SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

A study of SQIsign

av

Simon Lundborg

2026 - No M8

A study of SQIsign

Simon Lundborg

Självständigt arbete i matematik 30 högskolepoäng, avancerad nivå

Handledare: Jonas Bergström

2026

Abstract

Classical cryptographic schemes are widely used in secure digital communication. Essential to the security of many digital communication protocols are cryptographic signatures, which authorize digital messages. The most common classical cryptographic schemes are vulnerable to algorithms preformed by quantum computers and may need to be replaced. SQIsign (*Short Quaternion and Isogeny Signature*) is a recently proposed post-quantum cryptographic digital signature scheme based on isogenies between supersingular elliptic curves. In this thesis we present the SQIsign 1.0 protocol, outline the security of the scheme, prove parts of the scheme's soundness, and discuss the scheme in the context of post-quantum cryptography. Lastly we discuss SQIsign 2.0 and recent improvements to the protocol.

Sammanfattning

Klassiska kryptografiska system används i stor utsträckning för säker digital kommunikation. Avgörande för säkerheten i många digitala kommunikationsprotokoll är kryptografiska signaturer, vilket autentiserar digitala meddelanden. De vanligaste klassiska kryptografiska systemen är sårbara för algoritmer som kan utföras av kvantdatorer och kan därför behöva ersättas. SQIsign (*Short Quaternion and Isogeny Signature*) är ett nyligen föreslaget post-kvantkryptografiskt digitalt signatursystem baserat på isogenier mellan supersingulära elliptiska kurvor. I denna uppsats presenterar vi SQIsign 1.0-protokollet, beskriver systemets säkerhet, bevisar delar av dess korrekthet och diskuterar systemet i kontexten av post-kvantkryptografi. Slutligen behandlar vi SQIsign 2.0 och nyliga förbättringar av protokollet.

Contents

1 Introduction

Today, nearly all internet traffic is encrypted using mathematical methods. Encryption is essential, preventing eavesdroppers from interfering in communication, gathering passwords or collecting sensitive information. The security of these essential protocols relies on difficult mathematical problems such as factoring a large semi-prime number or the discrete log problem. In 1994 Peter Shor published Shor's algorithm [Sho97], efficiently solving these problems using a quantum computer. While quantum computers are yet to be powerful enough to run Shor's algorithm on a scale to break modern cryptography, there has been a search to find alternative cryptographic schemes which rely on different mathematical problems without any known quantum weaknesses. There is a range of proposed categories of cryptographic protocols relying on different well studied problems such as Lattice-based cryptography, Multivariate cryptography and Isogeny-based cryptography. In this thesis we will study a cryptographic protocol in the family of Isogeny-based cryptography.

There are different types of cryptographic schemes with different purposes. The most commonly used type is encryption schemes where a sender encrypts a secret message which only a secret key can decrypt. In contrast, a digital signature scheme is a cryptographic scheme in which a Verifier sends a message to a Prover, the Prover signs the message using their secret key and sends the message back to the Verifier, who can then verify the signature attached to their message using a public key. Digital signature schemes are commonly used to provide authentication to messages, which prevents man-in-the-middle attacks, where an attacker changes the contents of messages between two parties while in transit. Short Quaternion and Isogeny Signature (SQIsign) is a recently proposed digital signature scheme meant to replace digital signature schemes based on quantum-vulnerable mathematical problems.

SQIsign was first proposed in 2020, based on recent developments of certain algorithms related to isogenies [FKL+20]. In 2023, SQIsign was implemented and version 1.0 (SQIsign 1.0) was released [A+23]. SQIsign's greatest limitation was the comparatively long computation time required to generate and verify signatures. In 2025 SQIsign version 2.0 (SQIsign 2.0) was released and is under continuous development [A+25]. The authors have implemented a range of changes to the mathematical methods behind most algorithms. These optimizations make the underlying meth-

ods more difficult to interpret conceptually. The goal of this thesis is to describe the foundations of SQIsign. We will describe the SQIsign 1.0 protocol, with notes in each section describing the changes in SQIsign 2.0 on a high level. Unless otherwise specified, each section is based on the official SQIsign "Algorithm specifications and supporting documentation" [A+23] available on the SQIsign website.

Acknowledgments

I would like to thank Jonas for his encouragement, insight and feedback. I'm also thankful to Péter Suhajda for our discussions of this thesis and isogeny based cryptography.

2 Elliptic curves

SQIsign is based on isogenies and elliptic curves. We will only consider a particular type of elliptic curve called Montgomery elliptic curves. Let p be a prime and $\mathbb{F}_{p^2}$ be the finite field with p^2 elements. Let $A, B \in \mathbb{F}_{p^2}$ such that $B(A^2 - 4) \neq 0$. Now define $E_{A,B}$ as the elliptic curve with equation

$$E_{A,B} : By^2 = x^3 + Ax^2 + x.$$

If $B = 1$ we simplify the notation as E_A. The set $E_{A,B}(\mathbb{F}_{p^2})$ is the set of points $P = (x, y) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}$ which satisfy the equation above and the point at infinity $0_{E_{A,B}}$. We will only consider elliptic curves over finite fields $\mathbb{F}_{p^2}$. Since $A, B \in \mathbb{F}_{p^2}$ are chosen such that $B(A^2 - 4) \neq 0$ the following addition of points in $E_{A,B}(\mathbb{F}_{p^2})$ is well-defined. In SQIsign and the rest of this thesis we will only consider primes $p \equiv_4 3$.

Addition is defined on $E_{A,B}$ with two formulas. For two points P, Q on $E_{A,B}$ such that $Q \neq \pm P$ then their sum $R = P + Q = (x_R, y_R)$ is defined by

$$\begin{aligned} x_R &= B\lambda^2 - (x_P + x_Q) - A, \\ y_R &= \lambda(x_P - x_R) - y_P \end{aligned}$$

where

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q}.$$

We also define $-P = (x_P, -y_P)$. For $Q = -P$ we have $P + Q = P - P = 0_{E_{A,B}}$ and if $Q = P$ we denote the double $P + P = [2]P = (x_{[2]P}, y_{[2]P})$. Using the formulas above we find the following formulas

$$\begin{aligned} x_{[2]P} &= \frac{(x_P^2 - 1)^2}{4x_P(x_P^2 + Ax_P + 1)}, \\ y_{[2]P} = y_P \cdot \frac{(x_P^2 - 1)(x_P^4 + 2Ax_P^3 + 6x_P^2 + Ax_P + 1)}{8x_P^2(x_P^2 + Ax_P + 1)^2}&, \end{aligned}$$

If $P = -P$ then $[2]P = 0_E$. With this addition, the points $E_{A,B}(\mathbb{F}_{p^2})$ and the point at infinity $0_{E_{A,B}}$ form an abelian group. This is in general true for all elliptic curves. SQIsign only considers Montgomery curves for their computational efficiency for point addition.

For any integer $k \geq 0$ we now define $[k]P = \underbrace{P + P + \cdots + P}_{k}$ and for $k < 0$ we define $[k]P = -[-k]P$. Let D be an integer such that D^2 divides $|E_{A,B}(\mathbb{F}_{p^2})|$. Define the torsion group as the set of points P such that $[D]P = 0_{E_{A,B}}$. From the theory of elliptic curves [A+23, §2.2.3] we have

$$E_{A,B}[D] \cong \mathbb{Z}/D\mathbb{Z} \times \mathbb{Z}/D\mathbb{Z}.$$

For the elliptic curves we consider $|E_{A,B}(\mathbb{F}_{p^2})| = (p+1)^2$, so the available torsion groups are those which divide $p+1$. If two elliptic curves are isomorphic over a finite field extension of $\mathbb{F}_{p^2}$ rather than over $\mathbb{F}_{p^2}$, we call them a twist of each other. For Montgomery curves, $E_{A,B}$ and $E_{A,B'}$ are always quadratic twists of each other [A+23, §2.2.1]. The twist of an elliptic curve with $(p+1)^2$ points has $(p-1)^2$ points. This is not central to SQIsign, but by considering a finite field extension of $\mathbb{F}_{p^2}$, SQIsign is able to construct the torsion group $E[D]$ where D divides $p+1$ or $p-1$. We have $D \mid (p^2-1)$.

The Montgomery curve with $A = 0$ is special in the theory of supersingular elliptic curves as its endomorphism structure is well understood. We will refer to E_0 as the elliptic curve defined by

$$E_0 : y^2 = x^3 + x.$$

We can now consider a specific type of group homomorphism between elliptic curves called isogenies.

3 Isogenies

We now consider maps between elliptic curves over $\mathbb{F}_{p^2}$. An isogeny is a non-constant rational map $\varphi : E_1 \to E_2$ which is also a group homomorphism. If there is an isogeny between two curves E_1 and E_2 we say that they are isogenous. By Tate's theorem we have that two curves over $\mathbb{F}_{p^2}$ are isogenous if and only if $|E_1(\mathbb{F}_{p^2})| = |E_2(\mathbb{F}_{p^2})|$. The computationally complex problem which gives SQIsign its security is finding an isogeny between two given isogenous elliptic curves.

As isogenies are group homomorphisms we can construct the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve E which is the set of isogenies $\varphi : E \to E$ together with the zero map $[0] : E \to E$ defined by $[0]P = 0_E$ for all points. The ring addition is defined point-wise and multiplication defined as composition. For $\varphi, \psi \in \mathrm{End}(E)$ and any $P \in E$ we have

$$(\varphi + \psi)(P) := \varphi(P) + \psi(P)$$
$$(\varphi \cdot \psi)(P) := \varphi(\psi(P)) = (\varphi \circ \psi)(P)$$

Elliptic curves can be categorized into two types by the structure of their endomorphism ring. Briefly, if the endomorphism ring of an elliptic curve is commutative we call the elliptic curve ordinary. If the endomorphism ring is non-commutative we call it supersingular. The specific structure of the endomorphism rings of supersingular curves is presented in Section 5. We will only consider supersingular curves which satisfy

$$|E_{A,B}(\mathbb{F}_{p^2})| - 1 = 0 \mod p.$$

In most elliptic curve cryptography schemes, these types of supersingular elliptic curves are avoided to prevent efficient attacks on the discrete log problem [MVO91]. However, in isogeny based cryptography we will only consider supersingular as the more complicated structure of the endomorphism rings is central to the security of the scheme.

If an isogeny between two elliptic curves has an inverse isogeny we call the elliptic curves isomorphic. For Montgomery curves the j-invariant

$$j(E_{A,B}) = \frac{256(A^2 - 3)^3}{A^2 - 4}$$

characterizes the isomorphism class.

Isogenies of elliptic curves are essentially determined by their kernels. Let E_1 be an elliptic curve and let $G \subset E_1$ be a finite subgroup of order N. Then there exists an elliptic curve E_2, unique up to isomorphism, and an isogeny

$$\varphi : E_1 \to E_2$$

such that $\ker(\varphi) = G$. The degree of an isogeny φ is the size of its kernel, N. Moreover, E_2 is canonically isomorphic to the quotient curve E_1/G. SQIsign only considers isogenies where both E_1 and E_2 are Montgomery curves. In SQIsign and most other isogeny based schemes the specific isogeny is less important than the kernel of the isogeny and the domain and co-domain. Therefore we can safely ignore post-composition with isomorphisms.

For every isogeny $\varphi : E_1 \to E_2$ of degree N there exists a dual isogeny $\widehat{\varphi} : E_2 \to E_1$ such that

$$\varphi \circ \widehat{\varphi} = [N] \qquad \text{and} \qquad \widehat{\varphi} \circ \varphi = [N].$$

Which we prove in Lemma 6.1. Furthermore, it's computationally efficient to find the dual of an isogeny.

In the protocol we will refer to isogenies by the generators of their kernels. If the kernel of an isogeny is a cyclic group, we call the isogeny cyclic. These generated isogenies are central to SQIsign and are explicitly found using Vélu's formulas.

3.1 Vélu's formulas

Again consider Montgomery curves over $\mathbb{F}_{p^2}$ where p is a prime such that $p \equiv_4 3$. Given an elliptic curve E and a finite subgroup $G \subset E$, Vélu [Vé71] proves that

$$X(P) = x(P) + \sum_{Q \in G \setminus \{0_E\}} (x(P+Q) - x(Q)) \tag{1}$$

$$Y(P) = y(P) + \sum_{Q \in G \setminus \{0_E\}} (y(P+Q) - y(Q)) \tag{2}$$

define the isogeny $\varphi : E \to E/G$ by $(x, y) \mapsto (X, Y)$. The notation uses $(x(P), y(P)) = (x_P, y_P)$.

Note that composing isogenies multiplies the size their kernels. SQIsign uses this to calculate isogenies for large integers N with small prime factors. Integers with small prime factorizations are called smooth. In particular SQIsign uses isogenies with degrees which are large powers of 2 and 3. SQIsign implements Vélu's formulas in the case $N = 2$ and $G = \{0_E, Q\}$ for some Q of order 2. All such Q are of the form $(x_Q, 0)$ since $Q = -Q$. SQIsign implements Vélu's formulas to find $\varphi : E_{A,B} \to E_{A',B'}$ as follows.

Let $A', B' \in \mathbb{F}_{p^2}$ be the Montgomery coefficients for the target curve. If $x_Q = 0$ we have that the isogeny φ defined by the kernel G has the rational map

$$\varphi(x, y) = \left(\frac{1}{\sqrt{A^2 - 4}} \frac{x^2 + Ax + 1}{x}, \frac{1}{\sqrt[4]{A^4 - 4}} \cdot y \cdot \frac{x^2 - 1}{x^2} \right),$$
$$(A', B') = \left(-\frac{2A}{\sqrt{A^2 - 4}}, B \right)$$

If $x_Q \neq 0$ we instead have

$$\varphi(x, y) = \left(\frac{x_Q x^2 - x}{x - x_Q}, \sqrt{x_Q} \cdot y \cdot \frac{x_Q x^2 - 2x_Q^2 x + x_Q}{(x - x_Q)^2} \right),$$
$$(A', B') = (2(1 - 2x_Q^2), B).$$

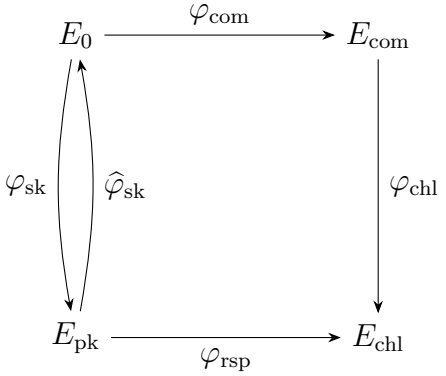
Note that B is constant, which is true for all SQIsign implementations of Vélu's formulas. From now on we will assume that $B = 1$ and denote a Montgomery curve by E_A. In theory, SQIsign can use (1) to find explicit rational maps for any prime p. The runtime of Vélu's formulas increases with the prime ℓ, effectively limiting the algorithm to primes in the hundreds.

4 A high level description of the SQIsign protocol

SQIsign is based on a proof of knowledge protocol where one party, the Prover, wants to convince another party, the Verifier, that the Prover knows some secret sk, without revealing that secret. In SQIsign this secret is an isogeny $\varphi_{\text{sk}} : E_0 \to E_{\text{pk}}$. The key-generation, signing and verification is described on a high level below.

Prover	Verifier
Generate $\varphi_{\text{sk}} : E_0 \to E_{\text{pk}}$ and publish E_{pk}	
Generate $\varphi_{\text{com}} : E_0 \to E_{\text{com}}$ and publish E_{com}	
	Generate and publish $\varphi_{\text{chl}} : E_{\text{com}} \to E_{\text{chl}}$ where E_{chl} is a random elliptic curve
Compute the dual $\widehat{\varphi}_{\text{sk}} : E_{\text{pk}} \to E_0$ Compute and publish $\varphi_{\text{rsp}} = \varphi_{\text{chl}} \circ \varphi_{\text{com}} \circ \widehat{\varphi}_{\text{sk}} : E_{\text{pk}} \to E_{\text{chl}}$	
	Verify that φ_{rsp} is an isogeny from E_{pk} to E_{chl}.

The relations of the elliptic curves are described in the diagram below



Having verified φ_{rsp}, the Verifier concludes that the Prover needed knowledge of φ_{sk}, and the verification is successful. All elliptic curves are public, so the security of SQIsign is reliant on the isogeny problem:

Problem (The Isogeny problem)**.** Given two isogenous supersingular elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$.

In Section 6 we prove that the Isogeny problem is equivalent to the Endomorphism problem:

Problem (The Endomorphism ring problem)**.** Given an elliptic curve E, find the endomorphism ring $\text{End}(E)$.

Note that instead of generating an elliptic curve E and then finding an isogeny to E, SQIsign generates a random isogeny φ and lets the the co-domain of φ be the random elliptic curve. Computing the dual $\widehat{\varphi}$ of an isogeny φ and computing the compositions of multiple isogenies is computationally efficient with known formulas which will be discussed in Section 5.

4.1 Notes on security and implementation

SQIsign is a signature scheme and the Prover needs to be able to sign a message msg provided by the Verifier. This is implemented by using the Σ protocol. On a high level msg is incorporated into the construction of E_{chl}. For an attacker both E_{pk} and E_{chl} are essentially random so the attacker needs to solve the isogeny problem in order to forge a signature. The verification protocol is implemented such that the Verifier reconstructs E_{chl} using φ_{rsp} and then concludes that φ_{rsp} is a solution to the isogeny problem, and therefore that the Verifier's message was signed using the secret φ_{sk}.

SQIsign further implements the Fiat-Shamir Transform which repeatedly hashes the message msg and other public parameters in order to find the parameter which generates E_{chl}. This is done to prevent an attacker from getting the Prover to reveal the secret key by having the Prover sign specially constructed messages. Critically the hashing process is deterministic which allows the Verifier to reconstruct E_{chl}.

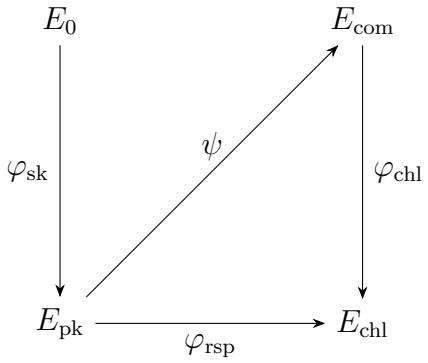
The isogeny problem states that it is difficult to find *any* isogeny between two given elliptic curves. As a consequence, protocols based on the isogeny problem are not too concerned with which specific isogeny is provided, as long as it has the correct domain, co-domain and degree. Section 7 describes how the degree of an isogeny can

be changed given some isogeny with the correct domain and co-domain. Therefore we need to be careful that an attacker does not have any way of constructing any isogeny which might reveal the secret key.

We will now discuss three critical points of security related to the isogenies used. Firstly, it is essential for the Prover to keep φ_{com} secret and difficult to guess. If an attacker finds *any* isogeny $\varphi : E_0 \to E_{\text{com}}$ then they can construct $\widehat{\varphi}_{\text{rsp}} \circ \varphi_{\text{chl}} \circ \varphi$ which can be used as the secret key to sign new messages.

Secondly, due to the known structure of the kernels of φ_{com} and φ_{chl}, publishing the composition $\varphi_{\text{rsp}} = \varphi_{\text{chl}} \circ \varphi_{\text{com}} \circ \widehat{\varphi}_{\text{sk}}$ may reveal part of the kernel of φ_{sk}. As discussed in Section 3 this is enough to reconstruct a valid secret key. SQIsign scrambles φ_{rsp} so the published isogeny is not equal to the composition provided in the high level description. See Section 7 and 11 for further description.

The third point of security is related to an algorithm a potential attacker might use to sign a message without φ_{sk}. The public key E_{pk} is fixed. Consider the diagram below where an attacker maliciously generates E_{com} with an isogeny ψ from E_{pk}. The challenge is then generated as usual and the attacker provides the signature $\varphi_{\text{rsp}} = \varphi_{\text{chl}} \circ \psi : E_{\text{pk}} \to E_{\text{chl}}$.



This attack is prevented by analyzing the "sub-isogenies" of φ_{rsp}, further discussed in Section 11.3.

5 Lattices, orders and ideals

While the proof of knowledge protocol above seems to be entirely based on elliptic curves, the underlying algorithms are based on algebra. Operations including generating random elements and composing elements are very inefficient if we restrict ourselves to elliptic curves. We are able to do these difficult operations using other mathematical objects, and then translating the results to elliptic curves and isogenies. This translation is called the Deuring Correspondence. Before considering this correspondence we first introduce the algebraic structures we can translate isogenies into.

The Quaternion Algebra $B_{p,\infty}$ is a generalization of Hamilton's quaternions, which is a generalization of the complex numbers. Formally, $B_{p,\infty}$ is the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. For our purposes, $B_{p,\infty}$ is a vector space over $\mathbb{Q}$ generated by $\{1, i, j, k\}$ with multiplication defined by

$$i^2 = -1, \qquad j^2 = -p, \qquad ij = -ji = k.$$

This is a 4-dimensional vector space with non-commutative multiplication where each element can be described as

$$\frac{a + bi + cj + dk}{r}$$

for $(a, b, c, d, r) \in \mathbb{Z}^5$, $r \neq 0$. For an element $\alpha \in B_{p,\infty}$ we define

$$\begin{aligned} \bar{\alpha} &= \frac{a - bi - cj - dk}{r} \\ \mathrm{nrd}(\alpha) = \alpha\bar{\alpha} &= \frac{a^2 + b^2 + p(c^2 + d^2)}{r^2} \in \mathbb{Q} \\ \mathrm{tr}(\alpha) = \alpha + \bar{\alpha} &= \frac{2a}{r} \in \mathbb{Q}. \end{aligned}$$

and for all non-zero α we have $\mathrm{nrd}(\alpha) > 0$ and

$$\frac{1}{\mathrm{nrd}(\alpha)}\alpha\bar{\alpha} = 1$$

so

$$\alpha^{-1} = \frac{\bar{\alpha}}{\mathrm{nrd}(\alpha)}.$$

In $B_{p,\infty}$ we consider sets of four linearly independent basis points $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ which define the lattice $L = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$. If a lattice in $B_{p,\infty}$ is also a subring (closed under multiplication and contains 1) of $B_{p,\infty}$, we call it an order. Since orders are both lattices and closed under multiplication, it follows that the elements of an order have integer norm and trace. A maximal order is an order which is not contained in any other order. A significant part of the computation done in SQIsign is manipulation of maximal orders, so we describe them further. A lattice is represented as a square matrix of side length 4 in $M_4(\mathbb{Q})$ where column i corresponds to α_i, and each row corresponds to a basis vector $\{1, i, j, k\}$. We have

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (1 \quad i \quad j \quad k) \cdot L.$$

Factoring out a common denominator of L we have that any lattice can be described as

$$L = M/r$$

where $M \in M_4(\mathbb{Z})$, $r \in \mathbb{Z}$. We will now consider lattices as integer matrices. Note that a lattice does not have a clear canonical matrix as, for example, permuting the columns produces the same lattice and a different matrix. We will consider the (column-style) Hermite normal form (HNF) of M, which is a variation of the reduced echelon form. The defining property of the matrix representation of a lattice is its column space over integer vectors. This is exactly what the Hermite normal form preserves. Equivalently, M is reduced, for example using Gauss elimination, until we have a matrix that is

- Upper triangular
- The leading non-zero element of each column is called the pivot. The pivot of a non-zero column is strictly smaller than the previous pivot. It is also positive.
- The elements to the left of pivots are zero and elements to the right of pivots are nonnegative and strictly smaller than the pivot.

The HNF exists for all integer matrices [Coh93, Thm. 2.4.3]. We now give some relevant definitions of operations with lattices. While there are additional operations with lattices in SQIsign, these are the most important. As these operations are not central to SQIsign we leave the proofs to [Coh93, §2.4.3]

- Two lattices L_1, L_2 are equal if their HNF is equal.
- The union (sum) of two lattices is the smallest lattice which includes the sum of all elements in L_1 and L_2. To calculate the HNF of the union, calculate the HNF of the 4×8 concatenation of the matrices, $\text{HNF}(L_1|L_2)$.
- The product of two lattices is the smallest lattice which includes the product of all elements in L_1 and L_2. To calculate the product multiply L_1 with each generator $\alpha_1, \ldots, \alpha_4$ of L_2 and use lattice union to compute the sum of the cosets
$$L_1\alpha_1 + L_1\alpha_2 + L_1\alpha_3 + L_1\alpha_4$$
- For our purposes, define the dual of a lattice as the transpose of the inverse, as HNF matrices.
- We now define the intersection of two lattices L_1, L_2 as the smallest lattice which contains the intersecting points of L_1 and L_2. We have that $L_1 \cap L_2$ is equal to the dual of the union of the dual of L_1 and L_2,
$$L_1 \cap L_2 = \widehat{(\widehat{L_1} + \widehat{L_2})}.$$

A sublattice of an order is called an ideal. Note that an ideal in this sense is not necessarily an ideal in the context of rings as this ideal is not necessarily closed under multiplication with elements in the order. Given an ideal I we now define two orders in which I is an ideal in the context of rings. The left and right order of an ideal I is

$$\mathcal{O}_L(I) = \{\alpha \in B_{p,\infty} : \alpha I \subset I\} \qquad \mathcal{O}_R(I) = \{\alpha \in B_{p,\infty} : I\alpha \subset I\}$$

It is clear that $\mathcal{O}_L(I)$ is an order and that I is a left ideal in the context of rings. We further say that an order $\mathcal{O}$ is the left order of I if $\mathcal{O} = \mathcal{O}_L(I)$. From the perspective of $\mathcal{O}$, we also say that I is a left ideal of $\mathcal{O}$. Note that if $\mathcal{O}$ is maximal and I is a left ideal of $\mathcal{O}$ then $\mathcal{O}_L(I) = \mathcal{O}$. All definitions and results work analogously with right orders and right ideals. An ideal with left order $\mathcal{O}_L$ and right ideal $\mathcal{O}_R$ is said to be a connecting ideal of $\mathcal{O}_L$ and $\mathcal{O}_R$.

A key part of SQIsign is generating random isogenies of a desired order. This can be done by instead sampling an ideal and then converting it into an isogeny. We first give three definitions

Definition 5.1. For a maximal order $\mathcal{O}$, quaternion $\alpha \in B_{p,\infty}$ and positive integer N such that $\gcd(\mathrm{nrd}(\alpha), N^2) = N$ let

$$\mathcal{O}\langle \alpha, N \rangle = \mathcal{O}\alpha + N\mathcal{O}.$$

Let I be an ideal. Define the reduced norm (norm) of I as

$$\mathrm{nrd}(I) = \gcd\{\mathrm{nrd}(x), x \in I\}.$$

Let the inverse of a left $\mathcal{O}$-ideal I be

$$I^{-1} = \{\alpha \in B_{p,\infty} : I\alpha \subset \mathcal{O}\}$$

We prove some useful lemmas related to quaternion ideals and orders.

Lemma 5.2. *Orders are stable under the involution $x \mapsto \bar{x}$.*

Proof. Let $\mathcal{O}$ be an order of $B_{p,\infty}$. Since $\mathcal{O}$ is a ring we have $1 \in \mathcal{O}$ and therefore $\mathbb{Z} \subset \mathcal{O}$. Let $x \in \mathcal{O}$ and consider

$$\bar{x} = x + \bar{x} - x = \underbrace{\mathrm{tr}(x)}_{\in \mathbb{Z}} - x.$$

which clearly is in $\mathcal{O}$ as $\mathcal{O}$ is closed under addition. We conclude that $\overline{\mathcal{O}} \subset \mathcal{O}$. Applying the involution again we have $\mathcal{O} = \overline{\overline{\mathcal{O}}} \subset \overline{\mathcal{O}}$ and we conclude $\overline{\mathcal{O}} = \mathcal{O}$. □

Lemma 5.3. *If $\mathcal{O}$ and $\mathcal{O}'$ are maximal ideals and I is a connecting $\mathcal{O}$, $\mathcal{O}'$ ideal we have*

$$I \cdot I^{-1} = \mathcal{O} \qquad I^{-1} \cdot I = \mathcal{O}'$$

and

$$I^{-1} = \frac{1}{nrd(I)} \bar{I}$$

Proof. We first prove the lemma for a principal ideal I. Since I is principal we have $I = \mathcal{O}\alpha$ for some non-zero $\alpha \in B_{p,\infty}$. We first prove that $I^{-1} = \alpha^{-1}\mathcal{O}$. Let $x \in I^{-1}$. We have

$$(\mathcal{O}\alpha)x = Ix \subset \mathcal{O}$$

and since $1 \in \mathcal{O}$ we have in particular

$$\alpha x \in \mathcal{O}$$

and we conclude that $x \in \alpha^{-1}\mathcal{O}$. Now let $x \in \alpha^{-1}\mathcal{O}$, $x = \alpha^{-1}o$ for some $o \in \mathcal{O}$. We have

$$Ix = (\mathcal{O}\alpha)(\alpha^{-1}o) = \mathcal{O}o \subset \mathcal{O}.$$

since $\mathcal{O}$ is closed under multiplication. We have that $x \in I^{-1}$ and conclude that $I^{-1} = \alpha^{-1}\mathcal{O}$. Now consider

$$I \cdot I^{-1} = (\mathcal{O}\alpha)(\alpha^{-1}\mathcal{O}) = \mathcal{O}\mathcal{O} = \mathcal{O}.$$

It follows similarly that

$$I^{-1} \cdot I = \mathcal{O}'$$

We now prove the second part of the lemma. Since $1 \in \mathcal{O}$ it follows that $\mathrm{nrd}(I) = \mathrm{nrd}(\alpha)$. We now have

$$I^{-1} = \alpha^{-1}\mathcal{O} = \frac{\bar{\alpha}}{\mathrm{nrd}(\alpha)}\mathcal{O} = \frac{1}{\mathrm{nrd}(\alpha)}\overline{\bar{\mathcal{O}}\alpha} = \frac{1}{\mathrm{nrd}(\alpha)}\overline{\mathcal{O}\alpha} = \frac{1}{\mathrm{nrd}(I)}\bar{I}$$

The result for non-principal ideals follows from considering *locally principal* ideals and using our results for principal ideal. The detail of this proof is beyond the scope of this thesis but are available at [Voi21, §16.2]. □

Lemma 5.4. *For any maximal order $\mathcal{O}$ and an integer N, let $\alpha \in \mathcal{O}$ where $\gcd(\mathrm{nrd}(\alpha), N^2) = N$. We then have that*

$$I = \mathcal{O}\langle \alpha, N \rangle$$

is a left $\mathcal{O}$-ideal with norm N. Furthermore, every left $\mathcal{O}$ ideal can be represented in this form.

Proof. Let $I = \mathcal{O}\langle \alpha, N \rangle$. It is clear that I is a sublattice of $\mathcal{O}$. Let $\beta \in \mathcal{O}$. We have

$$\beta I = \beta(\mathcal{O}\alpha + N\mathcal{O}) = (\beta\mathcal{O})\alpha + N(\beta\mathcal{O}) \subset \mathcal{O}\alpha + N\mathcal{O} = I$$

so I is a left-ideal of $\mathcal{O}$. Now consider the norm of I. Let $x = \beta\alpha + N\gamma \in I$. We

have

$$\begin{aligned}\mathrm{nrd}(x) &= x\bar{x} \\ &= (\beta\alpha + N\gamma)\cdot(\bar{\alpha}\bar{\beta} + N\bar{\gamma}) \\ &= \beta\alpha\bar{\alpha}\bar{\beta} + \underbrace{N\beta\alpha\bar{\gamma} + N\gamma\bar{\alpha}\bar{\beta}}_{N\mathrm{tr}(\beta\alpha\bar{\gamma})\in N\mathbb{Z}} + N^2\gamma\bar{\gamma} \\ &= \mathrm{nrd}(\alpha)\mathrm{nrd}(\beta) + N\mathrm{tr}(\beta\alpha\bar{\gamma}) + N^2\mathrm{nrd}(\gamma)\end{aligned}$$

Since β, γ are arbitrary in $\mathcal{O}$ it follows that x has norm which divides N and there is an x with norm N. We conclude that I has norm N.

The last part of the lemma follows from [A+23] and [Voi21, p.274]

□

6 The Deuring Correspondence

The Deuring Correspondence is central to the computation and representation of the elements in SQIsign. For the purposes of this thesis, the Deuring correspondence [A+23, §2.6.1] states the following:

- There is a correspondence between endomorphism rings of isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$ and conjugacy classes of maximal orders in $B_{p,\infty}$. Two orders $\mathcal{O}, \mathcal{O}'$ are in the same conjugacy class if there exists some $\alpha \in B_{p,\infty}$ such that $\alpha\mathcal{O} = \mathcal{O}'\alpha$.
- Fixing an elliptic curve E over $\mathbb{F}_{p^2}$ with endomorphism ring $\mathrm{End}(E)$ and a corresponding maximal order $\mathcal{O}$, there is a bijection between isogenies with domain E and left ideals of $\mathcal{O}$.
- Fixing isogenies φ and ψ corresponding to I_φ and I_ψ respectively we have
  - $|\ker(\varphi)| = \mathrm{nrd}(I_\varphi)$
  - If the composition $\psi \circ \varphi$ is defined we have $I_\varphi \cdot I_\psi = I_{\psi\circ\varphi}$. Note that the notation reverses the ordering.
  - The endomorphism ring of the co-domain E' of φ corresponds to the right order of I_φ, $\mathcal{O}_R(I_\varphi)$.

We will now consider isogenies as connecting ideals that connect maximal orders which represent the two endomorphism rings representing the domain and co-domain of the isogeny. In the implementation of SQIsign, these ideals and orders are instead represented as matrices in the Hermite normal form as described in Section 5.

Recall the Montgomery curve with coefficient $A = 0$, E_0. It has the known endomorphism structure

$$\mathrm{End}(E_0) \cong \mathcal{O}_0 = \mathbb{Z} \oplus i\,\mathbb{Z} \oplus \frac{i+j}{2}\,\mathbb{Z} \oplus \frac{1+k}{2}\,\mathbb{Z}.$$

In Section 8 we construct the isomorphism between the endomorphism rings of other curves E and their corresponding order $\mathcal{O}$ using an isogeny $\varphi : E_0 \to E$.

We now present some operations with ideals and orders and note how they correspond to isogenies.

- Two left $\mathcal{O}$-ideals I, J are equivalent if there exists an invertible $\beta \in B^*_{p,\infty}$ such that $I = J\beta$. That is, two left $\mathcal{O}$-ideals are considered equivalent if they have

the same right order. By the Deuring correspondence I, J are isogenies and β is an endomorphism of the target curve. Multiplication by β corresponds to post composition with an endomorphism, which does not change the co-domain. We have that the ideals corresponding to two isogenies are equivalent if the isogenies have the same domain and co-domain.

- Two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ are equivalent if there is an $\beta \in B^*_{p,\infty}$ such that $\beta\mathcal{O}_1 = \mathcal{O}_2\beta$. As endomorphism rings, this corresponds to the underlying elliptic curves being isomorphic. In the context of Montgomery curves, equivalent orders satisfy $j(\mathcal{O}_1) = j(\mathcal{O}_2)$.

- Given two maximal order $\mathcal{O}_L, \mathcal{O}_R$ we can construct a connecting ideal as

$$I = (\mathcal{O}_L + \mathcal{O}_L\mathcal{O}_R)N$$

  where $N = \text{nrd}(\mathcal{O}_L \cap \mathcal{O}_R)$. In the context of isogenies, we note that it is possible to find an isogeny between two elliptic curves if the endomorphism rings are known. Together with the formulas for $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$ we conclude that the isogeny problem and the endomorphism ring problem are equivalent.

- Given two ideals I, J such that $\mathcal{O}_R(J) = \mathcal{O}_L(I)$ with co-prime norm, define the pullback ideal

$$[J]^*I = JI + \text{nrd}(I)\mathcal{O}_L(J)$$

  which is a $\mathcal{O}_L(J)$-ideal. Also define the pushforward ideal

$$[J]_*I = J^{-1}(J \cap I)$$

  which is a left $\mathcal{O}_R(J)$-ideal. We have $[J]^*([J]_*I) = I$ and $\text{nrd}([J]^*I) = \text{nrd}([J]_*I) = \text{nrd}(I)$ [FKL+20, Lemma 3]. If $\mathcal{O}_L(J) = \mathcal{O}_0$ then the pullback operator is useful for converting an $\mathcal{O}$, $\mathcal{O}'$ ideal into a $\mathcal{O}_0$, $\mathcal{O}'$ ideal in order to do certain computations, which result can then be pushed forward to an $\mathcal{O}$, $\mathcal{O}'$ ideal.

From the high-level description of the signing protocol it is clear that efficiently computing the dual of an isogeny is necessary. While it is possible to generate the dual of φ only using torsion points, see Lemma 11.1, it's also necessary to compute $I_{\widehat{\varphi}}$. In the following lemmas we prove that $I_{\widehat{\varphi}} = \bar{I}_\varphi = \{\bar{x} : x \in I_\varphi\}$. We identify

the endomorphisms of the domain and co-domain of φ with the orders $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$.

Lemma 6.1. *For any left $\mathcal{O}$-ideal I where $\mathcal{O}$ is a maximal order*

$$\varphi_{\bar{I}} = \widehat{\varphi}$$

Proof. Let $\alpha \in \mathcal{O}_L(I)$. We have

$$\bar{I}\bar{\alpha} = \overline{\alpha I} \subset \bar{I}$$

so $\bar{\alpha} \in \mathcal{O}_R(\bar{I})$. Now assume that $\bar{\alpha} \in \mathcal{O}_R(\bar{I})$. We have

$$\alpha I = \overline{\bar{I}\bar{\alpha}} \subset \bar{I}$$

So we have $\alpha \in \mathcal{O}_L(I)$ and conclude that $\overline{\mathcal{O}_R(\bar{I})} = \mathcal{O}_L(I)$. By Lemma 5.2 we have

$$\mathcal{O}_R(\bar{I}) = \mathcal{O}_L(I)$$

It follows very similarly that

$$\mathcal{O}_L(\bar{I}) = \mathcal{O}_R(I).$$

Finally we consider $I\bar{I}$. By Lemma 5.3 we have $I \cdot \bar{I} = \mathrm{nrd}(I)I \cdot I^{-1}$ and $I \cdot I^{-1} = \mathcal{O}_L(I)$. It follows that $I \cdot \bar{I} = \mathrm{nrd}(I)\mathcal{O}_L(I)$. The explicit ring isomorphism between maximal orders and endomorphisms is discussed in Section 8 however we will now use that the quaternion $\mathrm{nrd}(I)$ corresponds to the scalar multiplication endomorphism $[\mathrm{nrd}(I)]$. Using the notation, definitions, and results from Section 8 we can conclude that $I \cdot \bar{I}$ corresponds to the endomorphism $[\mathrm{nrd}(I)]$ using the following argument:

$$I \cdot \bar{I} = \mathrm{nrd}(I)\mathcal{O}_L(I) = \mathcal{O}_L(I)\mathrm{nrd}(I) + \mathrm{nrd}(I)\mathcal{O}_L(I) = \mathcal{O}_L(I)\langle \mathrm{nrd}(I), \mathrm{nrd}(I)\rangle$$

which implies that the corresponding isogeny has kernel

$$E[I \cdot \bar{I}] = \ker([\mathrm{nrd}(I)]) \cap E[\mathrm{nrd}(I)] = E[\mathrm{nrd}(I)].$$

We now have

$$\varphi_{\bar{I}} \circ \varphi_I = \varphi_{I \cdot \bar{I}} = [\mathrm{nrd}(I)]$$

and can conclude $\varphi_{\bar{I}} = \widehat{\varphi}$ □

7 The KLPT algorithm

The KLPT algorithm is central to the security of SQIsign. Originally developed by Kohel, Lauter, Petit, and Tignol, the KLPT algorithm takes an ideal I with known left order $\mathcal{O}$ and computes an equivalent ideal $J = I\beta$, $\beta \in B^*_{p,\infty}$ with norm ℓ^e for some e and a given small prime ℓ. In SQIsign this prime is $\ell = 2$ or $\ell = 3$. This problem is the quaternion equivalent to a related problem called the the isogeny path problem. The exact details of the KLPT algorithm are beyond the scope of this thesis. We will give a high level description of the algorithm based on the original KLPT paper [KLPT14], what is required to use it, and how it reflects on the security of SQIsign.

Let I be a left $\mathcal{O}$-ideal. The algorithm is based on the surjection

$$\begin{aligned} \Psi : I \setminus \{0\} &\to \{\text{left } \mathcal{O}\text{-ideals equivalent to } I\} \\ \alpha &\mapsto \frac{I\bar{\alpha}}{\text{nrd}(I)} \end{aligned}$$

we prove that this is a surjection. Let J be an equivalent ideal to I. For some $\beta \in \mathcal{O} \setminus \{0\}$ we have

$$I\beta = J \subset \mathcal{O}$$

since J is a left $\mathcal{O}$-ideal. But this implies $\alpha \in I^{-1}$ and by Lemma 5.3 we have

$$\beta \in \frac{\bar{I}}{\text{nrd}(I)} \implies \beta = \frac{\bar{\alpha}}{\text{nrd}(I)}$$

for some $\alpha \in I \setminus \{0\}$. We finally have

$$J = I\beta = \frac{I\bar{\alpha}}{\text{nrd}(I)}.$$

We also note that

$$\text{nrd}(\Psi(\beta)) = \text{nrd}\left(\frac{I\bar{\alpha}}{\text{nrd}(I)}\right) = \frac{\text{nrd}(I)\text{nrd}(\bar{\alpha})}{\text{nrd}(I)^2} = \frac{\text{nrd}(\alpha)}{\text{nrd}(I)}$$

and that finding an equivalent ideal J with norm N is equivalent to finding an element $\alpha \in I$ with norm $N \cdot \text{nrd}(I)$. If we represent I as $I = \mathcal{O}\langle\gamma, \text{nrd}(I)\rangle$ then the

problem further reduces [KLPT14] to finding an α such that

$$\alpha \equiv \gamma \mod \text{nrd}(I)\mathcal{O}.$$

This is the core of the KLPT algorithm. We will assume that $N = \text{nrd}(I)$ is a large prime and that the desired norm is ℓ^e for given $\ell \in \{2, 3\}$. We find such an element in four steps:

1. Find a random $\delta \in \mathcal{O}$ with norm $N\ell^{e_0}$ for some e_0.
2. Find some $\tilde{\mu} \in (\mathcal{O}/N\mathcal{O})^*$ such that $(\mathcal{O}\delta/N\mathcal{O})\tilde{\mu} = I/N\mathcal{O}$
3. Find the *strong approximation* of $\tilde{\mu} \mod N$ by $\mu \in \mathcal{O}$ with norm ℓ^{e_1}
4. Output the solution $\alpha = \delta\mu$ with norm $N\ell^e$, $e = e_0 + e_1$

The details of the strong approximation algorithm is beyond the scope of this thesis but on a high level it's a generalization of the Chinese Remainder Theorem. The KLPT algorithm may fail to find a suitable μ for a given N, γ, so it might re-sample a new γ.

The authors further simplify the algorithm by only considering *special extremal* left orders $\mathcal{O}$. A special extremal order is a maximal order which allows an orthogonal decomposition, $R + Rj \subset \mathcal{O}$ which is a suborder where $R[\omega] \subset \mathbb{Q}[i]$ and ω is of minimal norm. The standard order $\mathcal{O}_0 = \mathbb{Z}\langle\sqrt{-1}, \sqrt{-p}\rangle$ contains the suborder $\mathbb{Z}[\sqrt{-1}] + \sqrt{-p}\,\mathbb{Z}[\sqrt{-1}]$ which is implemented in SQIsign. If the index of $R + Rj$ in $\mathcal{O}$ is co-prime to $\text{nrd}(I)$ we have the isomorphism

$$\frac{\mathcal{O}}{N\mathcal{O}} \cong \frac{R + Rj}{N(R + Rj)}$$

so we solve the equation for β in $R + Rj \mod N(R + Rj)$. One of the main contributions of the creators of SQIsign was generalizing the KLPT algorithm to work with all maximal orders [MW20].

We note two implications in the context of SQIsign. Firstly, in order to generate a smooth ideal which connects two given maximal orders, the KLPT algorithm requires an existing connecting ideal I. In the context of isogenies, we have that in order to generate a smooth isogeny between two given elliptic curves, we require an existing isogeny between them. That is, the KLPT algorithm does not simplify the isogeny problem.

Secondly, the maximal order $\mathcal{O}$ is required for the KLPT algorithm. If an attacker generates an isogeny between two elliptic curves without knowing the endomorphism ring structure of the domain curve, they will not be able to use the KLPT algorithm to generate a smooth isogeny between the curves. A further improvement implemented in SQIsign is related to step 3, finding strong approximations. Briefly, certain algorithms work better in the Eichler order $\mathfrak{D} = \mathcal{O} \cap \mathcal{O}_R(I)$ which further requires the maximal order corresponding to the target curve. As discussed in Section 5 it is possible to compute the right order $\mathcal{O}_R(I)$ given an ideal I.

8 Ideals to isogenies

In SQIsign, no isogenies are directly generated. Instead, ideals are generated or calculated from other algorithms and have to be converted into isogenies. In this section we describe this process. Let E be an elliptic curve with endomorphism ring corresponding to a maximal order $\mathcal{O}$ and let I be a left $\mathcal{O}$-ideal. By the Deuring correspondence we have that quaternion elements $\alpha \in \mathcal{O}$ correspond to endomorphisms on E. Define $\alpha(P)$ to be the image of $P \in E$ under the endomorphism corresponding to α. Now define

$$E[I] = \{P \in E : \alpha(P) = 0_E \ \forall \alpha \in I\}.$$

From the Deuring Correspondence we have that this subgroup of E generates the kernel of φ_I. We can then use Vélu's formulas to generate an explicit rational map. By Lemma 5.4 write I of the form $\mathcal{O}\langle \alpha, N\rangle = \mathcal{O}\alpha + N\mathcal{O}$. We have that elements of I are of the form $\beta_1\alpha + N\beta_2$ for some $\beta_1, \beta_2 \in \mathcal{O}$. It follows that

$$(\beta_1\alpha + N\beta_2)(P) = \beta_1(\alpha(P)) + \beta_2([N]P).$$

Which is identically equal to 0_{E_0} for arbitrary β_1, β_2 if and only if $P \in \ker\alpha \cap E[N]$ where $E[N]$ is the N-torsion. We have

$$E[I] = \ker\alpha \cap E[N]$$

and we only have to evaluate the kernel of a single quaternion element. Recall

$$\mathcal{O}_0 = \mathbb{Z} \oplus i\,\mathbb{Z} \oplus \frac{i+j}{2}\,\mathbb{Z} \oplus \frac{1+k}{2}\,\mathbb{Z}$$

which corresponds to $\mathrm{End}(E_0)$. For this particular order there is an explicit ring isomorphism between quaternions and endomorphisms. In a slight abuse of notation we have for any $P = (x, y) \in E_0(\mathbb{F}_{p^2})$

$$1(P) = [1]P \qquad i(P) = (-x, \sqrt{-1}y) \qquad j(P) = (x^p, y^p)$$

and the general behavior follows from the distributive properties of ring homomorphisms. SQIsign represents the quaternion element α as $x_1, x_2, x_3, x_4 \in \mathbb{Z}$

$$\alpha = x_1 \cdot 1 + x_2 i + x_3 \frac{i+j}{2} + x_4 \frac{1+ij}{2}.$$

The action of the endomorphisms $1, i, (i+j)/2, (1+k)/2$ on the deterministically generated D-torsion of E_0 are linear transformations as endomorphisms are homomorphisms. Furthermore, if ψ is an endomorphism and $P \in E[D]$ then

$$[D]\psi(P) = \psi([D]P) = \psi(0_E) = 0_E$$

so $\psi(P)$ is in the D-torsion. Recall that the torsion groups of E have structure

$$E[D] \cong \mathbb{Z}/D\mathbb{Z} \times \mathbb{Z}/D\mathbb{Z}.$$

If P, Q are generators for the D-torsion and ψ is an endomorphism we have that $\psi(P), \psi(Q) \in E[D]$ and

$$\begin{aligned}\psi(P) &= [a]P + [b]Q \\ \psi(Q) &= [c]P + [d]Q.\end{aligned}$$

Since any element of $E[D]$ can be constructed as a linear combination of P and Q we can consider the endomorphism ψ as a matrix on the vector space $E[D] \cong \mathbb{Z}/D\mathbb{Z} \times \mathbb{Z}/D\mathbb{Z}$ as

$$\mathbf{M}_\psi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Compute the matrices for the generators of $\mathrm{End}(E_0)$ presented above. The action of α on the basis of the D-torsion is then

$$\mathbf{M}_\alpha = x_1\mathbf{I} + x_2\mathbf{M}_i + x_3\mathbf{M}_{\frac{i+j}{2}} + x_4\mathbf{M}_{\frac{1+k}{2}}$$

and finding a solution $(a, b)^\intercal \in \ker \mathbf{M}_\alpha$ gives a generator $[a]P + [b]Q$ for the kernel of α where $\langle P, Q\rangle = E_0[D]$. This simply follows from

$$[a]P + [b]Q = a\begin{pmatrix}1\\0\end{pmatrix} + b\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix} \in \ker \mathbf{M}_\alpha = \ker \alpha.$$

Note that the algorithm described in this section is not limited to E_0. It is enough to be able to map the basis of the maximal order to endomorphisms in $\mathrm{End}(E)$. In Section 9 we use the known isomorphism between $\mathrm{End}(E_0)$ and $\mathcal{O}_0$ to compute this.

9 Decomposition of large isogenies

In this section we discuss how SQIsign decomposes an ideal J with norm 2^e into a chain of manageable ideals of order 2^f, where e is a multiple of f. Isogenies with order of a power of 2 are called even. Define f as the largest integers such that 2^f divides $p+1$, representing the largest order an element in E can have which is also a power of 2. While E has order $(p+1)^2$, this fact follows from the structure of the torsion group

$$E[D] \cong \mathbb{Z}/D\mathbb{Z} \times \mathbb{Z}/D\mathbb{Z}.$$

SQIsign requires all isogenies to be cyclic, having their kernel generated by a single point. Within these limitations we can only construct even isogenies of order at most 2^f. We conclude that decomposing ideals with norm 2^e into a chain of 2^f-isogenies is both required for the soundness of the protocol, and a method of compression. We require the response ideal to have order 2^e with $e > f$ for security reasons as f is too small for the desired search space of the response isogeny.

The algorithm for converting ideals to a chain of isogenies is the most computationally intensive step of the entire protocol. Both SQIsign 1.0 and SQIsign 2.0 have implemented a range of changes for improving the runtime of the algorithm. These mathematical optimizations are beyond the scope of this thesis and we instead describe the algorithm on which the improvements are based on [EHL+18]. We have altered the algorithm original to fit the purposes of SQIsign.

Recall that an ideal is a $\mathcal{O}_0$, $\mathcal{O}$ connecting ideal if it is both a left $\mathcal{O}_0$-ideal and a right $\mathcal{O}$-ideal. Let J be a $\mathcal{O}_0$, $\mathcal{O}$ connecting ideal with norm 2^e where $e = nf$. We wish to construct a sequence of ideals J_k such that

$$J = J_1 \cdot J_2 \dots J_n$$

where $\text{nrd}(J_k) = 2^f$ and $\mathcal{O}_L(J_k) = \mathcal{O}_{k-1}$, $\mathcal{O}_R(J_k) = \mathcal{O}_k$. We first define a sequence of ideals

$$I_k = J + 2^{kf}\mathcal{O}_0$$

which is a filtration of ideals,

$$J = I_n \subset I_{n-1} \cdots \subset I_1 \subset I_0 = \mathcal{O}_0.$$

The inclusions and endpoints are clear from the definition. Each J_k is constructed

as $J_k = I_{k-1}^{-1} I_k$. By Lemma 5.3 we have

$$\begin{aligned} J_1 \cdot J_2 \dots J_n &= (I_0^{-1} I_1) \cdot (I_1^{-1} I_2) \cdot (I_2^{-1} I_3) \cdot \dots \cdot I_{n-1}^{-1} I_n \\ &= (\mathcal{O}_0 \underbrace{I_1) \cdot (I_1^{-1}}_{\mathcal{O}_0} \underbrace{I_2) \cdot (I_2^{-1}}_{\mathcal{O}_0} I_3) \cdot \dots \cdot I_{n-1}^{-1} J \\ &= \mathcal{O}_0 \cdot \mathcal{O}_0 \dots \mathcal{O}_0 \cdot J \\ &= \mathcal{O}_0 J \\ &= J \end{aligned}$$

where the last step follows from the definition of a left $\mathcal{O}_0$-ideal. We conclude that

$$J = J_1 \cdot J_2 \dots J_n.$$

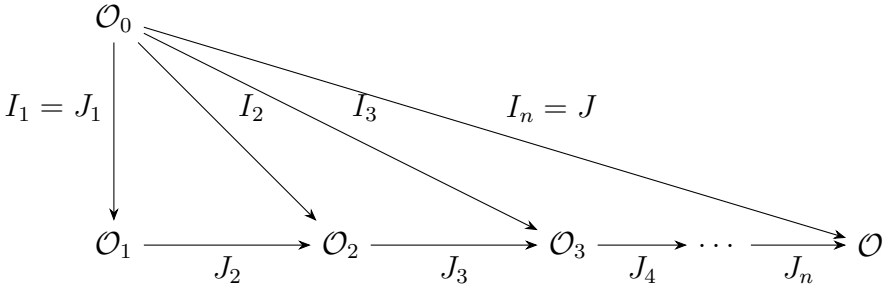
Since $1 \in \mathcal{O}$ it is clear that $\mathrm{nrd}(I_k) = 2^{kf}$ and from the identity

$$\mathrm{nrd}(\alpha^{-1}) = \mathrm{nrd}\left(\frac{\bar{\alpha}}{\mathrm{nrd}(\alpha)}\right) = \frac{\mathrm{nrd}(\bar{\alpha})}{\mathrm{nrd}(\alpha)^2} = \frac{1}{\mathrm{nrd}(\alpha)}$$

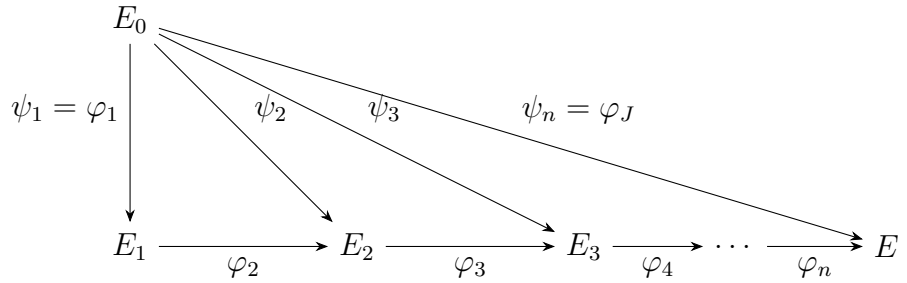
we have $\mathrm{nrd}(I_{k-1}^{-1}) = 1/\mathrm{nrd}(I_{k-1})$ and we conclude

$$\mathrm{nrd}(J_k) = \mathrm{nrd}(I_{k-1}^{-1})\mathrm{nrd}(I_k) = \frac{2^{kf}}{2^{(k-1)f}} = 2^f.$$

The orders and connecting ideals are described in the figure below. Note that $\mathcal{O}_k$ is defined as $\mathcal{O}_R(I_k)$ which is difficult to predict before running the algorithm.



Which under the Deuring correspondence corresponds to figure below



We must now construct the kernel of J_k in $\mathcal{O}_{k-1}$. As described in section 8, it is enough to find the linear transformation $\mathbf{M}_\alpha$ for a given $\alpha \in \mathcal{O}_k \cong \mathrm{End}(E_{k-1})$. We will now use the known structure of $\mathcal{O}_0$ and the isogenies $\varphi_1, \ldots, \varphi_{k-1}$ to create such a map between $\mathcal{O}_{k-1}$ and $\mathrm{End}(E_{k-1})$. On a high level this is done by computing the image of the torsion basis of E_0 under $\varphi_{k-1} \circ \cdots \circ \varphi_1$ and solving the discrete log problem

$$(\varphi_{k-1} \circ \cdots \circ \varphi_1)(P_{E_0}) = [a_P]P_{E_{k-1}} + [b_P]Q_{E_{k-1}}$$
$$(\varphi_{k-1} \circ \cdots \circ \varphi_1)(Q_{E_0}) = [a_Q]P_{E_{k-1}} + [b_Q]Q_{E_{k-1}}$$

where $\langle P_{E_0}, Q_{E_0} \rangle = E_0[2^f]$ and $\langle P_{E_{k-1}}, Q_{E_{k-1}} \rangle = E_{k-1}[2^f]$. Then, as in Section 8, use a_P, b_P, a_Q, and b_Q to construct $\mathbf{M}_\alpha$. Then, we have integers a_k, c_k which generate the kernel of J_k as $\langle K_k \rangle$ where $K_k = [a_k]P_{E_{k-1}} + [c_k]Q_{E_{k-1}}$. For compression, now wish to find an integer s_k such that $P_{E_{k-1}} + [s_k]Q_{E_{k-1}}$ generates the same kernel. Note that a_k and c_k cannot both be even, as the order of the kernel is 2^f and P, Q has order 2^f. If a_k is odd, let $b_k = 0$. Otherwise, swap P, Q (and a_k, c_k) and let $b_k = 1$. Since a_k is odd we have

$$\gcd(a_k, 2^f) = 1$$

and by the Extended Euclidean algorithm there are integers u, v such that

$$ua_k + v \cdot 2^f = 1 \iff ua_k \equiv_{2^f} 1.$$

Note from the first equation that u is co-prime to 2^f. Now scalar multiply K_k with u and we have

$$[u]K_k = [ua_k]P_{E_{k-1}} + [uc_k]Q_{E_{k-1}} = P_{E_{k-1}} + [uc_k]Q_{E_{k-1}}.$$

Since u is co-prime to 2^f, $\langle [u]K_k \rangle = \langle K_k \rangle$ and let $s_k = uc_k$. The pair (b_k, s_k) now encode all necessary information to reconstruct φ_k. The message can be further compressed as for $k > 1$, $Q_{E_{k-1}}$ is chosen to be the generator of the dual of the last isogeny φ_{k-1}. The kernel generator K_k is constructed to not backtrack. Suppose that a_k is even. Then $[2^{f-1}]K_k = [2^{f-1}]Q_{E_{k-1}}$ which is in the kernel of the dual of the previous isogeny. This would be backtracking and therefore a_k is odd and $b_k = 0$ for $k > 1$.

10 The Σ protocol and the Fiat-Shamir transform

While the proof-of-knowledge protocol implemented by SQIsign is new, the authors use an established framework for securely transforming it into a digital signature scheme. This protocol is called the Σ protocol. Furthermore the Fiat-Shamir transform is then implemented to use the Fiat-Shamir Heuristic which theorizes that the protocol is zero knowledge.

A Σ-protocol is a three phase interactive proof of knowledge between a Prover and a Verifier. Let w be a witness, or secret, known only to the Prover and let x be the public key. The three phases are

- Commitment
- Challenge
- Response

Each phase contributes to the transcript of the protocol $(\text{com}, \text{chl}, \text{rsp})$. The Prover does the Commitment phase, sends com to the Verifier who then does the Challenge phase. The Verifier sends chl to the Prover who then responds with the Response rsp. The Verifier also has a function V with binary output used to evaluate a transcript $(\text{com}, \text{chl}, \text{rsp})$. The two properties this Σ-protocol satisfies are

- Correctness. If a Prover knows the witness w and follows the Σ-protocol to produce $(\text{com}, \text{chl}, \text{rsp})$ with a Verifier, then

$$V(x, \text{com}, \text{chl}, \text{rsp}) = 1$$

- Special Soundness. If a dishonest Prover does not know w then they should be unable to produce a valid transcript. That is, producing valid transcripts is as difficult as finding a witness w to x. Formally we have that given two valid transcripts with the same commitment com

$$(\text{com}, \text{chl}_1, \text{rsp}_1), \qquad (\text{com}, \text{chl}_2, \text{rsp}_2)$$

  it is possible, in polynomial time, to produce a valid witness w to x.

The original SQIsign paper [MW20, Thm. 1] proves that the special soundness of SQIsign is equivalent to the Smooth Endomorphism Problem.

Problem. Given a prime p and a supersingular elliptic curve E over F_{p^2}, find a (non-trivial) cyclic endomorphism of E of smooth degree.

which, while slightly weaker than the Endomorphism Problem 4, is believed to be difficult [A+23, 9.1.3.1].

A protocol is "zero knowledge" if a transcript can verify that a prover knows the witness w, but does not reveal any helpful information for reconstructing w. The interactive Σ-protocol above is vulnerable as the Verifier has complete control of the challenge chl, which the Prover then uses in combination with the witness w and the commitment com to produce rsp. The concern is that a dishonest Verifier might pick a malicious challenge which forces the Prover to reveal information about the witness in the response. The Fiat-Shamir transform is implemented to prevent this attack. Formally it is defined using a random oracle, which deterministically produces a random string from some given inputs. Critically, the input of the random oracle is unrecoverable given the output.

We will simulate the random oracle using a strong cryptographic hash function, further discussed in Section 11.2.2. To prevent the Verifier from constructing a special challenge chl, the challenge phase is changed such that $\text{chl} = \text{Hash}(\text{msg}, \text{com})$ where the Verifier only controls msg and Hash is a cryptographic hash function. If the hash function is secure then it is not feasible to find a message msg such that

$$\text{chl}_{\text{mal}} = \text{Hash}(\text{msg}, \text{com})$$

for a given chl_{mal} and com. The authors of SQIsign also prove that the special soundness and the Fiat-Shamir transform as implemented is believed to preserve zero knowledge in the random oracle model [A+23, Cor. 9.1.10].

11 The SQIsign protocol

The SQIsign protocol is divided into three steps. We will first define the global parameters used in the protocol.

The prime p, which limits the available torsion groups of E which in turn are used to define the kernels of isogenies. Over the elliptic curve, the accessible torsion is $p+1$, and over its quadratic twist $p-1$. Therefore the accessible torsion is p^2-1, and we choose p such that the accessible torsion is as smooth as possible. We don't require the whole p^2-1 torsion and can instead limit the protocol to $T \mid (p^2-1)$ which is smooth. For security requirements we also require $T > p^{5/4}$. We now have the following definitions

- f is the largest integer such that $2^f \mid p+1$
- g is the largest integer such that $3^g \mid T$

The main priority is fast verification which involves computing an isogeny of degree D_{rsp} and an isogeny of degree D_{chl} which is chosen to be as smooth as possible. We will let $D_{\text{rsp}} = 2^e$ where e is a fixed parameter and a multiple of f. Let $D_{\text{chl}} = 2^f 3^g$ and $D_{\text{com}} = T/3^g$. Note that D_{chl}, D_{com} are co-prime, which is a requirement for the pullback and push-forward transformations to be defined. The option to pullback and push-forward ideals to $\mathcal{O}_0$ is crucial for computational reasons.

11.1 Key generation

The goal of the key generation is to generate a secret key sk and a public key pk. The public key pk consists of the Montgomery parameter A which defines E_{pk}. The secret key consists of elements which generate two $\mathcal{O}_0$, $\mathcal{O}_{\text{pk}}$ connecting ideals. Recall that a $\mathcal{O}$, $\mathcal{O}'$ connecting ideal is an ideal which is both a left $\mathcal{O}$-ideal and a right $\mathcal{O}'$-ideal. The connecting ideals are $I_{\text{sk}}, J_{\text{sk}}$ and the key generation also generates the image of the T torsion basis in E_0 under $\varphi_{J_{\text{sk}}}$, and a point $Q \in E_{\text{pk}}$ which generates the dual of the last 2^f isogeny in $\varphi_{J_{\text{sk}}}$. The image of the T-basis is required as the KLPT algorithm used in the signing requires information of how the known quaternion to endomorphism actions in E_0 translate to E_{pk}. The point Q is used to prevent backtracking in later algorithms.

The purpose of the two ideals is that I_{sk} is a random ideal with norm a large secret prime. This ideal defines the target curve E_{pk} and the large prime norm forces any potential attacker to consider a large search space for guessing I_{sk}. The

random prime is chosen to be about one quarter the length of p, making the search space exponential in the security parameter. As discussed previously, isogenies need to have smooth degrees to be evaluated. Therefore we also construct J_{sk} using the KLPT algorithm described in Section 7. In contrast to the KLPT algorithm used in the signing, J_{sk} does not have a predetermined order except that it is a power of 2. We then deconstruct the ideal J_{sk} into a chain of cyclic isogenies as described in Section 9.

11.2 Signing

The signing protocol is further divided into three phases: Commitment, Challenge and Response. In contrast to the high-level description of SQIsign, the entirety of the signing process is done by the Prover. In addition to the keys generated in the Key generation, we will use a message msg provided by the Verifier.

11.2.1 Commitment

In this step we randomly generate a commitment isogeny and commitment curve. We do this by randomly sampling quaternions in $\mathcal{O}_0$ until we find one with the norm D_{com}. Concretely, we sample integers $a, b \mod D_{\text{com}}$ uniformly until we have $\gcd(a, b, D_{\text{com}}) = 1$ and construct

$$\alpha = a + b\bar{\theta}$$

where

$$\theta = j + \frac{1+k}{2}.$$

It follows that $\gcd(\text{nrd}(\alpha), D_{\text{com}}^2) = D_{\text{com}}$. θ is chosen such that $P, \theta(P) \in E_0[D_{\text{com}}]$ are linearly independent where P is a predetermined generator of the D_{com} torsion. We have that $\langle P, \theta(P) \rangle = E_0[D_{\text{com}}]$ and $I = \mathcal{O}_0\langle \alpha, D_{\text{com}} \rangle$ corresponds to an isogeny with degree D_{com}. As described in Section 8 this defines the isogeny φ_{com} with kernel generated by

$$K_{\text{com}} = aP + b\theta(P)$$

where we interpret θ as an E_0 endomorphism. We define the ideal using the complex conjugate of θ, $\bar{\theta}$ as $\mathcal{O}_0\theta$ is a left $\mathcal{O}_0$-ideal. The main purpose of fixing θ in the documentation is that the action of θ as an endomorphism can be precomputed. The target Montgomery curve is then normalized and the isogeny φ_{com} is composed

with an isomorphism to the normalized Montgomery curve.

11.2.2 Challenge

The Challenge phase is the only phase of signing which is entirely deterministic. This is done for verification purposes as the message must be embedded into the challenge. Firstly we calculate an integer chl based on the message and commitment curve

$$\text{chl} = \text{Hash}(\text{msg} \,||\, j(E_{\text{com}})) \tag{3}$$

where $||$ denotes concatenation of binary strings and $j(E_{\text{com}})$ is the j-invariant of E_{com}. The hash function is public and chosen to be very difficult to reverse, which is required for the Fiat-Shamir Heuristic.

The hash function used is `SHAKE256` which is part of the SHA-3 family of hash functions published by NIST in 2015 [Nat15]. Currently the less secure SHA-2 family of hash functions are still considered secure by NIST [Nat22]. `SHAKE256` is an Extendable-output function which allows SQIsign to control the length of the output to match the other variables in the protocol, determined by the security level.

The Fiat-Shamir Transform also requires the challenge to include information from the commitment as it is prevents a malicious Verifier from crafting special messages which trick the Prover into revealing their secret key.

SQIsign 2.0 further includes the public key in the construction of chl which makes the challenge unique to the Prover, preventing two different public keys from generating the same signature. Although NIST considers SHA-3 to be secure from specific attacks, the output space required by SQIsign is considered too small for the corresponding security level, so SQIsign 2.0 introduces grinding. Grinding is the process of repeated hashing. Specifically in SQIsign 2.0, `SHAKE256` is applied a large number of times to the input, with a long output. The finally `SHAKE256` is applied a final time with the reduced length output. The length of the output and number of iterations is again determined by the security level.

The hashing is not required for the soundness of the protocol but is rather implemented to make it zero-knowledge. Furthermore it would probably be as secure with any other hash function which has variable output.

We must now generate an isogeny based on chl. This is done by constructing a generator for the kernel of an isogeny. We will require this isogeny to be of degree $2^f 3^g$ so SQIsign deterministically constructs generators R, S of $E_{\text{com}}[2^f 3^g]$. We then

define

$$K_{\text{chl}} = R + [\text{chl}]S$$

using (3) which is a point of order $2^f 3^g$. Then we generate the associated isogeny φ_{chl} with co-domain E_{chl}.

The central part of the verification is reconstructing K_{chl} using chl in order to ensure that E_{chl} was honestly generated. The Verifier will use the response isogeny φ_{rsp} to be able to work in E_{chl}, so we wish to reformulate the verification of K_{chl} mostly in E_{chl}. We use the lemma below.

Lemma 11.1. *Let D be an integer which defines a torsion group of E. If $E[D] = \langle K, P\rangle$, $\varphi : E_1 \to E_2$ and $\ker\varphi = \langle K\rangle$ then the isogeny $\widehat{\varphi} : E_2 \to E_1$ with kernel $\langle\varphi(P)\rangle$ is a dual isogeny of φ i.e $\widehat{\varphi}\circ\varphi = [D] = \varphi\circ\widehat{\varphi}$.*

Proof. Consider any $Q \in E_1$. We have for some $a, b \in \mathbb{Z}$

$$\begin{aligned}
&\widehat{\varphi}\circ\varphi(Q) = 0_{E_1}\\
\iff\ &\varphi(Q) \in \ker\widehat{\varphi}\\
\iff\ &\varphi(Q) = [a]\varphi(P)\\
\iff\ &\varphi(Q - [a]P) = 0_{E_2}\\
\iff\ &Q - [a]P \in \ker\varphi\\
\iff\ &Q - [a]P = [b]K\\
\iff\ &Q = [a]P + [b]K\\
\iff\ &Q \in E[D]\\
\iff\ &[D]Q = 0_{E_1}
\end{aligned}$$

and we have $\ker\widehat{\varphi}\circ\varphi = \ker[D]$. Since isogenies are determined by their kernel up to isomorphism and we have $\widehat{\varphi}\circ\varphi \cong [D]$. The other composition follows similarly. □

Note that if we have some $Q \in E_{\text{chl}}[2^f 3^g]$ which is linearly independent of $\varphi_{\text{chl}}(P) \in E_{\text{chl}}[2^f 3^g]$, then we have $\widehat{\varphi}_{\text{chl}}(Q) = [r]K_{\text{chl}}$ for some $r \not\equiv_{2^f 3^g} 0$. This

follows from

$$\widehat{\varphi}_{\text{chl}}(Q) = [r]K_{\text{chl}} + [b]P$$
$$\underbrace{\varphi_{\text{chl}} \circ \widehat{\varphi}_{\text{chl}}}_{[2^f 3^g]}(Q) = [r]\varphi_{\text{chl}}(K_{\text{chl}}) + [b]\varphi(P)$$
$$0_{E_{\text{com}}} = 0_{E_{\text{com}}} + [b]\varphi(P)$$
$$[b]\varphi(P) = 0_{E_{\text{com}}}$$

and we have $b \equiv_{2^f 3^g} 0$ as $\varphi(P)$ is a generator of $E_{\text{com}}[2^f 3^g]$. We will now calculate the integer r so the Verifier can simply generate Q based on $\varphi(P)$ included in the kernel of the dual isogeny $\widehat{\varphi}_{\text{chl}}$, evaluate it under $\widehat{\varphi}_{\text{chl}}$ and check

$$K_{\text{chl}} = [r]\widehat{\varphi}_{\text{chl}}(Q).$$

The proof of why this equality implies the challenge isogeny was generated by K_{chl} is provided in section 11.3.
The integer r is calculated as follows:

- Deterministically find $P \in E_{\text{com}}[2^f 3^g]$ such that $\langle K_{\text{chl}}, P\rangle = E_{\text{com}}[2^f 3^g]$
- Evaluate the image of P under φ_{chl} as a chain of an 2^f and 3^g isogeny to obtain $\varphi_{\text{chl}}(P)$
- Deterministically find $Q \in E_{\text{chl}}[2^f 3^g]$ such that $\langle \varphi(P), Q\rangle = E_{\text{chl}}[2^f 3^g]$
- Push the point Q through $\widehat{\varphi}_{\text{chl}}$ to obtain $\widehat{\varphi}_{\text{chl}}(Q)$
- Find an r such that $K_{\text{chl}} = [r]\widehat{\varphi}_{\text{chl}}(Q)$ which exists by the argument above.

Note that the last step is exactly the Elliptic curve discrete log problem (ECDLP). As discussed previously, there are reductions which makes this problem easier in supersingular curves. However these reductions would still make SQIsign too computationally complex to be practical. As opposed to normal instances of the ECDLP, we are looking for solution mod $2^f 3^g$ which is very smooth. SQIsign implements the Pohlig-Hellman [PH78] algorithm which efficiently solves the problem.

11.2.3 Response

The final phase of the signing is constructing the response. Using the ideals generated, SQIsign first constructs

$$K = \overline{J_{\text{sk}}} \cdot I_{\text{com}} \cdot I_{\text{chl}}$$

which corresponds to the isogeny

$$\varphi_K = \varphi_{\text{chl}} \circ \varphi_{\text{com}} \circ \widehat{\varphi_{\text{sk}}}.$$

Publishing K would reveal J_{sk} so SQIsign runs the KLPT-algorithm with K to find a new ideal J_{rsp} which corresponds to an isogeny from E_{pk} to E_{chl} of order 2^e where e is a fixed multiple of f depending on security level.

The constructed J_{rsp} is then decomposed into a chain of 2^f-isogenies of length $g = e/f$. Note that the KLPT-algorithm may fail and could be run multiple times until J_{rsp} is found. The ideal J_{rsp} is the decomposed into a list of integers

$$\text{rsp} = [b_1, s_1, s_2, \ldots, s_g]$$

according to the algorithm presented in Section 9. The response rsp is then sent to the Verifier.

11.3 Verification

The verification is done by the Verifier. At the beginning of verification the Verifier knows following parameters:

- The message msg
- The public key E_{pk}
- The commitment curve E_{com}
- φ_{rsp} as a chain of isogenies from E_{pk} to E_{chl}. It has the form of a list $[b_1, s_1, s_2 \ldots, s_g]$ where b_1 is a boolean and $s_i \in \mathbb{Z}$ for every i.
- $\widehat{\varphi}_{\text{chl}}$, the dual of φ_{chl}. The dual has degree $2^f 3^g$ and is split into two parts, the even part with degree 2^f and the odd part with degree 3^g represented as the list $[(b_{\text{even}}, s_{\text{even}}), (b_{\text{odd}}, s_{\text{odd}})]$

- The integer r computed in the Challenge phase.

The Verifier needs to verify the following:

- E_{chl} was generated using the Verifiers message, msg
- φ_{rsp} is an isogeny from E_{pk} to E_{chl}
- φ_{rsp} does not contain φ_{chl} as a "sub-isogeny"

Let E_{co} be the co-domain of the provided φ_{rsp}. The Verifier begins by calculating E_{co}. The Verifier deterministically finds generators $P_{\text{pk}}, Q_{\text{pk}}$ of the torsion $E_{\text{pk}}[2^f]$. If b_1 is true, swap $P_{\text{pk}}, Q_{\text{pk}}$. They then generate

$$K_1 = P_{\text{pk}} + [s_1]Q_{\text{pk}}$$

which has order 2^f as $P_{\text{pk}}, Q_{\text{pk}}$ are linearly independent. K_1 generates the kernel of a 2^f isogeny $\varphi_1 : E_{\text{pk}} \to E_1$ which is generated and $Q_1 = \varphi_1(Q_{\text{pk}})$ is calculated. Two elliptic curves are isogenous if and only if they have the same number of $\mathbb{F}_{p^2}$ points. We have that in the case of elliptic curves, the torsion of E_1 has the same structure as the torsion of E_{pk}. Note that the order of Q_1 is 2^f as

$$[2^f]Q = [2^f]\varphi_1(Q_{\text{pk}}) = \varphi_1([2^f]Q_{\text{pk}}) = \varphi(0_{E_{\text{pk}}}) = 0_{E_1}$$

and $[2^{f-1}]Q_1 = 0_{E_1}$ would imply $\varphi_1([2^{f-1}]Q_{\text{pk}}) = 0_{E_1}$ and we would have

$$\begin{aligned}[2^{f-1}]Q_{\text{pk}} &= [a]P_{\text{pk}} + [a \cdot s_1]Q_{\text{pk}} \\ [a]P_{\text{pk}} + [a \cdot s_1 - 2^{f-1}]Q_{\text{pk}} &= 0_{E_{\text{pk}}}\end{aligned}$$

which implies $a \equiv_{2^f} 0$ and thus $2^{f-1} \equiv_{2^f} 0$ which is a contradiction. We conclude that Q_1 has order 2^f.

We then deterministically find P_1 such that $\langle P_1, Q_1 \rangle = E_1[2^f]$, and continue with s_2. The procedure is done a total of g times where $e = gf$. Finally let $E_{\text{co}} = E_g$ and note the point Q which is the generator of the last 2-isogeny of φ_{rsp}. To ensure that the composition $\widehat{\varphi}_{\text{chl}} \circ \varphi_{\text{rsp}}$ is cyclic we only need to verify that the kernels which connect $\widehat{\varphi}_{\text{chl}}$ and φ_{rsp} do not intersect. That is, Q does not intersect the kernel of

the 2^f isogeny We then generate a basis P, Q for $E_{\text{co}}[2^f 3^g]$ and define

$$P_2 = [3^g]P \qquad Q_2 = [3^g]Q$$
$$P_3 = [2^f]P \qquad Q_3 = [2^f]Q$$

which define the torsion groups $E_{\text{co}}[3^g]$ and $E_{\text{co}}[2^f]$ respectively. If b_{even} is 1, swap P_2, Q_2 and if b_{odd} is 1, swap P_3, Q_3. Then define $K_2 = P_2 + [s_{\text{even}}]Q_1$ from the response which defines the kernel of the even part of $\widehat{\varphi}_{\text{chl}}$. Verifying $\langle Q \rangle \cap \langle K_2 \rangle = \varnothing$ is equivalent to $Q \notin \langle K_2 \rangle$. Since $\langle K_2 \rangle$ is cyclic there is only one element of order 2. We conclude that we only need to verify $Q \neq [2^{f-1}]K_2$, which SQIsign implements. If φ_{rsp} passes this test we conclude that $\widehat{\varphi}_{\text{chl}} \circ \varphi_{\text{rsp}}$ is cyclic.

Neither the SQIsign documentation nor any other sources have motivated a proof of why the composition being cyclic implies that φ_{rsp} needed knowledge of φ_{sk}. We will now outline some motivation of why this is true. Suppose that a nefarious attacker provides $\varphi_{\text{rsp}} = \varphi_{\text{chl}} \circ \psi$. Note that the attacker cannot use the KLPT algorithm to scramble the response isogeny as the KLPT algorithm requires knowledge of the endomorphism ring of the domain curve, which is equivalent to knowing φ_{sk}. We have

$$\widehat{\varphi}_{\text{chl}} \circ \varphi_{\text{rsp}} = \widehat{\varphi}_{\text{chl}} \circ \varphi_{\text{chl}} \circ \psi = [2^f 3^g] \circ \psi.$$

From the expected kernel of the composition, we have that the composition above must have degree $2^k 3^g$ and we have that ψ has degree which is a power of 2. However we then conclude that the composition cannot be cyclic, as there is no element with order such that a larger power of 2 than 2^f divides it, by the order of $E_{\text{chl}}(\mathbb{F}_{p^2})$. We conclude that φ_{rsp} must have been generated using φ_{sk}.

Now compute Q' such that $\langle \ker \widehat{\varphi}_{\text{chl}}, Q' \rangle = E_{\text{chl}}[2^f 3^g]$ and P as the generator of φ_{chl} as described in the Challenge phase. Now use the provided r to confirm $P = [r]\widehat{\varphi}_{\text{chl}}(Q')$ which, by the Challenge phase, implies that the challenge was generated using the provided message. This proves to the Verifier that the signature provided was to the message chosen by the Verifier. With these checks complete, the Verifier accepts the response.

12 Future of SQIsign

There is currently significant work being done on SQIsign, both on the implementation, mathematical methods and security analysis. The latest implementation of SQIsign [dt25] can generate keys, sign messages and verify signatures several orders of magnitude faster than the SQIsign 1.0 implementation [A+23, §6.5] [A+25, §1.1]. On modern hardware, signing messages takes on the order of 10 ms and verification takes on the order of 1 ms. Furthermore, SQIsign has the smallest combined secret and public key of any post quantum signature scheme, and also produces small signatures [A+25, §1.1].

The authors of SQIsign note that one of the most significant problems with the protocol is its intricate signing protocol and diversity of mathematical objects and methods. This makes SQIsign vulnerable to side-channel attacks, which attack the physical computations rather than the underlying mathematical problems. For example, the runtime and power consumption of some algorithms depend on the secret key used. The security concern is that an attacker could extract parts of the secret key by meticulously observing the runtime and power consumption of the signing algorithm. This concern was raised in a recent paper [MCJ+25] where the authors manage to extract the secret key using this method. Side-channel attacks are important to prevent, but they do not weaken the core security of SQIsign.

The mathematical theory behind critical algorithms is constantly being improved to decrease the runtime and improve the security [A+25, §1.3]. The purpose of this thesis was to present the SQIsign protocol, the key algorithms used and to prove aspects of the theory behind them. For this to be feasible we've reduced most algorithms to their core methods. In the current implementation, most algorithms are significantly more complicated than those presented in this thesis. While this has had clear impact on the runtime, one concern is that other post quantum schemes will be preferred due to their relative simplicity.

Nevertheless, SQIsign remains one of the most promising candidates for compact post quantum signatures. In particular, its remarkably small keys and signatures distinguish it from the preferred lattice-based schemes, whose signatures are often substantially larger. Furthermore, the continued improvements in both implementation and theoretical understanding suggest that many of the practical limitations of earlier versions can be mitigated.

SQIsign is still a relatively young protocol. The long-term security of the un-

derlying mathematical problems, the resistance against side-channel attacks and the complexity of secure implementations are all areas of ongoing research. As with all post quantum cryptography, confidence in the protocol will depend on continued public analysis over time.

Regardless of whether SQIsign eventually sees widespread deployment, the protocol has already had significant mathematical impact. The development of SQIsign has led to new advances in the study of supersingular isogenies, quaternion algebras and zero-knowledge techniques, and has demonstrated that isogeny-based cryptography remains a viable direction even after the collapse of the isogeny based schemes SIDH and SIKE [CD22]. The interaction between algebraic theory and practical cryptographic design makes SQIsign an interesting example of modern post quantum cryptography and an important subject for further research.

References

[A+23] Marius A. Aardal et al. SQIsign 1.0. Technical report, National Institute of Standards and Technology, 2023. URL: https://sqisign.org.

[A+25] Marius A. Aardal et al. SQIsign 2.0. Technical report, National Institute of Standards and Technology, 2025. URL: https://sqisign.org.

[CD22] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh. ePrint Report 2022/975, IACR Cryptology ePrint Archive, 2022. Includes a Magma implementation breaking SIKEp434 in approximately 10 minutes on a single core. URL: https://eprint.iacr.org/2022/975.

[Coh93] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1993. doi:10.1007/978-3-662-02945-9.

[dt25] SQISign development team. the-sqisign: Official sqisign code, version under continuous development. https://github.com/SQISign/the-sqisign, 2025. C implementation under Apache-2.0 license, last significant commit "second-round version of SQIsign" (11 months ago).

[EHL+18] Kirsten Eisentraeger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. Cryptology ePrint Archive, Paper 2018/371, 2018. URL: https://eprint.iacr.org/2018/371.

[FKL+20] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. Cryptology ePrint Archive, Paper 2020/1240, 2020. URL: https://eprint.iacr.org/2020/1240.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem, 2014. URL: https://arxiv.org/abs/1406.0981, arXiv:1406.0981.

[MCJ+25] Anisha Mukherjee, Maciej Czuprynko, David Jacquemin, Péter Kutas, and Sujoy Sinha Roy. Simple power analysis attack on sqisign. ePrint report 2025/830, IACR Cryptology ePrint Archive, 2025. Accepted at AfricaCrypt 2025. URL: https://eprint.iacr.org/2025/830.

[MVO91] Alfred Menezes, Scott Vanstone, and Tatsuaki Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing*, STOC '91, page 80–89, New York, NY, USA, 1991. Association for Computing Machinery. doi:10.1145/103418.103434.

[MW20] Shiho Moriai and Huaxiong Wang, editors. *Advances in Cryptology – ASIACRYPT 2020*, volume 12491 of *Lecture Notes in Computer Science*. Springer, 2020. doi:10.1007/978-3-030-64837-4.

[Nat15] National Institute of Standards and Technology. Fips pub 202: Sha-3 standard: Permutation-based hash and extendable-output functions. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf, August 2015. Federal Information Processing Standards Publication 202. doi:10.6028/NIST.FIPS.202.

[Nat22] National Institute of Standards and Technology. Nist transitioning away from sha-1 for all applications, December 2022. Accessed: 2026-04-22. URL: https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps.

[PH78] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms overgf(p)and its cryptographic significance (corresp.). *IEEE Transactions on Information Theory*, 24(1):106–110, 1978. doi:10.1109/TIT.1978.1055817.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. URL: http://dx.doi.org/10.1137/S0097539795293172, doi:10.1137/s0097539795293172.

[Voi21] John Voight. *Quaternion Algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, Cham, 2021. doi:10.1007/978-3-030-56694-4.

[Vé71] Jacques Vélu. Isogenies between elliptic curves. Translation by Alexandru Ghitza from the original French "Isogénies entre courbes

elliptiques", 1971. Original: C. R. Acad. Sci. Paris Sér. A-B 273 (1971), A238–A241. URL: https://aghitza.github.io/publications/translation-velu.pdf.