Eötvös Loránd University
Faculty of Science

# Attacks against Suppersingular Isogeny Diffie-Hellman

Szőri Vajk

Supervisor:
Kutas Péter

Masters Thesis

Department of Algebra and Number Theory

Budapest, 2024.

# Contents

# Chapter 1

# Introduction

Electronic communication and thus cryptography is part of our daily life. But quantum computers using Shor's algorithm can break any currently deployed cryptosystem. Isogeny-based cryptography has become one of the major candidates to develop protocols that are resistant against attacks from quantum computers. Supersingular Isogeny Diffie-Hellman(SIDH) by Luca De Feo, David Jao, and Jérôme Plût[1] is one of the most well-known isogeny-based protocols. It is a variant of the Diffie-Hellman protocol using isogenies between supersingular elliptic curves. Diffie-Hellman requires commutativity to work but isogenies between supersingular elliptic curves usually don't commute. To overcome this SIDH also provides the images of some torsion points. But these torsion points were the key together with a theorem from Kani [2] to breaking SIDH. The first successful attack was by Wouter Castryck and Thomas Decru[3] shortly followed by a similar attack by Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope and Benjamin Wesolowski[4]. These attacks only broke SIDH in polynomial time if the endomorphism ring of the starting curve was known. But the attack by Damien Robert[5] broke SIDH in polynomial time without any assumptions.

In chapter 2 and 3 I introduce some statments, theorems and concepts that are necessary to understand the SIDH protocol and the attacks. Chapter 2 is about elliptic curves I show the basic properties of isogenies between elliptic curves, the existance of a dual isogeny, the Weil pairing and an algorithm by Vélu[6] that shows that we can efficiently calculate an isogeny given its kernel if the degree of the isogeny is smooth. Chapter 3 is about abelian varieties and their polarisations, which are crucial for Kani's theorem.

Chapter 4 is about the SIDH protocol. The first part of the chapter is about Ramanujan graphs, the isogeny graph of supersingular elliptic curves is a Ramanujan graph and that means that random walks along the edges mix rapidly. Then comes the introduction of the key exchange and encryption protocols.

Chapter 5 is about an adaptive attack by Steven Galbraith, Christophe Petit, Barak Shani and Yan Bo Ti [7]. This attack works if one party uses a static private key. An adversary can recover one bit of information in every key exchange attempt unless validation methods are used in the key exchange.

Chapter 6 is about torsion point attacks, the first such attack was by Christophe Petit[8] however it was efficient in only some special cases namely when the parameters of SIDH were unbalanced, one being much larger than the other. The Castryck-Decru attack uses information about the torsion points to build $(2^a, 2^a)$ subgroups and then Kani's lemma to show that the isogeny belonging to this subgroup is an isogeny between products of elliptic curves. This information is then used as a decision tool to build the hidden isogeny by guessing parts of its composition as smaller degree isogenies. Similarly the Maino-Martindale-Panny-Pope-Wesolowsky attack uses Kani's theorem to break SIDH but instead of guessing smaller degree isogenies it directly recovers the isogeny by building an isogeny between products of elliptic curves which is then projected to one dimension. But thesse attacks are only in polinomial time if we know the endomorphism ring of the starting curve as otherwise it's hard to find an isogeny of degree $A - B$ that we can easily evaluate on the torsion points. Roberts attack overcomes this by going into higher dimensions as any integer can be written as a sum of four squares it is possible to write an isogeny of any degree as linear combination between components in dimension 8. Thus breaking SIDH in polynomial time for any starting curve.

While these attacks proved fatal for SIDH they also opened up a new chapter in isogeny based cryptography. I give two new cryptosystems based on them as examples of applications in chapter 7.

# Chapter 2

# Elliptic Curves

This chapter was made using [9](besides the section about Vélu's formula) all proofs can be found there.

**Definition 2.0.1.** The divisor group of a curve $C$, denoted by $Div(C)$, is the free abelian group generated by the points of $C$. Thus a divisor $D \in Div(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P),$$

where $n_P \in Z$ and $n_P = 0$ for all but finitely many $P \in C$. The degree of $D$ is defined by

$$degD = \sum_{P \in C} n_P.$$

The divisors of degree 0 form a subgroup of Div(C), which we denote by

$$Div^0(C) = \{D \in Div(C) : degD = 0\}.$$

**Definition 2.0.2.** Let $C$ be defined over $K$ and smooth, and let $f \in \bar{K}(C)^*$. Then the divisor of $f$ is

$$div(f) = \sum_{P \in C} ord_P(f)(P),$$

where $ord_P(f)$ is the order of vanishing or order of poles of $f$ at $P$.

**Definition 2.0.3.** A divisor $D \in Div(C)$ is principal if it has the form $D = div(f)$ for some $f \in \bar{K}(C)^*$. Two divisors are linearly equivalent, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The Picard group of $C$, denoted by $Pic(C)$, is the quotient of $Div(C)$ by its subgroup of principal divisors. We let $Pic_K(C)$ be the subgroup of $Pic(C)$ fixed by $G_{\bar{K}/K}$.

**Definition 2.0.4.** The principal divisors form a subgroup of $Div^0(C)$. We define the degree-0 part of the divisor class group of $C$ to be the quotient of $Div^0(C)$ by the subgroup of principal divisors. We denote this group by $Pic^0(C)$. Similarly, we write $Pic^0_K(C)$ for the subgroup of $Pic^0(C)$ fixed by $G_{\bar{K}/K}$.

We define these maps of divisor groups:

$$\phi^* Div(C_2) \to Div(C_1), \qquad (Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P),$$

$$\phi_* : Div(C_1) \to Div(C_2), \qquad (P) \mapsto (\phi P)$$

where $e_\phi(P)$ is the ramification index.

**Proposition 2.0.5.** *$\phi^*$ and $\phi_*$ take divisors of degree 0 to divisors of degree 0, and principal divisors to principal divisors. They thus induce maps $\phi^* : Pic^0(C_2) \to Pic^0(C_1)$ and $\phi_* : Pic^0(C_1) \to Pic^0(C_2)$. In particular, if $f \in \bar{K}(C)$ gives the map $f : C \to \mathbb{P}^1$, then $deg\ div(f) = deg f^*((0) - (\infty)) = deg f - deg f = 0$.*

**Proposition 2.0.6.** *Let (E, O) be an elliptic curve.*

1. *For every degree 0 divisor $D \in Div^0(E)$ there exists a unique point $P \in E$ satisfying*
$$D \sim (P) - (O).$$
*Define*
$$\sigma : Div^0(E) \to E$$
*to be the map that sends $D$ to its associated $P$ .*

2. *The map $\sigma$ is surjective.*

3. *Let $D_1, D_2 \in Div^0(E)$. Then*
$$\sigma(D_1) = \sigma(D_2) \textit{if and only if} D_1 \sim D_2$$
*Thus $\sigma$ induces a bijection of sets (which we also denote by $\sigma$),*
$$\sigma : Pic^0(E) \xrightarrow{\sim} E.$$

4. *The inverse to $\sigma$ is the map*

$$\kappa : E \xrightarrow{\sim} Pic^0(E), \quad P \mapsto (divisorclassof(P) - (O).$$

**Corollary 2.0.7.** *Let $E$ be an elliptic curve and let $D = \sum n_P(P) \in Div(E)$. Then $D$ is a principal divisor if and only if*

$$\sum_{P\in E} n_P = 0 \quad and \quad \sum_{P\in E} [n_P]P = 0.$$

## 2.1 Isogenies

**Definition 2.1.1.** Let $E_1$ and $E_2$ be elliptic curves. An isogeny from $E_1$ to $E_2$ is a morphism

$$\phi : E_1 \to E_2 \quad \text{satisfying} \quad \phi(O) = O.$$

Two elliptic curves $E_1$ and $E_2$ are isogenous if there is an isogeny from $E_1$ to $E_2$ with $\phi(E_1) \neq O$.

The degree of $\phi$, which is denoted by $deg(\phi)$, is the degree of the finite extension $\bar{K}(E_1/\phi^(*)\bar{K}(E_2)$. And the isogeny is separable if the extension is separable.

**Proposition 2.1.2.** 1. *Let $E/K$ be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$. Then the multiplication-by-m map*

$$[m] : E \to E$$

*is nonconstant.*

2. *Let $E_1$ and $E_2$ be elliptic curves. Then the group of isogenies*

$$Hom(E_1, E_2)$$

*is a torsion-free $\mathbb{Z}$-module*

3. *Let $E$ be an elliptic curve. Then the endomorphism ring $End(E)$ is a ring of characteristic $0$ with no zero divisors.*

**Theorem 2.1.3.** *Let $\phi : E_1 \to E_2$ be an isogeny. Then*

$$\phi(P+Q) = \phi(P) + \phi(Q) \quad for\ all \quad P, Q \in E_1.$$

**Corollary 2.1.4.** *Let $\phi : E_1 \to E_2$ be a nonzero isogeny. Then $ker\phi$ is a finite group.*

**Theorem 2.1.5.** *Let $\phi : E_1 \to E_2$ be a separable isogeny. Then $\phi$ is unramified,*

$$\# ker\phi = deg\phi$$

*and $\bar{K}(E_1)$ is a Galois extension of $\phi^*(\bar{K})(E_2)$.*

**Corollary 2.1.6.** *Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be nonconstant isogenies, and assume that $\phi$ is separable. If $ker\phi \subset ker\psi$, then there is a unique isogeny $\lambda : E_2 \to E_3$ satisfying $\phi = \lambda \circ \phi$.*

**Proposition 2.1.7.** *Let $E$ be an elliptic curve and let $\Phi$ be a finite subgroup of $E$. There are a unique elliptic curve $E'$ and a separable isogeny $\phi : E \to E'$ satisfying $ker\phi = \Phi$.*

## 2.2 Dual Isogeny

**Theorem 2.2.1.** *Let $E_1 \to E_2$ be a nonconstant isogeny of degree $m$.*

1. *There exists a unique isogeny*

$$\hat{\phi} : E_2 \to E_1 \quad satisfying \quad \hat{\phi} \circ \phi = [m]$$

2. *As a group homomorphism, $\hat{\phi}$ equals the composition*

$$E_2 \to Div^0(E_2) \xrightarrow{\quad \phi^* \quad} Div^0(E_1) \xrightarrow{sum} E_1,$$

$$Q \mapsto (Q) - (O) \qquad\qquad \sum n_P(P) \mapsto \sum [n_P]P.$$

**Theorem 2.2.2.** *Let $\phi : E_1 \to E_2$ be an isogeny.*

1. *Let $m = deg\phi$. Then*

$$\hat{\phi} \circ \phi = [m] \quad on \quad E_1 \qquad and \qquad \phi \circ \hat{\phi} = [m] \quad on \quad E_2$$

2. *Let $\lambda : E_2 \to E_3$ be another isogeny. Then $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.*

3. *Let $\psi : E_1 \to E_2$ be another isogeny. Then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$.*

4. *For all* $m \in \mathbb{Z}$,

$$\hat{[m]} = [m] \qquad and \qquad deg[m] = m^2.$$

5. $deg\hat{\phi} = deg\phi$.

6. $\hat{\hat{\phi}} = \phi$

**Corollary 2.2.3.** *Let* $E$ *be an elliptic curve and let* $m \in \mathbb{Z}$ *with* $m \neq 0$.

1. *If* $m \neq 0$ *in* $K$, *i.e. if either* $char(K) = 0$ *or* $p = char(K) > 0$ *and* $p \nmid m$, *then*

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

2. *If* $char(K) = p > 0$, *then one of the following is true:*

   (a) $E[p^r] = \{O\}$ *for all* $r = 1, 2, 3, \ldots$

   (b) $E[p^r] = \frac{\mathbb{Z}}{p^r\mathbb{Z}}$ *for all* $r = 1, 2, 3, \ldots$

**Theorem 2.2.4.** *Let* $K$ *be a field of characteristic* $p$, *and let* $E/K$ *be an elliptic curve. For each integer* $r \geq 1$, *then the following are equivalent:*

1. $E[p^r] = 0$ *for all* $r \geq 1$.

2. $End(E)$ *is an order in a quaternion algebra.*

**Definition 2.2.5.** If $E$ has properties given in 2.2.4, then we say that $E$ is supersingular.

## 2.3 Weil Pairing

Let $T \in E[m]$. Then there is a function $f \in \bar{K}(E)$ satisfying

$$div(f) = m(T) - m(O).$$

Next take $T' \in E$ to be a point with $[m]T' = T$ . Then there is similarly a function $g \in \bar{K}(E)$ satisfying

$$div(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R).$$

It is easy to verify that the functions $f \circ [m]$ and $g^m$ have the same divisor, so multiplying $f$ by an appropriate constant from $\bar{K}^*$, we may assume that $f \circ [m] = g^m$. Now let $S \in E[m]$ be another m-torsion point, where we allow $S = T$ . Then for any point $X \in E$, we have

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Thus considered as a function of $X$, the function $g(X+S)/g(X)$ takes on only finitely many values, i.e., for every $X$, it is an mth root of unity. In particular, the morphism

$$E \to \mathbb{P}^1, S \mapsto g(X+S)/g(X)$$

is not surjective, so it is constant.

**Definition 2.3.1.** Let $g$ be as above, then we call the pairing

$$e_m : E[m] \times E[m] \to \mu_m \qquad e_m(S,T) = \frac{g(X+S)}{g(X)}$$

the Weil pairing.

**Proposition 2.3.2.** *The Weil pairing has the following properties:*

1. *It is bilinear.*
2. *It is alternating.*
3. *It is nondegenerate:*

   $$\text{If } e_m(S,T) = 1 \text{ for all } S \in E[m], \text{ then } T = O.$$

4. *It is Galois invariant.*
5. *It is compatible:*

   $$e_{mm'}(S,T) = e_m([m']S,T) \text{ for all } S \in E[mm'] \text{ and } T \in E[m]$$

6. *If $\phi : E_1 \to E_2$ is an isogeny, then*

   $$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T).$$

   *and*

   $$e_m(\phi(S), \phi(T)) = e_m(S,T)^{deg(\phi)}$$

## 2.4 Vélu's formula

The algorithm takes as inputs a curve $E_1$ over a field $K$, which has the form

$$y^2 = x^3 + ax + b,$$

and a list of points of a finite subgroup of $E_1$ which we will call $G$. It outputs the Weierstrass model fot the codomain curve $E_2$ of a separable isogeny, $\phi$, withe kernel $G$, and $\phi$ as rational maps on $E_1$.

The strategy of the algorithm is to represent $\phi$ as follows for all $P \notin G$

$$\phi(P) = \left( x_P + \sum_{Q \in G\{O\}} (x_{P+Q} - x_q), y_P + \sum_{Q \in G\{O\}} (y_{P+Q} - y_Q) \right)$$

and for any $P \in G, \phi(P) = O$. This representation makes explicit the invariance of $\phi$ under translation by elements of $G$ and it is also clear that $G = ker\phi$.

To generate the rational founctions for $\phi$, let $G^+ = (G$
$\{O\})/\langle -1 \rangle$ be the equivalence classes of the points in $G$ without the identity where each point is identified with its inverse. Then for each $P \in G^+$, we define the values

$$g_P^x = 3x_P^2 + a, \quad g_P^y = -2y_P, \quad v_P = 2g_P^x, \quad u_P = (g_P^y)^2.$$

We also define

$$v = \sum_{P \in G^+} v_P, \quad w = \sum_{P \in G^+} u_P + x_P v_P.$$

Then $\phi : E_1 \to E_2$ is given by

$$\phi(x, y) - \left( x + \sum_{P \in G^+} \left( \frac{v_P}{x - x_P} - \frac{u_P}{(x - x_P)^2} \right), y + \sum_{P \in G^+} \left( \frac{2yu_P}{(x - x_P)^3} + v_P \frac{y - y_P - g_P^x g_P^y}{(x - x_P)^2} \right) \right).$$

The equation for $E_2$ is given by

$$y^2 = x^3 + (a - 5v)x + (b - 7w).$$

# Chapter 3

# Abelian Varieties

The sections about isogenies, polarisations and jacobians were mostly made using [10], part of polarisations and the section about Kani's theorem were made using [5], the subsection about Richelot isogenies was made using [11][3].

A group variety is a variety whose points form a group, and where the group operations are morphisms of varieties. An abelian variety is a projective group variety. The group structure of an abelian variety is necessarily commutative, so we write the group law additively.

A homomorphism of abelian varieties is a morphism that is also a homomorphism of abelian groups. The image of a homomorphism $X \to Y$ is an abelian subvariety of $Y$, and the kernel is a group subscheme of $X$. In fact, the kernel of a homomorphism of abelian varieties is the extension of a finite group scheme by an abelian subvariety of $X$, which may be zero (see Milne [45, §8]).

## 3.1 Isogenies

**Definition 3.1.1.** Let $X$ and $Y$ be abelian varieties, then a homomorphism $\phi : X \to Y$ is called an isogeny if it is surjective and has a finite kernel. The surjectivity of the isogeny induces a finite algebraic extension $\phi^*(K(Y)) \leq K(X)$. We define the (in)separable degree of $\phi$ to be the (in)separable degree of the field extensions $[K(X) : \phi^*(K(Y))]$.

**Proposition 3.1.2.** *Let $\phi : X \to Y$ be an isogeny. Then we have that $\#ker\phi = separable\ degree(\phi)$ .*

**Theorem 3.1.3.** *Let $X$ be an abelian variety. Then there is a 1–1 correspondence between the two sets of objects:*

1. *finite subgroups $K \subset X$*

2. *separable isogenies $\phi : X \to Y$, where two isogesnies $\phi_1 : X \to Y_1$, $\phi_2 : X \to Y_2$, are considered equal if there is an isomorphism $\psi : Y_1 \to Y_2$ such that $\phi_2 = \psi \circ \phi_1$, which is set up by $K = ker\phi$ and $Y = X/K$.*

**Theorem 3.1.4.** *Let $X$ be an abelian variety, then $Pic^0(X)$ exists uniquely up to isomorphism and is an abelian variety.*

**Definition 3.1.5.** We call $Pic^0(X)$ the dual of $X$ and denote it as $X^\vee$.

**Theorem 3.1.6.** *If $\phi : X \to Y$ is an isogeny, then so is $\phi^\vee : Y^\vee \to X^\vee$. Furthermore, if $\phi$ is separable, then $ker\phi$ and $ker\phi^\vee$ are isomorphic as finite abelian groups.*

**Theorem 3.1.7.** *Let $G$ be a finite group scheme acting on a scheme $X$ such that the orbit of any point is contained in an affine open subset of $X$. Then there is a pair $(Y, \pi)$, where $Y$ is a scheme and $\pi : X \to Y$ a morphism satisfying the following.*

1. *As a topological space, $(Y, \pi)$ is the quotient of $X$ for the action of the underlying finite group.*

2. *The morphism $\pi : X \to Y$ is $G$-invariant, and if $\pi_*(O)G$ denotes the subsheaf of $\pi_*(O)$ of $G$-invariant functions, the natural homomorphism $O_Y \to \pi_*(O_X)G$ is an isomorphism.*

*The pair $(Y, \pi)$ is uniquely determined up to isomorphism by these conditions. The morphism $\pi$ is finite and surjective. $Y$ will be denoted $X/G$, and it has the functorial property: every $G$-invariant morphisms $f : X \to Z$, exists a unique morphism $g : Y \to Z$ such that $f = g \circ \pi$.*

**Definition 3.1.8.** Let $A$ be an abelian variety we say that $A$ is superspecial if $A$ is isomorphic over $\bar{K}$ to a product of supersingular elliptic curves

This next theorem is due to Deligne, Ogus and Shioda[12].

**Theorem 3.1.9.** *All superspecial abelian varieties are isomorphic (without polarisation).*

## 3.2 Polarisation

**Definition 3.2.1.** Given an abelian variety $X$, recall that the dual variety $X^\vee$ exists and is unique up to isomorphism. An isogeny $\lambda : X \to X^\vee$ is known as a polarisation of $X$. If the polarisation is an isomorphism, then we say that it is principal.

There is a non-degenerate skew-symmetric bilinear pairing on a principally polarised abelian variety $X$ over $K$ given by

$$e_m : X[m](K) \times X^\vee[m](K) \to \bar{K}^*,$$

e where $m$ is co-prime to $p$. This is the Weil pairing.

For principally polarised abelian varieties we can identify $X$ and $X^\vee$ to obtain a pairing on $X$.

**Definition 3.2.2.** Let $X$ be a principally polarised abelian variety over $\mathbb{F}_q$ , and let $N$ be a positive integer co-prime to $q$. We say a subgroup $S$ of $X[N]$ is maximal $N$-isotropic if

1. the $l$-Weil pairing on $X[N]$ restricts trivially to $S$, and

2. $S$ is not properly contained in any other subgroup of $X[N]$ satisfying (1)

**Definition 3.2.3.** Let $X$ be a principally polarised abelian variety over $F_q$ , and let $l$ be a prime co-prime to $q$. Then an $(l,l)$-isogeny is an isogeny on $X$ such that its kernel is maximal $l$-isotropic.

**Definition 3.2.4.** Let $N$ be a positive integer, an $N$-isogeny $\phi : (X, \lambda_X) \to (Y, \lambda_Y)$ of principally polarised abelian varieties is an isogeny such that $\phi^*\lambda_Y := \phi^\vee \circ \lambda_Y \circ \phi = [N]\lambda_X$, where $\phi^\vee : X^\vee \to Y^\vee$ is the dual isogeny. Letting $\hat{\phi} = \lambda_X^{-1}\phi^\vee\lambda_Y$ be the dual isogeny $\hat{\phi} : Y \to X$ of $\phi$ with respect to the principal polarisations, this condition is equivalent to $\hat{\phi}\phi = [N]$.

**Lemma 3.2.5.** *If* $\Phi = \begin{pmatrix} \phi_{11} & \phi_{12} \\ \phi_{21} & \phi_{22} \end{pmatrix} : (X, \lambda_X \times (Y, \lambda_Y) \to (Z, \lambda_Z) \times (V, \lambda_V)$, *then for the product polarisation on* $X \times Y$ *and* $Z \times V$, $\hat{\Phi} = \begin{pmatrix} \hat{\phi}_{11} & \hat{\phi}_{21} \\ \hat{\phi}_{12} & \hat{\phi}_{22} \end{pmatrix}$.

*Proof.* We have a cannonical isomorphism $X^\vee \cong Pic^0(X)$, and that under this isomorphism the dual of $\phi$ is given by $\phi^\vee = \phi^*$. This shows that $\Phi^\vee : Z^\vee \times V^\vee \to X^\vee \times Y^\vee$ is given by $\Phi^\vee = \begin{pmatrix} \phi_{11}^\vee & \phi_{21}^\vee \\ \phi_{12}^\vee & \phi_{22}^\vee \end{pmatrix}$. Since the product polarisations act component by component, we then get that $\hat{\Phi} = \begin{pmatrix} \hat{\phi}_{11} & \hat{\phi}_{21} \\ \hat{\phi}_{12} & \hat{\phi}_{22} \end{pmatrix}$. $\square$

The next lemma shows that it's easy to evaluate any N-torsion point once a basis of the N-torsion has been evaluated.

**Lemma 3.2.6.** *Let $\phi : X \to Y$ be an isogeny between abelian varieties. Assume that the N-torsion of $X$ is rational and that we are given a basis $(P_1, \ldots, P_{2g})$ of it. Then given the evaluation $\phi(P_i$ of all $P_i$, it is possible to evaluate $\phi$ on a point $P \in X[N]$ in time $\tilde{O}(logNl_N^{1/2})$ arithmetic operations.*

*Furthermore, if $\phi$ is an $N$-isogeny and we are given a rational basis of $Y[N]$, it is possible to recover generators for its kernel $ker\phi$ in $\tilde{O}(logNl_N^{1/2})$ arithmetic operations*

## 3.3 Jacobians

**Definition 3.3.1.** The Jacobian $J_X$ of a curve $X$ is a principally polarised abelian variety, satisfying the following universal property: any map from $X$ into another abelian variety $A$ factors through $J_X$ , as in the diagram below.

$$\begin{tikzcd} X \arrow[r, dashed] \arrow[dr] & J_X \arrow[d, dashed] \\ & A \end{tikzcd}$$

The Jacobian of $X$ is unique up to isomorphism: consider the universal property with $J_X$ in place of $A$. A curve of genus greater than zero may always be embedded in its own Jacobian (if $X$ is a curve of genus zero, then $J_X$ is trivial, and so $X$ cannot embed in $J_X$ ). For the embedding to be defined over $K$, it suffices for $X$ to have a $K$-rational divisor of degree one; suppose that $D$ is such a divisor. There is a canonical embedding $\alpha D : X \hookrightarrow J_X$ , defined by $P \mapsto [P - D]$, which sends $D$ to the zero element of $J_X$

**Theorem 3.3.2.** *Let $X$ be a curve, with $g_X > 0$. Let $J_X$ be the Jacobian of $X$, and $\alpha : X \hookrightarrow J_X$ an embedding. For each integer $r \geq 0$, let*

$$W_r := \underbrace{\alpha(X) + \cdots + \alpha(X)}_{r times} \subset J_X$$

*and define $\Theta := W_{g_X - 1}$. The following properties hold:*

1. *Extending $\alpha$ linearly to a map on divisors, we have an isomorphism of groups between $Pic^0(X)$ and $J_X$*

2. *$W_r$ is a subvariety of $J_X$ of dimension $dim W_r = min(r, g_X)$.*

3. *$dim J_X = g_X$*

4. *$\Theta$ is an irreducible ample divisor on $J_X$*

**Corollary 3.3.3.** *Let $\psi : C \to X$ be a morphism of curves. The pullback $\psi^*$ and the pushforward $\psi_*$ induce well-defined homomorphisms of Jacobians*

$$\psi^* : J_X \to J_C \quad and \quad \psi_* : J_C \to J_X.$$

### 3.3.1 Richelot isogenies

Richelot isogenies are isogenies between genus 2 curves. Starting from a hyperelliptic curve $H : y^2 = h(x)$ and a $(2, 2)$-subgroup. For a contemporary exposition, including explicit formulae, we refer to Smith's thesis[11].

$$\rangle [g_1(x), 0], [g_2(x), 0] \langle, \quad g_1(x) = x^2 + g_{11}x + g_{10}, \quad g_2(x) = x^2 + g_{21}x + g_{20}$$

of its Jacobian, one lets $g_3(x) = h(x)/(g_1(x)g_2(x)) = g_{32}x^2 + g_{31}x + g_{30}$. One then computes

$$\delta = det \begin{pmatrix} g_{10} & g_{11} & 1 \\ g_{20} & g_{21} & 1 \\ g_{30} & g_{31} & g_{32} \end{pmatrix}$$

and $h'(x) = g'_1(x)g'_2(x)g'_3(x)$ where

$$g'_i(x) = \delta^{-1} \left( \frac{dg_j}{dx} g_k - g_j \frac{dg_k}{dx} \right) for (i, j, k) = (1, 2, 3), (2, 3, 1), (3, 2, 1).$$

Then the codomain of our Richelot isogeny is the Jacogian of $H' : \boldsymbol{y}^2 = h'(\boldsymbol{x})$. The Richelot correspondance is the curve $X \subset H \times H'$ defined by

$$X : g_1(x)g_1'(\boldsymbol{x}) + g_2(x)g_2'(\boldsymbol{x}) = y\boldsymbol{y} - g_1(x)g_1'(\boldsymbol{x})(x - \boldsymbol{x}) = 0.$$

It naturally comes equipped with two projection maps $\pi : X \to H, \pi' : X \to H'$. The isogeny is then

$$J_H \to J_{H'} : [D] \mapsto [\pi'_* \pi^* D] \quad .$$

This means that in order to compute the image of a point $[x^2+u_1x+u_0, v_1x+v_0] \in J_H$, one should eliminate the variables $x, y$ from the system

$$\begin{cases} x^2 + u_1x + u_0 = 0, \\ y = v_1x + v_0, \\ y^2 = h(x), \\ g_1(x)g_1'(\boldsymbol{x}) + g_2(x)g_2'(\boldsymbol{x}) = 0, \\ y\boldsymbol{y} = g_1(x)g_1'(\boldsymbol{x})(x - \boldsymbol{x}). \end{cases}$$

We expect the last two equations of its reduced Gröbner basis (with respect to the lexicographic order with $\boldsymbol{x} \prec \boldsymbol{y} \prec y \prec x$) to be of the form

$$\boldsymbol{y} = v_3'\boldsymbol{x}^3 + v_2'\boldsymbol{x}^2 + v_1'\boldsymbol{x} + v_0', \quad \boldsymbol{x}^4 + u_3'\boldsymbol{x}^3 + u_2'\boldsymbol{x}^2 + u_1'\boldsymbol{x} + u_0' = 0$$

and then $[\boldsymbol{x}^4+u_3'\boldsymbol{x}^3+u_2'\boldsymbol{x}^2+u_1'\boldsymbol{x}+u_0', v_3'\boldsymbol{x}^3+v_2'\boldsymbol{x}^2+v_1'\boldsymbol{x}+v_0']$ are non-reduced Mumford coordinates for the image on $J_{H'}$.

## 3.4 Kani's theorem

**Definition 3.4.1.** A $(d_1, d_2)$-isogeny diamond is the decomposition of a $d_1d_2$-isogeny $\phi : X \to Y$ between principally polarised abelian varieties of dimension g into two different decompositions $\phi = \phi_1' \circ \phi_1 = \phi_2' \circ \phi_2$ where $\phi_1$ is a $d_1$-isogeny and $\phi_2$ is a $d_2$-isogeny. Then $\phi_1'$ will be a $d_2$-isogeny and $\phi_2'$ a $d_1$-isogeny:

$$\begin{tikzcd} X \arrow[r, "\phi_1"] \arrow[d, "\phi_2"'] & X_1 \arrow[d, "\phi_1'"] \\ X_2 \arrow[r, "\phi_2'"'] & Y \end{tikzcd}$$

**Theorem 3.4.2** (Kani). *Let $\phi = \phi_1' \circ \phi_1 = \phi_2' \circ \phi_2$ be a $(d_1, d_2)$-isogeny diamond as above. Then $\Phi = \begin{pmatrix} \phi_1 & \hat{\phi}_1' \\ -\phi_2 & \hat{\phi}_2' \end{pmatrix}$ is a $d$-isogeny $\Phi : X \times Y \to X_1 \times X_2$ where $d = d_1 + d_2$.*

*Its kernel is given by the image of $\hat{\Phi}$ on $(X_1 \times X_2)[d]$. If $d_1$ is prime to $d_2$, we also have $ker \Phi = \{(\hat{\phi}_1(P), \phi_1'(P)) | P \in X_1[d]\}$, the kernels is thus of rank $2g$.*

*Proof.* We check using 3.2.5 that $\hat{\Phi}\Phi = [d]$. Furthermore if $d_1$ is prime to $d_2$, then the restriction of $\hat{\Phi}$ to $X_1 \times (0)$ is injective, hence its image spans the full kernel since $\#X_1[d] = d^{2g}$. □

# Chapter 4

# SIDH

## 4.1 Ramanujan graphs

Let $G = (V, E)$ be a finite graph on $h$ vertices $V = \{v_1, \ldots, v_h\}$ with undirected edges $E$. Suppose $G$ is a regular graph of degree $k$. Let $A$ be its adjacency matrix. It is convenient to identify functions on $V$ with vectors in $\mathbb{R}^h$, and therefore also think of $A$ as a self-adjoint operator on $L^2(V)$. All of the eigenvalues of $A$ satisfy the bound $|\lambda| \leq k$. Constant vectors are eigenfunctions of $A$ with eigenvalue $k$, which for obvious reasons is called the trivial eigenvalue $\lambda_{triv}$. A faimily of such graphs with $h \to \infty$ is said to be a sequence of expander graphs if all other eigenvalues of their adjacency matrices are bound away from $\lambda_{triv} = k$ by a fixed amount. In particular, no other eigenvalue is equal to $k$; this implies the graph is connected.

**Definition 4.1.1.** A Ramanujan graph is a special type of expander which has $|\lambda| \leq \sqrt{k-1}$ for any nontrivial eigenvalue which is not equal to $-k$.

**Proposition 4.1.2** ([13])**.** *Let $G$ be a regular graph of degree $k$ oh $h$ vertices. Suppose that the eigenvalue $\lambda$ of any nonconstant eigenvector satisfies the bound $|\lambda| \leq c$ for some $c < k$. Let $S$ be any subset of the vertices of $G$, and $x$ be any vertex in $G$. Then a random walk of length at least $\frac{log 2h/|S|^{1/2}}{log k/c}$ starting from $x$ will land in $S$ with probability at least $\frac{|S|}{2h} = \frac{|S|}{2|G|}$.*

An isogeny graph is a graph whose nodes consist of all elliptic curves in $\mathbb{F}_q$ belonging to a fixed isogeny class, up to $\bar{\mathbb{F}}_q$-isomorphism. In practice, the nodes are represented using j-invariants, which are invariant up to isomorphism. Isogeny graphs for supersingular elliptic curves were first considered by Mestre [14], and were shown by Pizer [15][16] to have the Ramanujan property

Every supersingular elliptic curve in characteristic $p$ is defined over either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$[9], so it suffices to fix $\mathbb{F}_q = \mathbb{F}_{p^2}$ as the field of definition for this discussion. Thus, in contrast to ordinary curves, there are a finite number of isomorphism classes of supersingular curves in any given isogeny class; this number is in fact $g+1$, where $g$ is the genus of the modular curve $X_0(p)$, which is roughly $p/12$. All supersingular curves defined over $\mathbb{F}_{p^2}$ belong to the same isogeny class. For a fixed prime value of $l \neq p$ , we define the vertices of the supersingular isogeny graph $G$ to consist of these $g$ isomorphism classes of curves, with edges given by isomorphism classes of degree-$l$ isogenies, defined as follows: two isogenies $\phi_1, \phi_2 : E_i \to E_j$ are isomorphic if there exists an automorphism $\alpha \in Aut(E_j)$ (i.e., an invertible endomorphism) such that $\phi_2 = \alpha\phi_1$. Pizer has shown that $G$ is a connected $k = l+1$-regular multigraph satisfying the Ramanujan bound of $|\lambda| \leq 2\sqrt{l} = 2\sqrt{k-1}$ for the nontrivial eigenvalues of its adjacency matrix[15][16].

## 4.2 Key-exchange protocol

The protocol requires supersingular curves of smooth order. Such curves are normally unsuitable for cryptography since discrete logarithms on them are easy. However, since the discrete logarithm problem is unimportant in our setting, this issue does not affect us. In the supersingular setting, it is easy to construct curves of smooth order, and using a smooth order curve will give a large number of isogenies that are fast to compute. Specifically, we fix $\mathbb{F}_q = \mathbb{F}_{p^2}$ as the field of definition, where $p$ is a prime of the form $l_A^{e_A} l_B^{e_B} f \pm 1$. Here $l_A$ and $l_B$ are small primes, and $f$ is a cofactor such that $p$ is prime. Then we construct a supersingular curve $E$ defined over $\mathbb{F}_q$ of cardinality $(l_A^{e_A} l_B^{e_B})^2$. By construction, $E[l_A^{e_A}]$ is $\mathbb{F}_Q$-rational and contains $l_A^{e_A - 1}(l_A + 1)$ cyclic subgroups of order $l_A^{e_A}$, each defining a different isogeny; the analogous statement holds for $E[l_B^{e_B}]$.

The protocol revolves around the following commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E/\langle P\rangle \\ {\scriptstyle\psi}\downarrow & & \downarrow \\ E/\langle Q\rangle & \longrightarrow & E/\langle P, Q\rangle \end{array}$$

where $\phi$ and $\psi$ are random walks in the graphs of isogenies of degrees $l_A$ and $l_B$ respectively. Their security is based on the difficulty of finding a path connecting two given vertices in a graph of supersingular isogenies.

The key exchange protocol is a variation of Diffie-Hellman over the diagram. The idea is to let Alice choose $\phi$, whie Bob chooses $\psi$. We fix as public parameters a supersingular curve $E_0$ defined over $\mathbb{F}_q$ , and bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ which generate $E_0[l_A^{e_A}]$ and $E_0[l_B^{e_B}]$ respectively, so that $\langle P_A, Q_A\rangle = E_0[l_A^{e_A}]$ and $\langle P_B, Q_B\rangle = E_0[l_B^{e_B}]$. Alice chooses two random elements $a_1, a_2 \in \mathbb{Z}/l_A^{e_A}\mathbb{Z}$, not both divisible by $l_A$, and computes an isogeny $\phi_A : E_0 \to E_A$ with kernel $K_A := \langle [a_1]P_A, [a_2]Q_A\rangle$. Alice also computes the image $\{\phi_A(P_B), \phi_A(Q_B)\} \subset E_A$ of the basis $\{P_B, Q_B\}$ for $E_0[l_B^{e_B}]$ under her secret isogeny $\phi_A$, and sends these points to Bob together with $E_A$.

Similarly, Bob selects random elements $b_1, b_2 \in \mathbb{Z}/l_B^{e_B}\mathbb{Z}$ and computes an isogeny $\phi_B : E_0 \to E_B$ having kernel $K_B := \langle [b_1]P_B, [b_2]Q_B\rangle$, along with the points $\{\phi_B(P_A), \phi_B(Q_A)\}$ . Upon receipt of $E_B$ and $\phi_B(P_A), \phi_B(Q_A) \in E_B$ from Bob, Alice computes an isogeny $\phi'_A : E_B \to E_{AB}$ having kernel equal to $\langle [a_1]\phi_B(P_A) + [a_2]\phi_B(Q_A)\rangle$ ; Bob proceeds likewise. Alice and Bob can then use the common j-invariant of

$$E_{AB} = \phi'_B(\phi_A(E_0)) = \phi'_A(\phi_B(E_0)) = E_0/\langle [a_1]P_A + [a_2]Q_A, [b_1]P_B + [b_2]Q_B\rangle$$

to form a secret shared key.

The degree of the isogenies is large but smooth so they can compute them using Vélu's formula as a composition of small degree isogenies. But Vélu's formula only determines codomain curves up to isomorphism, hence it's not necessary that both parties have the same curve $E_{AB}$. Therefore in the key derivation, the parties take the j-invariant $j(E_{AB})$ to be their shared key.

## 4.3 Encryption protocol

The public-key encryption scheme is constructed from the key exchange scheme with a few adaptations. Namely, the shared secret would be used as a key for a symmetric encryption scheme to encrypt the message. We will use the same notation as above and assume that Bob wants to send a message to Alice. There are four steps to the encryption protocol: The set-up, key generation, encryption and decryption.

**Setup:** Choose $p = l_A^{e_A} l_B^{e_B} f \pm 1, E_0, \{P_A, P_B\}, \{P_B, Q_B\}$ as above. Let $H = \{H_k : k \in I\}$ be a hash function family indexed by a finite set $I$, where each $H_k$ is a function from $\mathbb{F}_{p^2}$ to the message space $\{0,1\}^w$.

**Key generation:** Choose two random elements $a_1, a_2 \in \mathbb{Z}/l_A^{e_A}\mathbb{Z}$, not both divisible by $l_A$. Compute $E_A, \phi_A(P_B), \phi_A(Q_B)$ as above, and choose a random element $k \in I$. The public key is the tuple $(E_A, \phi_A(P_B), \phi_A(Q_B), k)$ and the private key is $(a_1, a_2, k)$.

**Encryption:** Given a public key $(E_A, \phi_A(P_B), \phi_A(Q_B), k)$ and a message $m \in \{0,1\}^w$, choose two random elements $b_1, b_2 \in \mathbb{Z}/l_B^{e_B}\mathbb{Z}$, not both divisible by $l_B$, and compute

$$h = H_k(j(E_{AB})),$$
$$c = h \oplus c.$$

The ciphertext is $(E_B, \phi_B(P_A), \phi_B(Q_A), c)$.

**Decryption:** Given a ciphertext $(E_B, \phi_B(P_A), \phi_B(Q_A), c)$ and a private key $(a_1, a_2, k)$, compute the j-invariant $j(E_{AB})$ and set

$$h = H_k(j(E_{AB})),$$
$$m = h \oplus c.$$

The plaintext is m.

The security of the key exchange and encryption protocol relies on the supersingular isogeny with torsion problem.

**Problem 4.3.1** (Supersingular Isogeny with Torsion(SSI-T)). *Given coprime integers $A$ and $B$, two supersingular elliptic curves $E_0/\mathbb{F}_{p^2}$ and $E_A/\mathbb{F}_{p^2}$ connected by an unknown degree-$A$ isogeny $\phi_A : E_0 \to E_A$, and given the restriction of $\phi_A$ to the $B$-torsion of $E_0$, recover an isogeny $\phi$ matching these contraints.*

# Chapter 5

# Adaptive attack

In this chapter, we will assume that Alice is using a static key $(a_1, a_2)$, and that a dishonest user is playing the role of Bob and trying to learn her key. Our discussion is entirely about Alice's key and points in $E[2^n]$, but it should be clear that the same methods would work for points in $E[l^m]$ for any small prime $l$.

There are two attack models that can be defined in therms of access to an oracle $O$ :

1. $O(E, R, S) = E/\langle [a_1]R + [a_2]S \rangle$. If the scheme under attack is the key exchange scheme, this corresponds to Alice taking Bob's protocol message, completing her side of the protocol, and outputting the shared key. In the encryption protocol, this would correspond to an encryption $c = m \oplus j(E_{AB})$ without the hash function and Alice decrypting Bob's ciphertext and returning the plaintext $m$.

2. $O(E, R, S, E')$ which returns 1 if $j(E') = j(E/\langle [a_1]R + [a_2]S \rangle)$ and 0 otherwise.

   In the key exchange setting, this corresponds to Alice taking Bob's protocol message, completing her side of the protocol, and then performing some operations using the shared key that return an error message if the shared key is not the same as the j-invariant provided (e.g., the protocol involves verifying a MAC corresponding to a key derived from the session key). In the encryption scenario, this would correspond to Bob having access to a decryption oracle for Alice. By choosing a random ciphertext $c$ Bob could ask for a decryption of $(E_B, R, S, c)$ and get $m$ such that $c = m \oplus H_k(j(E_{AB})$. Bob can then check whether or not $c \oplus m = H_k(j(E'))$. Hence a decryption oracle for the encryption scheme gives an oracle $O$ of this type.

The attack can be mounted in both models. To emphasise their power we explain them in the context of the second weaker model.

## 5.1 First Step of the Attack

We define an equivalence relation on the private keys, by saying $(a_1, a_2) \sim (a_1', a_2'$ if the two keys lead to the same subgroup for all possible input points. The relation is satisfied by $(a_1', a_2') = (\theta a_1, \theta a_2)$ for any $\theta \in \mathbb{Z}_{2^n}^*$ , and so the equivalence class is a point in projective space over a ring. We may define a unique equivalence class representative by "normalising" as explained in the following lemma

**Lemma 5.1.1.** *Let $P, Q \in E[2^n]$ be linearly independent generators of $E[2^n]$. Then for some $(a_1, a_2) \in \mathbb{Z}^2$ (not simultaneously even), we have that $(a_1, a_2) \sim (1, \alpha)$ or $(a_1, a_2) \sim (\alpha, 1)$ for some $\alpha \in \mathbb{Z}$ (using the equivalence relation defined above).*

*Proof.* If $a_1$ is odd, then it is invertible modulo the order of the group, so let $\theta \equiv a_1^{-1} \pmod{2^n}$, then $\theta$ must be odd, hence

$$\langle [a_1]P_A + [a_2]Q_A \rangle = \langle [\theta a_1]P_A + [\theta a_2]Q_A \rangle = \langle P_A + [\alpha]Q_A \rangle,$$

where the first equality stems from the fact that $\theta$ is co-prime to the order of the generator, and the last equality is obtained by setting $\alpha = \theta a_2$. If $a_1$ is even, then $a_2$ must be odd, and repeating the procedure gives $(\alpha, 1)$. $\square$

We may assume that the private key is normalised without loss of generality. In the following exposition, we will assume that the normalisation is $(1, \alpha)$. The case where we have $(\alpha', 1)$ where $\alpha'$ is even is performed in exactly the same way with some tweaks. Note that if $\alpha'$ is odd then it can be converted to the $(1, \alpha)$ case, so we may assume $\alpha'$ is even in the second case.

To differentiate between $(1, \alpha)$ and $(\alpha', 1)$ an attacker honestly generates Bob's ephemeral values $(E_B, R = \phi_B(P_A), S = \phi_B(Q_A))$ and follows the protocol to compute the resulting key $E_{AB}$ . Then the attacker sends

$(E_B, R, S + [2^{n-1}]R)$ to Alice and tests the resulting j-invariant. Expressing this in terms of the oracle access: The attacker queries an oracle of the second type on $(E_B, R, S+[2^{n-1}]R, E_{AB})$. If the oracle returns 1 then the curve $EB/\langle [a_1]R+[a_2](S+[2^{n-1}]R)\rangle$ is isomorphic to $E_{AB}$ and so $\langle [a_1]R+[a_2](S+[2^{n-1}]R)\rangle = \langle [a_1]R + [a_2]S\rangle$. Hence, by the following Lemma, $a_2$ is even and we are in the first case. If the oracle returns 0 then $a_2$ is odd.

**Lemma 5.1.2.** *Let $R, S \in E[2^n]$ be linearly independent points of order $2^n$ and let $a_1, a_2 \in \mathbb{Z}$. Then*

$$\langle [a_1]R + [a_2](S + [2^{n-1}]R)\rangle = \langle [a_1]R + [a_2]S\rangle$$

*if and only if $a_2$ is even.*

*Proof.* If $a_2$ is even then $[a_2][2^{n-1}]R = 0$ and so the result follows. Conversely, if the two groups are equal then there is some $\lambda \in \mathbb{Z}_{2^n}^*$ such that

$$\lambda([a_1]R + [a_2](S + [2^{n-1}]R)) = [a_1]R + [a_2]S.$$

Since the points are independent we have $\lambda a_2 = a_2$ and so $\lambda = 1$. Hence, since $S$ has order $2^n$, we have $a_2^{2n-1} \equiv 0 \pmod{2^n}$ and $a_2$ is even. □

Note that the Weil pairing

$$e_{2^n}(R, S + [2^{n-1}]R) = e_{2^n}(R, S) = e_{2^n}(P_A, Q_A)^{3^m}$$

and so the attack is not detectable using pairings. Similarly one can call the oracle on $(E_B, R + [2^{n-1}]S, S, E_{AB})$. The oracle returns 1 if and only if $a_1$ is even. Hence, we can determine which of the two cases we are in and determine if $\alpha$ is even or odd. Having recovered asingle bit of $\alpha$, we will now explain how to use similar ideas to recover the rest of the bits of $\alpha$.

## 5.2 Continuing the Attack

We now assume that Alice's static key is of the form $(1, \alpha)$ and we write

$$\alpha = \alpha_0 + 2^1\alpha_1 + \cdots + 2^{n-1}\alpha_{n-1}.$$

The attacker will learn one bit of $\alpha$ for each query of the oracle. Algorithm 1 gives pseudo-code for the attack. We now give some explanation and present the derivation of the algorithm. Suppose an attacker has recovered the first $i$ bits of $\alpha$, so that

$$\alpha = K_i + 2^i\alpha_i + 2^{i+1}\alpha',$$

where $K_i$ is known but $\alpha_i \in \{0, 1\}$ and $\alpha' \in \mathbb{Z}$ are not known. The attacker generates $E_B, R = \phi_B(P_A), S = \phi_B(Q_A)$ and $E_{AB}$ as in the protocol. To recover $\alpha_i$, the attacker will choose suitable integers $a, b, c, d$ and query the oracle on

$$(E_B, [a]R + [b]S, [c]R + [d]S, E_{AB}).$$

The integers $a, b, c$, and $d$ will be chosen to satisfy the following conditions:

1. If$\alpha_i = 0$, then $\langle [a + \alpha c]R + [b + \alpha d]S\rangle = \langle R + [\alpha]S\rangle$.

2. If $\alpha_i = 1$, then $\langle [a + \alpha c]R + [b + \alpha d]S\rangle \neq \langle R + [\alpha]S\rangle$.

3. $[a]R + [b]S$ and $[c]R + [d]S$ both have order $2^n$.

4. The Weil pairing $e_{2^n}([a]R + [b]S, [c]R + [d]S)$ must be equal to

$$e_{2^n}(\phi_B(P_A), \phi_B(Q_A)) = e_{2^n}(P_A, Q_A)^{deg\phi_B} = e_{2^n}(P_A, Q_A)^{3m}.$$

The first two conditions help us distinguish the bit $\alpha_i$ and the latter two prevent the attack from being detected via order checking and Weil pairing validation checks respectively. Consider the following integers:

$$a_i = 1, b_i = -2^{n-i-1}K_i,$$
$$c_i = 0, d_i = 1 + 2^{n-i-1} .$$

One can verify that they satisfy the third condition. To satisfy the fourth condition we need to use a scaling by $\theta$ that we will discuss later.

To show that the first two conditions are satisfied, note that $\langle [a]R+[b]S+[\alpha]([c]R + [d]S)\rangle$ is equal to

$$\begin{aligned}
&\langle R - [2^{n-i-1}K_i]S + [\alpha][1 + 2^{n-i-1}]S\rangle \\
&= \langle R + [\alpha]S + [-2^{n-i-1}K_i + 2^{n-i-1}(K_i + 2^i\alpha_i + 2^{i+}1\alpha')]S\rangle \\
&= \langle R + [\alpha]S + [\alpha_i 2^{n-1}]S\rangle \\
&= \begin{cases} \langle R + [\alpha]S\rangle & if \quad \alpha_i = 0, \\ \langle R + [\alpha]S + [2^{n-1}]S\rangle & if \quad \alpha_i = 1. \end{cases}
\end{aligned}$$

By the following Lemma, these two subgroups are different. Hence the response of the oracle tells us $\alpha_i$

**Lemma 5.2.1.** *Let $R$ and $S$ be linearly independent elements of the group $E[2^n]$ with full order, then the subgroups*

$$\langle R + [\alpha]S + [2^{n-1}]S \rangle \quad \textit{and} \quad \langle R + [\alpha]S \rangle$$

*are different.*

*Proof.* The subgroups have order $2^n$, since $R$ has order $2^n$, and $R$ and $S$ are linearly independent. Then if the subgroups are the same, we must have some $\lambda$ such that

$$[\lambda]R + [\lambda\alpha]S = R + [\alpha]S + [2^{n-1}]S.$$

By the linear independence of $R$ and $S$, we can compare coefficients and conclude that $\lambda = 1$, and that $[2^{n-1}]S = O$, which implies that $S$ has order a factor of $2^{n-1}$, which is a contradiction. $\square$

Finally, we address the fourth condition. We need that

$$e_{2^n}([a]R + [b]S, [c]R + [d]S) = e_{2^n}(R, S)^{ad-bc} = e_{2^n}(P_A, Q_A)^{3^m}.$$

The idea is that we can mask the points chosen from the attack above to satisfy the fourth condition. Recall that the points we wish to send to Alice are

$$(R', S') = (R - [2^{n-i-1}K_i]S, [1 + 2^{n-i-1}]S).$$

Computing the Weil pairing of the two points, we have

$$\begin{aligned}
&e_{2^n}(R', S') \\
&= e_{2^n}(R - [K_i 2^{n-i-1}]S, [1 + 2^{n-i-1}]S) \\
&= e_{2^n}(R, [1 + 2^{n-i-1}]S) \cdot e_{2^n}(-[K_i 2^{n-i-1}]S, [1 + 2^{n-i-1}]S) \\
&= e_{2^n}(R, S)^{1+2^{n-i-1}},
\end{aligned}$$

which is not the correct value. So we choose $\theta$ such that

$$e_{2^n}(\theta R', \theta S') = e_{2^n}(R, S)^{\theta^2(1+2n-i-1)} = e_{2^n}(P_A, Q_A)^{3^m} = e_{2^n}(R, S).$$

Note that $\langle [\theta]R' + [\alpha][\theta]S' \rangle = \langle [\theta](R' + [\alpha]S') \rangle = \langle R' + [\alpha]S' \rangle$ as long as $\theta$ is coprime to the order $2^n$. Hence we need $\theta$ to be the square root of $1 + 2^{n-i-1}$ modulo $2^n$. The following lemma shows that such a square root exists as long as $n - i - 1/geq3$. Note that $\theta$ will be odd, as required.

**Lemma 5.2.2.** *If $a$ is an odd number and $m = 8, 16$, or some higher power of 2, then $a$ is a quadratic residue modulo $m$ if and only if $a \equiv 1 \pmod 8$.*

The condition $n - i - 1 \geq 3$ means we may not be able to launch the attack in an undetected way for the last two bits. This is why we use a brute force method to determine these bits. The attack in the case $(\alpha', 1)$ follows by swapping the roles of $R$ and $S$.

**Algorithm 1:** Adaptive attack using oracle $O(E, R, S, E')$

**Data:** $n, E, P_A, Q_A, P_B, Q_B, E_A, \phi_A(P_B), \phi_A(Q_B)$
**Result:** $\alpha$

Set $K_0 \leftarrow 0$;
**for** $i \leftarrow 0$ **to** $n-3$ **do**
  Set $\alpha_i \leftarrow 0$;
  Choose random $(b_1, b_2)$;
  Set $G_B \leftarrow \langle [b_1]P_B + [b_2]Q_B \rangle$;
  Set $E_B \leftarrow E/G_B$ and let $\phi_B : E \to E_B$ be the isogeny with kernel $G_B$;
  Set $(R, S) \leftarrow (\phi_B(P_A), \phi_B(Q_A))$;
  Set $E_{AB} \leftarrow E_A / \langle [b_1]\phi_A(P_B) + [b_2]\phi_A(Q_B) \rangle$;
  Set $\theta \leftarrow \sqrt{(1 + 2^{n-i-1})^{-1}} \pmod{2^n}$;
  Query the oracle on $(E_B, [\theta](R - [2^{n-i-1}K_i]S), [\theta][1 + 2^{n-i-1}]S, E_{AB})$;
  **if** *Response is false* **then**
    $\alpha_i = 1$
  **end**
  Set $K_{i+1} \leftarrow K_i + 2^i \alpha_i$;
**end**
Brute force $\alpha_{n-2}, \alpha_{n-1}$ using $E$ and $E_A$ and $K_{n-2} = \alpha \pmod{2^{n-2}}$ to find $\alpha$(this requires no oracle calls);
Return $\alpha$;

## 5.3 Complexity of the Attack

The attack requires fewer than $n \approx 1/2 log_2(p)$ interactions with Alice. This seems close to optimal for the second attack model, where the attacker only gets one bit of information at each query. One can reduce the number of queries by doing more computation (increasing the range of the brute-force search).

## 5.4 Countermeasures

Kirkwood et al. introduced a method to secure the key exchange protocol of isogeny cryptosystems. This is based on the Fujisaki–Okamoto transform [FO13] which is also explained by Peikert [Pei14, §5.2] and Galbraith et al. [GPST16, §2.3]. The method allows for one party to validate the other, but for the ease of exposition, let us suppose that Alice is using a static secret and Bob needs to prove to her that he is performing the protocol correctly.

Bob would prove to Alice that he performed the protocol correctly by executing the key exchange, encrypting the random seed used to generate his private key and sending this ciphertext to Alice for her to verify that the random seed leads to the correct keys.

Applied to the Jao–De Feo protocol, we will briefly explain how Bob can prove to Alice that he has executed the protocol correctly. This is especially applicable if Alice is using a static key and Bob is potentially a malicious party.

1. Alice computes and sends the public key $(E_A, \phi_A(P_B), \phi_A(Q_B))$.

2. Bob receives Alice's public key.

3. Bob obtains his random seed $r_B$ from a random source and derives his private key using a key derivation function, $KDF_1$,

   $$(b_1, b_2) = KDF_1(r_B).$$

   He uses the secret key to compute $GB = \langle [b_1]P_B + [b_2]Q_B \rangle$, and uses the Vélu formula to compute $\phi_B$ and $E_B = E/G_B$.

4. Bob derives the shared secret $SS_B = j(E_{AB})$ using his private key and Alice's public key. He then computes a session key $(SK)$ and a validation key $(VK)$ using a key derivation function, $KDF_2$,

   $$SK|VK = KDF_2(j(E_{AB})).$$

5. Bob sends his public key $(E_B, \phi_B(P_A), \phi_B(Q_A))$ and $c_B = Enc_{VK}(r_B \oplus SK)$ to Alice.

6. Using her private key and Bob's public key, Alice computes the shared secret $SSA = j(E'_{AB})$ and derives the session and validation keys $SK'$ and $VK'$. She uses these to compute

$$r'_B = Dec_{VK'}(c_B \oplus SK'.$$

   She then computes Bob's secret keys from $r'_B$ and recomputes all of Bob's operations and compares $(E'_B, \phi'_B(P_A), \phi'_B(Q_A))$ with $(E_B, \phi_B(P_A), \phi_B(Q_A))$.If they are equal, then Alice verifies that Bob has computed the protocol correctly and proceeds to use $SK' = SK$ for future communication with Bob. Else, the protocol terminates in a non-accepting state.

This validation method can be used for both the key exchange and the encryption protocols. It also compels one party to reveal the secret used and so requires a change in secret keys after each verification

# Chapter 6

# Torsion-point Attacks

## 6.1 Christophe Petit's Attack

The idea of Petit's attack is to reduce the SSI-T problem to the following problem:

**Problem 6.1.1.** *Let $p$ be a prime and let $E$ be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. Let $\phi$ be a non scalar endomorphism of $E$ with smooth degree $A$. Let $B$ be a smooth integer with $gcd(A, B) = 1$, and let $P, Q$ be a basis of $E[B]$. Let $R$ be a subring of $End(E)$ that is either easy to compute, or given. Given $E, P, Q, \phi(P), \phi(Q), deg\phi, R$, compute $\phi$.*

Then for the reduced problem use the following algorithm.

From what is given in the problem we can compute the image of $\phi$ on any point in $E[B]$. Let $\theta_1, \theta_2 \in R$ be known endomorphisms of $E$, to which we associate another endomorphism

$$\psi := \theta_1\phi + \theta_2.$$

We can evaluate $\psi$ on any point of $E[B]$ since we konw $\theta_1, \theta_2$ and the action of $\phi$ on $E_B$.

Let us assume that the maps $\theta_1, \theta_2$ are chosen such that $deg\psi = A'B$ for some $A' \in \mathbb{Z}$. An algorithm to achieve this depends on $R$. Now $\psi$ can be written as:

$$\psi = \psi_{A'}\psi_B$$

with $\psi_{A'}$ and $\psi_B$ respectively of degrees $A'$ and $B$.

**Algorithm 2:** Computing an Endomorphism from Additional Information

**Data:** As in 6.1.1, plus parameter $C$

**Result:** A description of $\phi$ as a composition of low degree maps.

1 Find $A' \in \mathbb{N}$ and $\theta_1, \theta_2 \in R$ such that $deg(\theta_1\phi + \theta_2$=A'B and $gcd(deg\theta_1, A) = 1$, and such that $A'$ is $C$-smooth and as small as possible.

2 Compute $ker\psi_B$ using the additional information, where $\theta_1\phi + \theta_2 = \psi_{A'}\psi_B$ and $\psi_{A'}, \psi_B$ are respectively of degrees $A'$ and $B$.

3 Compute $\psi_{A'}$ using a meet-in-the-middle approach.

4 Compute $\ker\phi = ker(\phi_1^{-1}(\psi_{A'}\psi_B - \theta_2))$ by evaluating al maps on the $A$ torsion.

5 Compute $\phi$ from $ker\phi$

By computing $\psi$ on a basis of $E[B]$ and solving some discrete logarithm problems in $E[B]$ we deduce the kernel of $\psi_B$ and then deduce $\psi_B$ itself.

At this point, the map $\psi_{A'}$ is an isogeny of degree $A'$ between two known j-invariants, namely the curve image of $\psi_B$ and the original curve $E$. We recover this isogeny using the meet-in-the-middle approach. Thus we have computed $\psi = \psi_{A'}\psi_B$ we express $\phi$ as $\theta_1^{-1}(\psi_{A'}\psi_B - \theta_2)$, and assuming $gcd(deg\theta_1, A) = 1$ we evaluate this map on the $A'$ torsion to identify $ker\phi$.

The reduction from SSI-T to Problem6.1.1 is the following. For any known endomorphism $\theta \in End(E_0$ and $d \in \mathbb{Z}$ we can consider the endomorphism $\tau = \phi\theta\hat{\phi} + [d] \in End(E)$. Moreover if $\theta$ is non scalar then $\tau$ is also non scalar. Using our knowledge of how $\phi$ acts on the $B$ torsion we can also evaluate $\tau$ on the $B$ torsion, and hence apply the aforementioned techniques. Once we have an expression for $\tau$ we can use it to evaluate $\phi\theta\hat{\phi}$ on the $A$ torsion. Since $A$ is smooth an easy discrete logarithm computation gives generators for $G := ker(\phi\theta\hat{\phi}) \cap E[A]$. This group contains $ker\hat{\phi}$ as a cyclic subgroup of order $A$. When it is cyclic we directly recover $ker\hat{\phi}$ and deduce $\phi$.

When $G$ is not cyclic, let $M|A$ be the largest integer such that $E[M] \subset G$. The isogeny $\phi : E_0 \to E$ can be decomposed as an isogeny of $\phi_M : E_0 \to E_M$ of degree $M$, and a second isogeny of degree $A/M$ from $E_M$ to $E$. We denote by $\phi_{A/M}$ the dual of this second isogeny.

**Lemma 6.1.2.** *We have* $ker(\phi_{A/M} = M(ker \left(\phi\theta\hat{\phi} \cap E[A]\right)$.

*Proof.* Clearly $ker\phi_{A/M} = Mker\hat{\phi}$. The later is a cyclic subgroup of $M(ker\left(\phi\theta\hat{\phi}\cap E[A]\right)$ of order $A/M$. By our definition of M, the group $M(ker\left(\phi\theta\hat{\phi}\cap E[A]\right)$ is cyclic, hence equal to $Mker\hat{\phi}$ as well. □

**Lemma 6.1.3.** *We have $\theta(ker\phi_M) = ker\phi_M$.*

*Proof.* Equivalently, we want to prove $\theta^{-1}(ker\phi_M) = ker(\phi_M)$. We have $ker\phi_M = ker\phi \cap E_0[M] = \hat{\phi}(E[M])$ and similarly $\theta^{-1}(ker\phi_M) = \theta^{-1}(ker\phi)\cap E_0[M] = ker(\phi\theta)\cap E_0[M]$, so we can rephrase the lemma as $\hat{\phi}(E[M]) = ker(\phi\theta)\cap E_0[M]$.

Since $\hat{\phi}(E[A])$ is cyclic, so is $\hat{\theta}(E[M])$. Therefore $E[M] \subset ker(\phi\theta\hat{\phi})\cap E[M]$ if and only if $\hat{\phi}(E[M]) \subset ker\phi\theta$.

By defintion of $M$ we have $E[M] \subset ker(\phi\theta\hat{\phi})\cap E[M]$ so $\hat{\phi}(E[M]) \subset ker\phi\theta$. Moreover $M$ is the largest such integer and $\hat{\phi}(E[M])$ is cyclic, so the equality holds. □

**Lemma 6.1.4.** *Let $k$ be the number of distinct prime factors of $M$ . Then there are at most $2^k$ cyclic subgroups $H$ of order $M$ in $E_0[M]$ such that $\theta(H) = H$.*

*Proof.* Let $\{P, Q\}$ be a basis for $E_0[M]$, and let $\alpha, \beta$ be integers such that$ker\phi_M = \langle\alpha P + \beta Q\rangle$. We have $gcd(\alpha, \beta, M) = 1$. The action of $\theta$ on $E_0[M]$ can be described by a matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{Z}_M)$ such that $\theta(P) = aP + bQ$ and $\theta(Q) = cP + dQ$. Moreover we have $det(m) = ad - bc = deg\theta mod M$ and $Tr(m) = a + d = Tr(\phi) mod M$.

The condition $\theta(ker\phi_M) = ker\phi_M$ now becomes

$$\langle\alpha P + \beta Q\rangle = \langle(a\alpha + c\beta)P + (b\alpha + d\beta)Q\rangle$$

or equivalently

$$(a\alpha + c\beta)\beta = (b\alpha + d\beta)\alpha \quad modM,$$

or

$$c\beta^2 + (a - d)\alpha\beta - b\alpha^2 = 0 \quad modM.$$

Which has solutions if and only if the discriminant

$$(a - d)^2 - 4bc = (Tr(\theta)^2 - 4deg\theta \quad modM$$

is a quadratic residue, and this is the case by assumption. Clearly there are at most two solutions modulo any prime $l|M$, and by Hensel's lifting lemma a solution modulo a prime $l|M$ determines a unique solution modulo any power of $l$ dividing $M$. □

When $A$ is smooth, the proof implicitly provides an efficient algorithm to identify all the candidate kernels. When $A$ is a prime power then $k$ is at most one, and we are done. For powersmooth numbers the expected value of $k$ is small enough to allow a polynomial time exhaustive search of all candidate kernels.

**Remark 6.1.5.** *The problem with this attack is that we simply can't expect there to be suitable pairs $(\theta, d)$ when $A$ and $B$ are of comparable size.*

## 6.2 Castryck-Decru Attack

The attack by Wouter Castryck and Thomas Decru takes as input the parameters of a version of SIDH submitted to NIST:

1. a prime $p = 2^a 3^b f - 1$ for integers $a \geq 2, b, f \geq 1$ with $2^a \approx 3^b$,
2. an elliptic curve $E_0/\mathbb{F}_{p^2}$ with $\#E_0(\mathbb{F}_{p^2}) = (p+1)^2$,
3. generators $P_0, Q_0$ of $E_0[2^a]$,
4. a $3^\beta$-isogeny $\tau : E_0 \to E_{start}$ for some $\beta \geq 0$, where $E_{start}$ is one of the two curves that have served as starting curves in SIKE,
5. the codomain $E_B/\mathbb{F}_{p^2}$ of a secret cyclic $3^b$-isogeny $\phi : E_0 \to E_B$,
6. the generators $P = \phi(P_0)$ and $Q = \phi(Q_0)$ of $E[2^a]$

and returns the isogeny $\phi$.

Suppose that $2^a > 3^b$ and let $c = 2^a - 3^b$. Assume that we can compute the images $P_c = \gamma(P_0)$ and $Q_c = \gamma(Q_0)$ under an arbitrary c-isogeny $\gamma : E_0 \to C$ to some codomain curve $C$.

Let $x \in \mathbb{Z}$ denote a multiplicative inverse of $3^b$ modulo $2^a$. Note that $-x$ is then a multiplicative inverse of $c$ modulo $2^a$.

### 6.2.1 Subgroups built from torsion point information

If there is a $3^b$ isogeny $\phi : E_0 \to E_B$ such that $\phi(P_0) = P$ and $\phi(Q_0) = Q$ then we consider the isogeny

$$\psi = [-1] \circ \phi \circ \hat{\gamma} : C \to E_B,$$

where we not that $\psi(P_c) = -cP$ and $\psi(Q_c) = -cQ$. For all $R, S \in C[2^a]$ we have that

$$e_{2^a}(x\psi(R), x\psi(S)) = e_{2^a}(R, S)^{x^2 c 3^b} = e_{2^a}(R, S)^{-1}.$$

This implies that the group

$$\langle (P_c, x\psi(P_c)), (Q_c, x\psi(Q_c)) \rangle = \langle (P_c, P), (Q_c, Q) \rangle \tag{6.1}$$

is maximally isotropic with respect to the $2^a$-Weil pairing on the product $C \times E$. Indeed,

$$e_{2^a}((P_c, x\psi(P_c)), (Q_c, x\psi(Q_c))) = e_{2^a}(P_c, Q_c) e_{2^a}(x\psi(P_c), x\psi(Q_c)) = 1$$

because the Weil pairing on $C \times E$ is just the product of the Weil pairings of the corresponding components. Therefore it concerns the kernel of a $(2^a, 2^a)$-isogeny of principally polarised abelian surfaces. By writing this isogeny as a composition of $(2, 2)$-isogenies, it can be viewed as a walk of length $a$ in the $(2, 2)$-isogeny graph of superspecial principally polarised abelian surfaces over $\bar{\mathbb{F}}_p$, all of whose vertices are defined over $\mathbb{F}_{p^2}$.

These vertices come in two types: about $p^2/288$ products of supersingular elliptic curves and about $p^3/2880$ Jacobians of superspecial genus 2 curves [17]. Therefore it is to be expected that most isogenies in the chain are between Jacobians of genus 2 curves, and such isogenies can be computed efficiently using "classical" formulae due to Richelot . But the first step is clearly an exception to this: with overwhelming probability, this is a "gluing" step, mapping the product $C \times E$ to a Jacobian. And by Kani's theorem the codomain of our $(2^a, 2^a)$-isogeny is a product of elliptic curves. The attack uses this as a decision tool to build $\phi$ as the composition of small degree isogenies.

### 6.2.2 Iteration

For simplicity we assume that the base curve $E_0$ coincides with $E_{start}$(this is the case in SIKE). In the general case, one should just replace the maps $\hat{K}_i : E_i \to E_0$ below with their compositions with $\tau$.

Choose $\beta_i \geq 1$ minimal such that there exists some $\alpha_i \geq 0$ for which

$$c_i = 2^{a-\alpha_i} - 3^{b-\beta_i}$$

is of the form $u_i^2 + 4v_i^2$. Write $\phi = \phi_i \circ \kappa_i \circ \cdots \circ \kappa 2 \circ \kappa_1$ with $\kappa_i$ a $3^{\beta_i - \beta i - 1}$-isogeny with $\beta_0 = 0$. To an attacker, there are a priori $3^{\beta_i - \beta i - 1}$ options for $\kappa_i$. For each of these options, we can run our decision algorithm.

For simplicity write $K_i = \kappa_i \circ \cdots \circ \kappa_2 \circ \kappa_1$ Let $E_i$ be the codomain of $K_i(E_0)$. Let $P_i = K_i(2^{\alpha_i} P_0)$ and $Q_i = K_i(2^{\alpha_i} Q_0)$ be the generators of $E_i[2^{a-\alpha_i}]$. If the guess is correct then $E$ is the codomain of an unknown isogeny $\phi_i : E_i \to E$ of degree $3^{b-\beta_i}$.

$\gamma_i^{start} = [u_i] + [v_i] \circ 2i$ is an easy-to-evaluate degree-$c$ endomorphism of $E_0$. Then in order to find $\gamma_i : E_i \to C_i$ degree $c_i$ isogeny to arbitrary $C_i$ curve, we use $\hat{K}_i$. Let $\tilde{K}_i : E_0 \to C_i$ be the isogeny with kernel $\gamma_i^{start}(\hat{K}_i(E_i[3^{\beta_i}])) = \gamma_i^{start}(kerK_i)$. Then $\hat{\tilde{K}}_i \circ \gamma_i^{start} \circ \hat{K}_i : E_i \to C_i$ is a $3^{2\beta_i} c_i$-isogeny vanishing on $E_i[3^{\beta_i}]$, so it factors over $[3^{\beta_i}]$ and we can let

$$\gamma_i = \frac{\hat{\tilde{K}}_i \circ \gamma_i^{start} \circ \hat{K}_i}{3^{\beta_i}}.$$

It is easy to evaluate $\gamma_i$ on our $2^{a-\alpha_i}$-torsion points $P_i$ and $Q_i$. We have that $kerK_i \subset E_0[3^b] \subset E_0(\mathbb{F}_{p^2})$. So we can explicitly write down a generator $T \in E_0(\mathbb{F}_{p^2})$ of $kerK_i$ and compute the isogeny $\hat{\tilde{K}}_i$ with kernel $\langle \gamma_i^{start}(T) \rangle$. Evaluating $\gamma_i$ in our $2^{a-\alpha_i}$-torsion points $P_i$ and $Q_i$ is then simply done by

$$P_{c_i} = 2^{\alpha_i} \hat{\tilde{K}}_i \gamma_i^{start}(P_0), \quad Q_{c_i} = 2^{\alpha_i} \hat{\tilde{K}}_i \gamma_i^{start}(Q_0).$$

Then we have that the following diagram.

$$\begin{tikzcd}
E_0 \arrow[loop left, "\gamma_i^{start}"] \arrow[rrrr, "\phi"] \arrow[dr, "\kappa_1"] \arrow[drrr, "K_i"] \arrow[dd, "\tilde{K}_i"'] & & & & E_B \\
& E_1 \arrow[r, "\kappa_1"] & \dots \arrow[r, "\kappa_i"] & E_i \arrow[urr, "\phi_i"] \arrow[dlll, "\gamma_i"] & \\
C_i & & & &
\end{tikzcd}$$

And we have

$$\begin{tikzcd} C_i \arrow[r, "\hat{\gamma}_i"] \arrow[d] \arrow[dr, "\phi_i \circ \hat{\gamma}_i"] & E_i \arrow[d, "\phi_i"] \\ F_i \arrow[r] & E_B \end{tikzcd}$$

By Kani's theorem there is a $deg\hat{\gamma}_i + deg\phi_i = 2^{a-\alpha_i}$-isogeny $\Phi : C_i \times E_B \to E_i \times F_i$. As we have shown earlier this isogeny has kernel

$$\begin{aligned} &\langle ([c_i]P_{c_i}, \phi_i \circ \hat{\gamma}_i(P_{c_i})), ([c_i]Q_{c_i}, \phi_i \circ \hat{\gamma}_i(Q_{c_i}))\rangle \\ &= \langle (P_{c_i}, x_i\psi_i(P_{c_i})), (Q_{c_i}, x_i\psi_i(Q_{c_i}))\rangle \\ &= \langle (P_{c_i}, 2^{\alpha_i}P), (Q_{c_i}, 2^{\alpha_i}Q)\rangle \end{aligned}$$

We calculate $\Phi$ and check if it realy is an isogeny between products of elliptic curves. This is done by computing the corresponding chain of $(2, 2)$-isogenies. With overwhelming probability, the first $a-\alpha_i-1$ steps in this chain amount to one gluing step followed by $a-\alpha_i-2$ Richelot isogenies between Jacobians of genus 2 curves. An easy "$\delta = 0$ test" then checks whether or not the last step splits.

If the test fails, then we try again with a different guess for $\kappa_i$. We remark that, even in the case of a wrong guess, the subgroup is always maximally isotropic with respect to the Weil pairing, so this is not the way in which one can detect having taken the wrong direction: one really has to perform the gluing and its successive Richelot walk.

### 6.2.3 Polynomial runtime

As $x \to \infty$, the number of integers $c$ in the interval $[0, x]$ that admit a decomposition of the form $c = u^2 + 4v^2$ is asymptotic to

$$\frac{0.5731\ldots}{\sqrt{lnx}}x$$

by (a variation on) a theorem of Landau, see [18]. We can use this to estimate the probability that our strategy in constructing an isogeny $\gamma : E_0 \to C$ of degree $c = 2^a - 3^b$: it is about $0.5731/\sqrt{aln2} \approx 0.6884/\sqrt{a}$.

Let us now revisit the first iteration of our key recovery, where we choose $\beta_1 \geq 1$ such that there exists an $\alpha_1 \geq 0$ for which $c_1 = 2^{a-\alpha_1} - 3^{b-\beta_1}$ is of the form $u_1^2 + 4v_1^2$. In view of Landau's theorem, we expect that we should try in the order of $\sqrt{a}$ pairs $(\alpha_1, \beta_1)$ before we succeed. So the smallest $\beta_1$ is expected to be of magnitude $\sqrt[4]{a}$. While this is good enough for breaking the concrete parameter sets of SIKE, the asymptotic runtime is $L_p(1/4)$ rather than polynomial: indeed, there are $3^{\beta_1}$ options for $\kappa_1$ to guess from.

**Remark 6.2.1.** *The first iteration dominates the overall runtime. Indeed, once suitable $\alpha_1, \beta_1$ are found, the expression $2^{a-\alpha_1} - 3^{b-\beta_1}$ can be recycled in the remaining iterations by extending Bob's secret isogeny. We can prolong Bob's secret isogeny with an arbitrary 3-isogeny $\phi'$ and let $P' = \phi'(P)$ and $Q' = \phi'(Q)$. Treating $\phi' \circ \phi_B$ as the new secret isogeny, the relevant expression now becomes $2^{a-\alpha_1} - 3^{b+1-\beta_1}$. We can now use our attack to determine Bob's secret key modulo $3^{\beta_1}$.*

To achieve a polynomial time complexity, we extend the attack from sums of squares to more general quadratic forms and hope that there is a prime number $n \leq a$ such that $c_1$ can be written as $u_1^2 + nv_1^2$. Heuristically, this happens with overwhelming probability. We can loosely argue this as follows. Based on a generalization of Landau's theorem, see again [18], for every $n$ the success probability remains inversely proportional to $\sqrt{a}$. If the events of being of the form $u_1^2 + nv_1^2$ are "sufficiently independent" as $n$ varies, and if the implicit constants do not decay too quickly, then the probability of failure overall is in the order of

$$\left(1 - \frac{1}{\sqrt{a}}\right)^{\pi(a)} \approx \left(1 - \frac{1}{\sqrt{a}}\right)^{a/lna}$$

which decreases as $e^{-\sqrt{a}/lna}$ (here $\pi$ is the prime-counting function). In particular, we expect that we can simply take $\beta_1 = 1$ in this case.

Once such a decomposition $u_1^2 + nv_1^2$ is found, we proceed as follows. The techniques from Love and Boneh [19] allow for the polynomial-time construction of an isogeny $\nu : E_{start} \to N_{start}$, where $N_{start}$ is an elliptic curve possessing an endomorphism $\sqrt{n}i$ satisfying $\sqrt{n}i \circ \sqrt{n}i = [-n]$. Thus we can consider the degree-$c$ endomorphism $\gamma^{start} = [u_1] + \sqrt{n}i \circ [v_1]$ on $N_{start}$. This endomorphism can be transformed into the desired degree-$c$ isogeny $\gamma : E_0 \to C$ along $\nu \circ \tau : E_0 \to N_{start}$, as we have done before with $\gamma_i$ and $\gamma_i^{start}$

## 6.3 Maino-Martindale-Panny-Pope-Wesolowski Attack

### 6.3.1 Core of the attack

Suppose that $A > B$, and that we have access to some isogeny $\phi_c : E \to E_0$ of degree $c = A - B$, given in any form that allows to evaluate it on the $A$-torsion. We postpone the discussion on finding such a $\phi_c$ as the method may depend on the context. Assuming $\phi_c$ is provided, we give an algorithm that recovers a generator of $ker(\phi_B)$, at a cost dominated by one evaluation of a $(A, A)$-isogeny with known kernel (with a $B - torsionpointasinput$), and two evaluations of $\hat{\phi}_c$ (with two $A$-torsion points as input).

Let $\psi_B : E \to F$ be the isogeny with kernel $\hat{\phi}_c(ker(\phi_B))$, and $\psi_c : F \to E_B$ be the isogeny with kernel $\psi_B(ker(\phi_c))$, so that the following diagram commutes:

$$\begin{tikzcd}
E_0 \arrow[r, "\phi_B"] & E_B \\
E \arrow[u, "\phi_c"] \arrow[ur, "\phi"] \arrow[r, "\psi_B"'] & F \arrow[u, "\psi_c"']
\end{tikzcd}$$

Then by Kani's theorem $\Phi = \begin{pmatrix} \phi_c & \hat{\phi}_B \\ -\psi_B & \hat{\psi}_c \end{pmatrix}$ is an $(A, A)$-isogeny $\Phi : E \times E_B \to E_0 \times F$ with kernel $ker(\Phi) = \{[B]P, \phi(P) | P \in E[2^a]\}$.

Observe that $-\hat{\phi}_B$ is equal to the composition

$$E_B \xrightarrow{0 \times id_{E_B}} E \times E_B \xrightarrow{\Phi} E_0 \times F \xrightarrow{pr_1} E_0$$

where the first map is the inclusion map with image $\{0\} \times E_B$, the middle map is $\Phi$, and the last is the natural projection map. Assuming that each map in this composition is efficiently computable, then we can evaluate $\hat{\phi}_B$ on any input. That directly leads to a recovery of $ker(\phi_B)$. The difficulty is in proving that each step is indeed efficiently computable. The computation of the first inclusion is trivial. The step $\Phi$ requires a delicate analysis of this 2-dimensional isogeny, to prove that its kernel can be computed, and that this kernel permits an efficient evaluation of $\Phi$. The last step, the projection, may seem clear, but in fact hides a subtlety. The decomposition $E_0 \times F$ is only available if $\Phi$ is of a certain kind: it must behave well with respect to the implicit product polarisations of the domain and codomain.

### 6.3.2 Case of known endomorphism ring

In the case of known endomorphism ring we can find $\phi_c$ efficiently.The idea is the following: first, find an ideal $I$ in $End(E_0)$ of norm $c$ . Then, assuming the generalised Riemann hypothesis, one can find the codomain of $\phi = \phi_I$ : $E_0 \to E_B$ and evaluate $\phi$ on any input using [20] lemma 3.3.

---

**Algorithm 3:** Finding an ideal of prescribed norm.

---

**Data:** A basis $(\alpha_i)_{i=1}^4$ of $End(E_0$ in efficient representation, and an integer $c$ coprime to 2 and p.

**Result:** A left ideal $I$ of norm $c$ in $End(E_0)$

1 Find a solution of $deg(\alpha_0) = z_0^2 c$ with $\alpha_0 \in End(E_0)$ and $z_0 \in \mathbb{Z}$. It is a homogeneous quadratic equptions of dimension 5, so can be solved in polynomial time.

2 Deduce another solution $(\alpha, z)$ for which $z$ is coprime with $c$, using the thechnique... Return $I = End(E_0)\alpha + End(E_0)c$.

---

Finding the ideal $I$ requires more explanation. First observe that the problem reduces to the case where $c$ is coprime to $2p$: write $c = 2ip^i c'$ with $(c', 2p) = 1$, solve the problem for $c'$, and then compose the resulting isogeny with $i$ isogenies of degree 2 and $j$ Frobenius isogenies. The steps to find $I$ are then given in Algorithm 3. Let us explain Step (2). Finding the desired solution heuristically is simple, so the motivation of the following discussion is mostly to get a provable method. Write the solutions $(\alpha, z)$ in the form $(x, z) \in \mathbb{Z}^4 \times \mathbb{Z}$, where $x$ represents the coefficients of $\alpha$ in the provided basis of $End(E_0)$. The equation can then be written as $x^T G x = z^2 c$ , or $x^T Q x = 0$, where $G$ is the Gram matrix of the basis, and $Q = G \oplus \langle -c \rangle$ (the $5 \times 5$ matrix with $G$ in the upper-left corner, $-c$ in the lower-right corner, and zeros elsewhere). Note that we can assume that $x_0$ (the vector of coordinates of $\alpha_0$) is primitive (i.e., the greatest common divisor of its coefficients is 1) and $z_0 \in \mathbb{Z} > 0$. We are looking for another solution where $x$ is coprime with $c$ . The rest of the proof reproduces mutatis mutandi the technique of ([21], Algorithm 7, Step 3). From ([22], Proposition 6.3.2), the general solution

$X = (x, z)$ is given by

$$X = d((R^T QR)X_0 - 2(R^T QX_0)R),$$

for arbitrary $R \in \mathbb{Q}^5$ and $d \in \mathbb{Q}^*$, where $X_0 = (x_0, z_0)$ is our initial solution. Fix $d = 1$. Write $R = (r_x, r_z)$ with $r_x \in \mathbb{Z}^4$ and $r_z \in \mathbb{Z}$. The last coordinate of $X$ is given by the integral quadratic form

$$r_x^T G r_x z_0 - 2r_x^T G x_0 r_z + f z_0 r_z^2 = \frac{(r_x z_0 - x_0 r_z)^T G (r_x z_0 - x_0 r_z)}{z_0}.$$

It is of rank 4, so let $M \in M_{4\times4}(\mathbb{Z})$ be a matrix whose columns generate $\Lambda = z_0\mathbb{Z}^4 + x_0\mathbb{Z}$, and

$$g(v) = \frac{v^T(M^T GM)v}{z_0}$$

It is positive definite, since $G$ is and $z_0 > 0$. Let us show that $g$ is (almost) primitive. If $s$ is a prime that does not divide $z_0$, both $M$ and $z_0$ are invertible modulo $s$, so $g$ is primitive at $s$ because $G$ is. Now suppose $s|z_0$. Then, writing $Mv = r_x z_0 - x_0 r_z$ , we have

$$g(v) \equiv -2r_x^T G x_0 r_z \pmod{s}.$$

Therefore, if $s \neq 2$ and $Gx_0 \not\equiv 0 \pmod{s}$, then $g$ is primitive at $s$. If $Gx_0 \equiv 0 \pmod{s}$, since $x_0$ is primitive, $s$ must divide $disc(G)$, so $s$ is 2 or $p$. This proves that the only primes where $g$ might not be primitive are 2 and $p$. We can then write $g = g'/a$ where $g'$ is primitive and a may only be divisible by the primes 2 and $p$. Applying ([21], Proposition 3.6), we can find in polynomial time a $v$ such that $z' = g'(v)$ is a prime larger than $c$ . With $z = az'$, we obtain a solution of $x^T Gx = cz^2$. Since $c$ is coprime to $2p$, it is also coprime to $z$.

## 6.4 Damien Robert's Attack

### 6.4.1 Dimension 8 attack

Suppose that $A > B$, let $c = A - B$. Every integer can be written as the sum of four squares so write $c = c_1^2 + c_2^2 + c_3^2 + c_4^2$ and let $M \in M_{4\times4}(\mathbb{Z})$ a

$4 \times 4$ matrix such that $M^T M = cId$. Explicitly:

$$M = \begin{pmatrix} c_1 & -c_2 & -c_3 & -c_4 \\ c_2 & c_1 & c_4 & -c_3 \\ c_3 & -c_4 & c_1 & c_2 \\ c_4 & c_3 & -c_2 & c_1 \end{pmatrix}$$

the matrix of the multiplication of $c_1 + c_2 i + c_3 j + c_4 k$ in the standard quaternion algebra $\mathbb{Z}[i,j,k]$. Let $\gamma_0$ be the endomorphism on $E_0^4$ given matricially by $M$. The dual with respect to the product principal polarisation) $\tilde{\gamma}_0$ of $\gamma_0$ is given matricially by $M^T$(since integer multiplications are their own dual), so $\tilde{\gamma}_0 \gamma_0 = cId$, hence $\gamma_0$ is a $c$-isogeny, which can be evaluated in $O(logc)$ arithmetic operations. We let $\gamma_B$ be the endomorphism of $E_B^4$ given by the same matrix $M$, and by abuse of notation we denote by $\phi_B Id : E_0^4 \to E^4)B$ the diagonal embedding of $\phi_B : E_0 \to E_B$. We remark that since $\gamma_0$ is given by an integral matrix, it commutes with $\phi_B$ in the sense that we have the equation: $\phi_B \gamma_0 = \gamma_B \phi_B$:

$$\begin{tikzcd} E_0^4 \arrow[r, "\phi_B Id"] \arrow[d, "\gamma_0"'] & E_B^4 \arrow[d, "\gamma_B"] \\ E_0^4 \arrow[r, "\phi_B Id"'] & E_B^4 \end{tikzcd}$$

Then we have by Kani's theorem that $\Phi = \begin{pmatrix} \gamma_0 & \hat{\phi}_B Id \\ -\Phi_B Id & \hat{\gamma}_B \end{pmatrix}$ is a degree $A$ endomorphism on the 8-dimensional abelian variety $X = E_0^4 \times E_B^4$.

**Remark 6.4.1.** *We can reach this conclusion without Kani, just by calculating* $\Phi\hat{\Phi}$.

Since $c$ is prime to $A$, the kernel of $\Phi$ is exactly the image of $\hat{\Phi}$ on $E_0^4[A] \times \{0\}$, so we immediately get the 8 generators of the kernel of $\Phi$. This step costs $O(logc)$ arithmetic operations in $E_0(\mathbb{F}_q)$.

We can then compute $\Phi$ (on any point $P \in X(\mathbb{F}_q)$) using an isogeny algorithm in dimension 8, decomposing the $A$-endomorphism $\Phi$ as a chain of $l$-isogeny for $l$ the prime factors of $A$. Thus we can evaluate $\Phi$ on any point of $X$, so we can evaluate $\Phi$ or $\hat{\Phi}$ on any point of $E_0$ (resp. $E_B$). We can now recover the kernel of $\phi_B$ on $E_0$ as the image of $\hat{\phi}_B$ on $E_B[B]$. If $(P_B, Q_B)$ is a basis of $E_B[B]$, we compute $P'_B = \hat{\phi}_B(P_B)$ and $Q'_B = \hat{\phi}_B(Q_B)$ by evaluating $\Phi$ on the points $(0,0,0,0,P_B,0,0,0)$ and $(0,0,0,0,Q_B,0,0,0)$, and the kernel of $\phi_B$ is generated by whichever has order $B$. This step costs $O(\omega(B) log B)$ operations in $E_0(\mathbb{F}_q)$, where $\omega(B)$ is the number of distinct prime divisors of $B$.

**Remark 6.4.2.** *The downside of this attack is that $E_0^4 \times E_B^4$ is not a convenient object to work with. While algorithms for isogenies of abelian varieties are known whose complexity is polynomial in $(log(q), log(A), l_A)$, the complexity remains exponential in the dimension, contributing a massive constant fact ot the cost. This leads as to the dimension 4 attack.*

### 6.4.2 Dimension 4 attack

In dimension 2, we can always write an $a$-endomorphism on $E_0^2$ whenever $a = a_1^2 + a_2^2$. We can do a dimension 4 attack whenever we can find $a, b > 0$ such that $A = bB + a$ and both $a$ and $b$ are a sum of two squares.

Write $a = a_1^2 + a_2^2, b = b_1^2 + b_2^2$. Note that unlike the decomposition as a sum of four squares, these decompositions into a sum of two squares requires the factorisation of $a, b$. Write $\alpha = \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix}, \beta = \begin{pmatrix} b_1 & -b_2 \\ b_2 & b_1 \end{pmatrix}$. These matrices can be interpreted as endomorphisms of $E_0^2$ or $E_B^2$ and commute with $\phi_B Id$ : $\beta_B \phi_B Id = \phi_B Id \beta_0, \quad \alpha_B \phi_B Id = \phi_B Id \alpha_0$. Furthermore,$\alpha\hat{\alpha} = (a_1^2 + a_2^2)Id$, so $\alpha$ is an $a$-endomorphism, and similarly $\beta$ is a $b$-endomorphism:

$$\begin{array}{ccc} E_0^2 & \xrightarrow{\phi_B \beta} & E_B^2 \\ \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha_B} \\ E_0^2 & \xrightarrow[\phi_B \beta]{} & E_B^2 \end{array}$$

Kani's theorem shows that $\Phi = \begin{pmatrix} \alpha_0 & \hat{\phi}_B Id \hat{\beta}_B \\ -\beta_B \phi_B Id & \hat{\alpha}_B \end{pmatrix}$ is a $A = bB + a$-endomorphism of $E_0^2 \times E_B^2$

We can thus evaluate $\Phi$, hence evaluate $\beta_B \phi_B Id = \phi_B Id \beta_0$ on any point in $E_0^2(\mathbb{F}_q)$ in $O(log^2 A + log A l_A^4)$ arithmetic operations over $\mathbb{F}_q$, where $l_A$ is the largest prime divisor of $A$. In this situation we can recover more than just $b\phi_B$. Indeed from the matrix $\beta_B\phi_B Id$ we can directly recover $b_1\phi_B$ and $b_2\phi_B$; so if $b' = gcd(b_1, b_2)$, we can recover $b'\phi_B$ in $O(logb)$ arithmetic operations on $E_B$. This means that we can recover the kernel of a $B/gcd(B, b')$-isogeny $E_0 \to E'_B$ through which $\phi_B$ factors. If $gcd(B, b') = 1$ we have directly recovered $\phi_B$, otherwise we iterate the process, which is possible as long as $gcd(B, b') < B$.

**Remark 6.4.3.** *Under the heuristic that we can tweak the paramaters so that $a = A - bB$ is a sum of two squares with a large probablity the dimension 4 attack has complexity $\tilde{O}(logAl_A^4$. For more detail on parameter tweaking see [5].*

# Chapter 7

# Constructive Applications

## 7.1 SQIsignHD

SQIsignHD[23] is a digital signature sheme derived from SGIsign[24] QIsign uses the Deuring correspondence between supersingular elliptic curves and quaternion orders. This Deuring correspondence is a powerful tool to construct cryptosystems because it is one way: it is easy to turn an order into the corresponding elliptic curve, but the converse direction is the presumably hard supersingular endomorphism ring problem[25]. The new scheme SQIsignHD follows a similar outline as SQIsign, but resolves its main drawbacks by fundamentally reforging the computational approach. Robert's attack[5] allows one to represent an isogeny with its action on a large enough torsion group; from this description, one can efficiently evaluate the isogeny on any other point, regardless of the factorisation pattern of the underlying isogeny.

Below we can find a short description of the protocol:

**Public set-up:** We choose a prime $p$ and a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$ of known endomorphism ring $End(E_0)$ such that $E_0$ has smooth torsion defined over a small extension of $\mathbb{F}_{p^2}$ (of degree 1 or 2). In practice, one may use the curve $E_0 : y^2 = x^3 + x$ (and $p \equiv 3 mod 4$).

**Key generation:** The prover generates a random secret isogeny $\tau : E_0 \to E_A$ of fixed smooth degree $D_\tau$ . Then, the prover publishes $E_A$. Knowing $\tau$, only the prover can compute the endomorphism ring $End(E_A)$.

**Commitment:** The prover generates a random isogeny $\psi : E_0 \to E_1$ of smooth degree $D_\psi$ and returns $E_1$ to the verifier ($\psi$ being secret). The resulting distribution for $E_1$ is as close as possible to the uniform distribution in the supersingular isogeny graph.

**Challenge:** The verifier generates a random isogeny $\phi : E_A \to E_2$ of smooth degree $D_\phi$ sufficiently large for $\phi$ to have high entropy. Then, $\phi$ is sent to the prover.

**Response:** The prover generates an efficient representation of an isogeny $\sigma : E_1 \to E_2$ of small degree $q \approx \sqrt{p}$ and returns it to the verifier.

## 7.2 FESTA

Fast Encryption from Supersingular Torsion Attacks(FESTA)[26] is a public key exchange protocol based on a trapdoor function.

In the trapdoor formulation, the trapdoor key is an isogeny $\phi_A : E_0 \to E_A$ and a random special matrix $A$; the public parameters are the codomain $E_A$, together with the image of a large torsion basis $(P_b, Q_b)$ under $\phi_A$. The image points, before being revealed, are scaled by the matrix $A$, which protects the isogeny $\phi_A$ from the SIDH attacks. The one-way function receives as input two isogenies $\phi_1 : E_0 \to E_1, \phi_2 : E_A \to E_2$, and a random special matrix $B$.

Evaluating the function then consists in computing the images of the torsion basis on $E_0$ and $E_A$ under $\phi_1$ and $\phi_2$, respectively, and scaling them both with the matrix $B$. The matrices $A$ and $B$ are special in the sense that they commute; this is the case, for instance, for diagonal matrices. Commutativity of the matrices is what enables the trapdoor inversion: applying the inverse matrix $A^{-1}$ to scale the points on $E_2$ yields the correct images of the torsion points on $E_1$ under the isogeny $\phi := \phi_2 \circ \phi_A \circ \hat{\phi}_1$. Hence, the SIDH attacks allow the trapdoor holder to recover the function input $\phi_1, \phi_2$, and the matrix $B$, while the attacks are infeasible to anyone who does not know the secret matrix $A$.

# Bibliography

[1] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Paper 2011/506, 2011. `https://eprint.iacr.org/2011/506`.

[2] Ernst Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik*, 1997(485):93–122, 1997.

[3] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh. Cryptology ePrint Archive, Paper 2022/975, 2022. `https://eprint.iacr.org/2022/975`.

[4] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. An attack on sidh with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026, 2022. `https://eprint.iacr.org/2022/1026`.

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

[6] Jacques Vélu. Isogénies entre courbes elliptiques, 1971.

[7] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. Cryptology ePrint Archive, Paper 2016/859, 2016. `https://eprint.iacr.org/2016/859`.

[8] Christophe Petit. Faster algorithms for isogeny problems using torsion point images, 2017.

[9] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[10] Yan Bo Ti. Isogenies of abelian varieties in cryptography. Ph.D. thesis, University of Auckland, 2019.

[11] Benjamin Smith. Explicit endomorphisms and correspondences. Ph.D. thesis, University of Sydney, 2006.

[12] Tetsuji Shioda. *Supersingular K3 surfaces*. Springer, 1979.

[13] Ramarathnam Venkatesan David Jao, Stephen D. Miller. Expander graphs based on grh with an application to elliptic curve cryptography, 2009.

[14] Jean-Francois Mestre. La méthode des graphes. exemples et applications, 1986.

[15] Arnold K. Pizer. Ramanujan grarphs and hecke operators, 1990.

[16] Arnold K. Pizer. Ramanujan grarphs, 1995.

[17] Bradley W. Brock. Superspecial curves of genera two and three. Ph.D. thesis, Princeton University, 1994.

[18] Daniel Shanks and Larry P. Schmid. Variations on a theorem of landau. part i. *Mathematics of Computation*, 20(96):551–569, 1966.

[19] Dan Boneh Jonathan Love. Supersingular curves with small non-integer endomorphisms., 2020.

[20] Tako Boris Fouotsa, Péter Kutas, Simon-Philipp Merz, and Yan Bo Ti. On the isogeny problem with torsion point information. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *Public-Key Cryptography – PKC 2022*, pages 142–161, Cham, 2022. Springer International Publishing.

[21] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent, 2022.

[22] Henri Cohen. *Number Theory: VolumeI: Tools and Diophantine Equations*. Springer Science & Business Media, 2008.

[23] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. Sqisignhd: New dimensions in cryptography. Cryptology ePrint Archive, Paper 2023/436, 2023. https://eprint.iacr.org/2023/436.

[24] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. Journal of Cryptology, 2020.

[25] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion $\ell$-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

[26] Andrea Basso, Luciano Maino, and Giacomo Pope. Festa: Fast encryption from supersingular torsion attacks. Cryptology ePrint Archive, Paper 2023/660, 2023. https://eprint.iacr.org/2023/660.