i^{th} user is an ℓ_p-torsion point. Assume that $\langle P_S, Q_S \rangle = E[\ell_p]$, $sk_i \in \mathbb{Z}/\ell_p\mathbb{Z}$ and sk_i is relatively prime to the smooth base (i.e., if $\ell_p = 2^a$ then $gcd(sk_i, 2) = 1$), then the secret key of the i^{th} user is defined as $S_i = P_S + sk_i Q_S$. Therefore, it is enough to represent the secret key with the integer sk_i.

We present the efficiency analysis of the supersingular isogeny-based sigma protocol for a ring. R consists of n public keys $pk_i = (j(E_i), x(P_i), x(Q_i))$, where one of these public keys corresponds with the prover's secret key sk_r. The size of the ring is $|R| = 6n \log p$, where the size of a public key is $|pk_i| = 6 \log p$ since $j(E_i), x(P_i), x(Q_i) \in \mathbb{F}_{p^2}$, the secret key size is $|sk| = \frac{1}{2} \log p$, providing that the generators of the torsion group $E[\ell_p]$ are given as public information. The prover sends a commitment $com = [j_{i_1}, j_{i_2}, \ldots, j_{i_{n+1}}]$ consists of j-invariants of $n+1$ curves that are computed using the ℓ_v-isogeny maps from E and the curves in R. In this case, the size of the commitment is $|com| = 2(n+1) \log p$ where $j_i \in \mathbb{F}_{p^2}$. By applying the Merkle tree, the size of the commitment can be decreased to a Merkle tree hash root of size q. The prover's response is either $resp = (\omega, \tau)$ or $resp = (j(E_V), x(\beta(S_r)))$ based on challenge $ch = 1$ and $ch = 0$, respectively. On average, the size of the response $|resp| = \frac{1}{2}(\frac{1}{2} \log p + \log \tau + [2 \log p + \frac{1}{2} \log p])$ where $|\omega| = \frac{1}{2} \log p$, $|\tau| = \log \tau$, $|x(\beta(S_r))| = \frac{1}{2} \log p$, and $|j(E_V)| = 2 \log p$. By applying the Merkle tree, the size of the prover's response can be changed to $|resp| = 3 \log p + q \log n + \log \tau$ where $q \log n$ is the Merkle tree path size from a leaf node to root. The computation of the supersingular isogeny map is the main operation in the proposed sigma protocol. In the commitment phase, the prover computes $n+1$ isogenies to generate the commitment. In the verification phase, the verifier computes $n+1$ isogenies if $ch = 1$ and one isogeny if $ch = 0$.

Efficiency analysis of the supersingular isogeny-based ring signature can be explained as follows: A public key $(j(E_i), x(P_i), x(Q_i)) \in R$ where $j(E_i), x(P_i), x(Q_i) \in \mathbb{F}_{p^2}$ requires $|pk_i| = 6\log p$ bits. The secret key requires $|sk| = \frac{1}{2}\log p$ bits. The signature $\sigma = (z, R)$ contains the ring R of n public keys and $|R| = 6n\log p$. A hash function H with output h of size q bits where the number of $h_k = 0$ and $h_k = 1$ of the output are roughly equal. So, the size of z is calculated as follows: In the case that $h_k = 1$, $|z_k| = \frac{1}{2}\log p + \log \tau$ and in the case that $h_k = 0$, $|z_k| = \frac{5}{2}\log p + q\log n$, where $|j(E_{V_k})| + |x(\beta_k(S_r))| = \frac{5}{2}\log p$ and $|Path(j(E_{S_r V_k}))| = q\log n$. Consequently, $|z| = \frac{q}{2}\big(\frac{1}{2}\log p + \log\tau + \big(\frac{5}{2}\log p + q\log n\big)\big)$. When we put them all together, we come up with the size of the signature on average: $|\sigma| = 6n\log p + \frac{q}{2}\big[3\log p + q\log n + \log\tau\big]$. In the proposed ring signature, the signer computes $q(n+1)$ isogenies to generate the signature, and the verifier computes $\frac{q}{2}(n+1)$ isogenies on average to verify the signature.

If we have an ordered set of public keys, instead of including a ring of public keys as a part of the signature, which increases the total size of signature $6n\log p$, the signer can provide seed and an integer as part of the signature. The seed generates n random integers. The signer then finds an integer such that the addition of the random numbers and integer modulo n will generate the indices of n public keys, including the signer public key from the ordered public key list. This optimization saves approximately $6n\log p$ bits in the signature size.

6 Conclusion

In this paper, we have presented a post-quantum sigma protocol for a ring based on supersingular isogenies. We have proved the correctness, 2-special soundness, and honest-verifier zero-knowledge properties of this supersingular isogeny-based sigma protocol for a ring. We have also proposed a supersingular isogeny-based ring signature obtained by applying Fiat-Shamir transform to the supersingular isogeny-based sigma protocol for a ring. The correctness, anonymity, and existential unforgeability properties of this ring signature scheme have been provided. We have applied the Merkle tree to our constructions to improve the efficiency of the proposed protocols. Finally, we have provided the efficiency analyses of the given protocols. In the proposed ring signature, the signature size grows logarithmically in the size of the ring where Merkle tree paths or roots have formed a part of the verification keys.

References

1. Abe, M., Ohkubo, M., Suzuki, K.: 1-out-of-n signatures from a variety of keys. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 415–432. Springer (2002)
2. Backes, M., Döttling, N., Hanzlik, L., Kluczniak, K., Schneider, J.: Ring signatures: Logarithmic-size, no setup—from standard assumptions. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 281–311. Springer (2019)

3. Baum, C., Lin, H., Oechsner, S.: Towards practical lattice-based one-time linkable ring signatures. In: International Conference on Information and Communications Security. pp. 303–322. Springer (2018)
4. Bender, A., Katz, J., Morselli, R.: Ring signatures: Stronger definitions, and constructions without random oracles. In: Theory of Cryptography Conference. pp. 60–79. Springer (2006)
5. Beullens, W., Katsumata, S., Pintore, F.: Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices (2020)
6. Chase, M., Lysyanskaya, A.: On signatures of knowledge. In: Annual International Cryptology Conference. pp. 78–96. Springer (2006)
7. Chow, S.S., Yiu, S.M., Hui, L.C.: Efficient identity based ring signature. In: International Conference on Applied Cryptography and Network Security. pp. 499–512. Springer (2005)
8. Costello, C., Longa, P., Naehrig, M.: Efficient algorithms for supersingular isogeny diffie-hellman. In: Annual International Cryptology Conference. pp. 572–601. Springer (2016)
9. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology **8**(3), 209–247 (2014)
10. Derler, D., Ramacher, S., Slamanig, D.: Post-quantum zero-knowledge proofs for accumulators with applications to ring signatures from symmetric-key primitives. In: International Conference on Post-Quantum Cryptography. pp. 419–440. Springer (2018)
11. Dodis, Y., Kiayias, A., Nicolosi, A., Shoup, V.: Anonymous identification in ad hoc groups. In: International Conference on the Theory and Applications of Cryptographic Techniques. pp. 609–626. Springer (2004)
12. Duong, D.H., Tran, H.T., Susilo, W., et al.: An efficient multivariate threshold ring signature scheme. Computer Standards & Interfaces **74**, 103489 (2020)
13. Esgin, M.F., Zhao, R.K., Steinfeld, R., Liu, J.K., Liu, D.: Matrict: efficient, scalable and post-quantum blockchain confidential transactions protocol. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. pp. 567–584 (2019)
14. Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. Journal of Cryptology **33**(1), 130–175 (2020)
15. Groth, J., Kohlweiss, M.: One-out-of-many proofs: Or how to leak a secret and spend a coin. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 253–280. Springer (2015)
16. Herranz, J., Sáez, G.: Forking lemmas for ring signature schemes. In: International Conference on Cryptology in India. pp. 266–279. Springer (2003)
17. Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: International Workshop on Post-Quantum Cryptography. pp. 19–34. Springer (2011)
18. Katz, J., Kolesnikov, V., Wang, X.: Improved non-interactive zero knowledge with applications to post-quantum signatures. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. pp. 525–537 (2018)
19. Libert, B., Ling, S., Nguyen, K., Wang, H.: Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 1–31. Springer (2016)

20. Liu, J.K., Wei, V.K., Wong, D.S.: Linkable spontaneous anonymous group signature for ad hoc groups. In: Australasian Conference on Information Security and Privacy. pp. 325–335. Springer (2004)
21. Liu, J.K., Wong, D.S.: Linkable ring signatures: Security models and new schemes. In: International Conference on Computational Science and Its Applications. pp. 614–623. Springer (2005)
22. Mohamed, M.S.E., Petzoldt, A.: Ringrainbow–an efficient multivariate ring signature scheme. In: International Conference on Cryptology in Africa. pp. 3–20. Springer (2017)
23. Nguyen, L.: Accumulators from bilinear pairings and applications. In: Cryptographers' track at the RSA conference. pp. 275–292. Springer (2005)
24. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 552–565. Springer (2001)
25. de Saint Guilhem, C.D., Kutas, P., Petit, C., Silva, J.: Séta: Supersingular encryption from torsion attacks (2019)
26. Shacham, H., Waters, B.: Efficient ring signatures without random oracles. In: International Workshop on Public Key Cryptography. pp. 166–180. Springer (2007)
27. Silverman, J.H.: The arithmetic of elliptic curves, vol. 106. Springer Science & Business Media (2009)
28. Torres, W.A.A., Steinfeld, R., Sakzad, A., Liu, J.K., Kuchta, V., Bhattacharjee, N., Au, M.H., Cheng, J.: Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice ringct v1. 0). In: Australasian Conference on Information Security and Privacy. pp. 558–576. Springer (2018)
29. Tsang, P.P., Wei, V.K.: Short linkable ring signatures for e-voting, e-cash and attestation. In: International Conference on Information Security Practice and Experience. pp. 48–60. Springer (2005)
30. Vélu, J.: Isogenies entre courbes elliptiques. Communications de lÁcademie royale des Sciences de Paris **273**, 238–241 (1971)
31. Yoo, Y., Azarderakhsh, R., Jalali, A., Jao, D., Soukharev, V.: A post-quantum digital signature scheme based on supersingular isogenies. In: International Conference on Financial Cryptography and Data Security. pp. 163–181. Springer (2017)