university of groningen

faculty of science and engineering

mathematics and applied mathematics

Supersingular Isogeny Diffie-Hellman: Finding the Distribution of the Secret Key by Computation of Brandt Matrices

Bachelor's Project Mathematics

July 2018

Student: H.E.H. van der Laan

First supervisor: Dr. M. Derickx

Second assessor: Dr. J.S. Müller

Abstract

Quantum computing poses a threat to classical cryptosystems, so new protocols are needed. One possible candidate to replace currently used key exchange protocols is Supersingular Isogeny Diffie-Hellman (SIDH). The security of SIDH depends on a uniform distribution of the secret key, for which heuristic estimations exist. These heuristics have been verified by Thormarker (2017), via simulation of random walks on isogeny graphs.
This thesis studies the theoretical background of SIDH and investigates the relation between supersingular elliptic curves and quaternion algebras. Through this relation it is shown that the distribution of the secret key in SIDH can be found by computing Brandt matrices. This is then compared to the results from the heuristic estimations.

Contents

1. Introduction

A widely used protocol for establishing a shared secret key between two parties is the elliptic curve Diffie-Hellman key exchange (ECDH). This can for example be used in the classical cryptosystem AES. The safety of this protocol relies on the difficulty of solving the discrete logarithm problem for elliptic curves.

Problem 1 (Discrete logarithm problem for elliptic curves)**.** Let E be an elliptic curve over a finite field K. For $P \in E$ and $Q \in \langle P \rangle$ where $\langle P \rangle \subset E$ is the cyclic subgroup generated by P, find an integer x such that $xP = Q$.

The ECDH protocol allows two parties, say Alice and Bob, to encrypt data with a shared secret key and then share this data via a public channel. They construct this key together, following the Diffie-Hellman method (see [Gal12, chapter 20]). Let $\mathbb{F}_p$ be a finite field of size p. The ECDH protocol is as follows ([Was08, section 6.2]):

1. Alice and Bob choose an elliptic curve $E/\mathbb{F}_p$ so that problem 1 is difficult to solve. They pick a point $P \in E(\mathbb{F}_p)$ of order N.

2. Alice and Bob each choose their respective secret elements $a, b \in \mathbb{Z}/N\mathbb{Z}$. Alice computes aP, Bob computes bP and they publicly share this result with each other.

3. Now Alice computes abP and Bob computes baP. Since $abP = baP$, this can be used as their shared key.

A schematic representation of ECDH is shown in table 1.1. It is believed to be difficult to solve problem 1 using currently existing computers. Once a third party is able to solve this problem, they can also find abP when given P, aP, bP. Possible methods of attack are the Pohlig-Hellman algorithm, Pollard's rho algorithm and the MOV algorithm (see [Tho17, section 3.2]).

	Alice	**Public**	**Bob**
Pick public parameter		$P \in E(\mathbb{F}_p)$	
Pick secret keys	$a \in \mathbb{Z}/N\mathbb{Z}$		$b \in \mathbb{Z}/N\mathbb{Z}$
Generate public keys		aP, bP	
Compute shared key	abP=(ab)P		baP=(ab)P

Table 1.1: Schematic overview of the ECDH protocol. Here $P \in E(\mathbb{F}_p)$ is a point of order N.

Although problem 1 is currently difficult to solve, this may not be the case in the near future due to the development of quantum computers, which use qubits rather than regular bits (see [DPV06, chapter 10]). This danger was first addressed in [Sho97], by the construction of Shor's algorithm. This algorithm can successfully perform a quantum attack on the RSA system in polynomial time. There currently exist several other algorithms that allow quantum computers to break classical cryptosystems in polynomial time.
This indicates a need for encryption methods that are safe from quantum attacks. A potentially quantum-resistant protocol that can replace ECDH is the supersingular isogeny

Diffie-Hellman key exchange (SIDH).
The goal of this thesis is to study the security of SIDH, which depends on the uniformity of the distribution of the generated shared secret in the space of shared secrets. The theoretical basis for a uniform distribution has not yet been proven, but there exist heuristics that show that this distribution is indeed uniform. These heuristics have been verified by simulation by [Tho17] for isogenies of degree 2 and 3. The correspondence between supersingular elliptic curves and maximal orders in a quaternion algebra suggests a relation between Brandt matrices and the distribution of the shared secret in SIDH. This paper investigates the background theory of this relation and aims to recreate the results in [Tho17, chapter 7] by generating Brandt matrices. Moreover, it addresses the question whether it is more efficient to use the quaternion algebra approach rather than the supersingular elliptic curve approach.
The first part of this thesis focuses on the theory behind SIDH. To this end, chapter 2 treats background theory on elliptic curves and chapter 3 treats theory on isogenies and isogeny graphs. In chapter 4 the SIDH protocol and the results of [Tho17] are discussed. The second part of this thesis treats the necessary background information to define a correspondence between supersingular elliptic curves and quaternion algebras. Chapter 5 contains background theory on quaternion algebras. Chapter 6 justifies the interpretation of Brandt matrices as the distribution of secret keys by the existence of an equivalence of categories. In chapter 7 the heuristic estimations are verified by using said Brandt matrices. Chapter 8 contains concluding remarks and addresses topics for further research.
The reader is assumed to be familiar with group, ring and field theory, modules and basic concepts of cryptography.

2. Elliptic curves

The SIDH protocol uses supersingular isogenous elliptic curves. Before discussing the protocol, background theory on elliptic curves will be treated in this chapter. In section 2.1 the group structure and the j-invariant of elliptic curves will be discussed. Section 2.2 treats torsion points and supersingularity. The content of this chapter mainly follows [Sil09] and [Was08].

2.1. The group law and j-invariant

Definition 2.1.1 (Elliptic curve)**.** Let F be a field with char$(F) \neq 2,3$. An *elliptic curve* E/F is the graph of the Weierstrass equation

$$y^2 = x^3 + Ax + B, \tag{2.1}$$

where $A, B \in F$ and $-16(4A^3 + 27B^2) \neq 0$. The set of points $\{(x, y) \in E\} \cup \{\mathcal{O}\}$ is denoted by $E(F)$, where $\mathcal{O}$ is the point at infinity.

Remark 2.1.2. In this paper only elliptic curves over fields of characteristic not 2 or 3 will be considered. For this reason the generalized Weierstrass equation will not be discussed here and all elliptic curves will be assumed to take the form (2.1).

Definition 2.1.1 mentions the point at infinity $\mathcal{O}$, which exists for every elliptic curve E. This point can be interpreted as the point that lies at the "top" of the y-axis. A strict definition can be made in terms of the projective space.

Definition 2.1.3 (Projective space)**.** Let F be a field and let $(x_1, y_1, z_1), (x_2, y_2, z_2) \in F^3 \setminus (0,0,0)$. If there exists a $\lambda \in F^\times$ such that $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$, then (x_1, y_1, z_1) and (x_2, y_2, z_2) are called equivalent. The *projective space* $\mathbb{P}^2_F$ contains all equivalence classes $(x : y : z)$ of triples $(x, y, z) \in F^3$.

Definition 2.1.4 (Point at infinity)**.** The *point at infinity* $\mathcal{O}$ on an elliptic curve E/F is given by $(0 : 1 : 0) \in \mathbb{P}^2_F$.

For a further discussion of definition 2.1.4, see [Was08, section 2.3].
Following [Sil09, p. 51], an elliptic curve $E/F \subset \mathbb{P}^2_F$ of the form (2.1) is of degree 3. By a special case of Bézout's theorem a line $l \subset \mathbb{P}^2_F$ intersects E in exactly 3 points, which are not necessarily distinct. For a detailed discussion of this topic, see [His14]. The above allows the construction of the following composition law.

Definition 2.1.5 (Composition law)**.** Let P and Q be points on elliptic curve E and let l be the line through both points. Line l then intersects E in a point R'. Let k be the vertical line through $\mathcal{O}$ and R', which intersects E in a point R. The *composition law* $+ : E \times E \to E$ is given by $P + Q = R$.

The composition law is illustrated in figure 2.1.

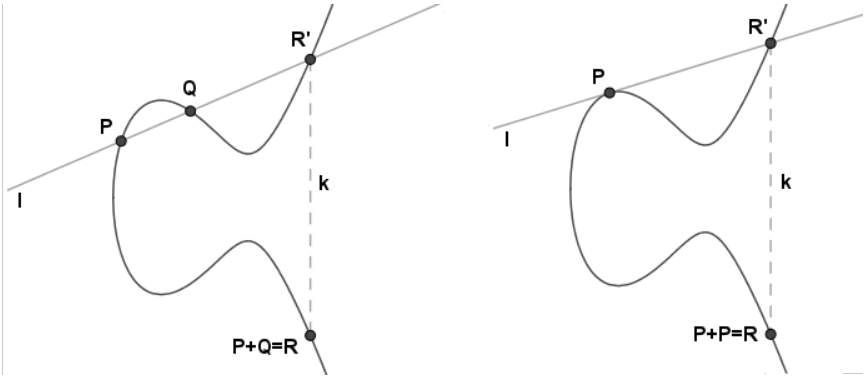


Figure 2.1: The composition law on an elliptic curve. The left figure shows addition of separate points P and Q. The right figure shows addition of P with itself, in which case line l is the line tangent to P.

Theorem 2.1.6. *Let F be a field. The composition law $+$ on elliptic curve E/F has the following properties:*

1. $(P+Q)+R = P+(Q+R)$ *for all* $P,Q,R \in E$ *(associativity);*
2. $P+\mathcal{O} = P$ *for all* $P \in E$ *(identity element);*
3. *For all* $P=(x,y) \in E$*, there exists a* $P'=(x,-y) \in E$ *such that* $P+P'=\mathcal{O}$ *(inverse element);*
4. $P+Q=Q+P$ *for all* $P,Q \in E$ *(commutativity).*

This makes $(E(F),+,\mathcal{O})$ *an abelian group.*

Proof. See [Was08, theorem 2.1]. □

Definition 2.1.7 (Isomorphic elliptic curves)**.** Let E_1 and E_2 be elliptic curves. If there exist morphisms $\varphi_1 : E_1 \to E_2$ and $\varphi_2 : E_2 \to E_1$ such that

$$\varphi_2 \circ \varphi_1 = \mathrm{id}_{E_1},$$
$$\varphi_1 \circ \varphi_2 = \mathrm{id}_{E_2},$$

then E_1 and E_2 are said to be *isomorphic*. This is denoted by $E_1 \cong E_2$.

By [Feo17, chapter 2, the first paragraph], an isomorphism between two elliptic curves can be given as follows. Let the following be Weierstrass equations of two elliptic curves:

$$y^2 = x^3 + au^4x + bu^6,$$
$$(y^2) = (x')^3 + ax' + b.$$

An isomorphism between these curves that preserves both their Weierstrass form and the group law is given by the map

$$(x,y) \mapsto (u^2x', u^3y'.$$

Definition 2.1.8 (j-invariant)**.** Let E be an elliptic curve over a field F of the form (2.1). The *j-invariant* $E(F)$ is given by

$$j(E) \coloneqq 1728\frac{4A^3}{4A^3+27B^2} \in F.$$

Theorem 2.1.9. *Let F be a field with algebraic closure $\overline{F}$ and let E_1 and E_2 be elliptic curves over F. Then $j(E_1) = j(E_2)$ if and only if E_1 and E_2 are isomorphic over $\overline{F}$.*

Proof. See [Sil09, proposition III.1.4.b]. □

Theorem 2.1.9 states that all elliptic curves over F in an isomorphism class have the same unique j-invariant, independent of the chosen representative for the class.

2.2. Torsion points and supersingular elliptic curves

For a positive integer n and an elliptic curve E with $P \in E$, write

$$nP = \underbrace{P + \cdots + P}_{\text{n times}}.$$

Definition 2.2.1 (Torsion group)**.** Let E be an elliptic curve over a field F. For a positive integer n, the *n-torsion group* of $E(F)$ is defined as

$$E(F)[n] \coloneqq \{P \in E(F) : nP = \mathcal{O}\}.$$

Theorem 2.2.2. *Let E be an elliptic curve over a field F and n a positive integer. If $char(F) \neq 0$ does not divide n, then*

$$E(F)[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Proof. See [Was08, section 3.2]. □

By theorem 2.2.2, there exist generators $P_1, P_2 \in E(F)[n]$ such that

$$E(F)[n] = \{m_1P_1 + m_2P_2 : m_1, m_2 \in \mathbb{Z}/n\mathbb{Z}\}.$$

Definition 2.2.3 (Supersingular elliptic curves)**.** Let p be a prime and F a field of characteristic p and E/F an elliptic curve. If $E(F)[p] = \{\mathcal{O}\}$, E is called *supersingular*. If $E(F)[p] \cong \mathbb{Z}_p$, E is called ordinary.

Definition 2.2.4 (Endomorphism ring)**.** Let E be an elliptic curve. The *endomorphism ring* $\mathrm{End}(E)$ is the ring containing all endomorphisms $\phi : E \to E$.

Theorem 2.2.5. *If E is a supersingular elliptic curve, $End(E)$ is a non-commutative ring.*

Proof. See [Sil09, theorem V.3.1]. □

Theorem 2.2.5 suggests a relation between supersingular elliptic curves and quaternion algebras, which are also non-commutative. This will be investigated further in section 5.2.
Let $\mathbb{F}_p$ be a finite field of size p, where p is prime, and denote by $\overline{\mathbb{F}}_p$ an algebraic closure. In the rest of this paper elliptic curves will mainly be defined over $\overline{\mathbb{F}}_p$.

Theorem 2.2.6 ([Tho17], theorem 5.4.1)**.** *Let $E/\overline{\mathbb{F}}_p$ be a supersingular elliptic curve. Then $j(E) \in \mathbb{F}_{p^2}$.*

Proof. See [Sil09, theorem V.3.1(a)(iii)]. □

Proposition 2.2.7 ([Tho17], proposition 5.4.2)**.** *Let $j_0 \in \mathbb{F}_{p^2}$ be a supersingular j-invariant. Then there exists a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ such that $j(E) = j_0$ and*

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \oplus \mathbb{Z}_{p+1}.$$

3. Isogenies

Isogenies are a particular type of morphisms between elliptic curves. In section 3.1 they will be defined and some of their properties will be discussed. Section 3.2 treats basic notions of graph theory, followed by the definition of isogeny graphs.

3.1. Isogenies between elliptic curves

Definition 3.1.1 (Isogenies)**.** Let F and let E_1, E_2 be elliptic curves over F. An *isogeny* is a non-constant homomorphism of abelian groups, given by

$$\begin{aligned} &\varphi : E_1(\overline{F}) \to E_2(\overline{F}), \\ &(x, y) \mapsto (r_1(x, y), r_2(x, y)), \end{aligned} \tag{3.1}$$

where $r_1(x, y), r_2(x, y)$ are rational functions. If such an isogeny exists, E_1 and E_2 are said to be isogenous.

Remark 3.1.2. Isogenies are not only homomorphisms between elliptic curves as abelian groups, but also morphisms between said curves as algebraic varieties. However, the theory of algebraic varieties lies beyond the scope of this thesis and will not be discussed further here. See [Sil09, chapter 1] for background theory on this topic.

Any isogeny φ of the form (3.1) is equivalent to

$$\varphi(x, y) = (R_1(x), yR_2(x)), \tag{3.2}$$

where $R_1(x), R_2(x)$ are rational functions (see [Was08, section 2.9 and 12.2]).

Definition 3.1.3 (Degree of an isogeny)**.** Let φ be an isogeny of the form 3.2. Since $R_1(x)$ is a rational function, $R_1(x) = \frac{p(x)}{q(x)}$ for some polynomials $p(x)$ and $q(x)$. The *degree* of φ is defined by

$$\deg \varphi = \max\{\deg(p), \deg(q)\}.$$

If φ is an isogeny with $\deg \varphi = n$, then φ is called an n-isogeny.

Definition 3.1.4 (Separability)**.** An isogeny φ of the form 3.2 is *separable* if $R_1'(x)$ is not identically 0.

Definition 3.1.5 (Dual isogeny)**.** For any isogeny $\varphi : E_1 \to E_2$ there exists a *dual isogeny*

$$\hat{\varphi} : E_2 \to E_1,$$

such that for a point $P \in E_1$,

$$\hat{\varphi} \circ \varphi : P \mapsto (\deg \varphi)P.$$

The dual isogeny $\hat{\varphi}$ is uniquely determined, with the property that $\hat{\hat{\varphi}} = \varphi$.

Proposition 3.1.6. *Let E/F be an elliptic curve and $H \subseteq E(\overline{F})$ a finite subgroup. Then there exists an isogeny $\varphi : E \to E/H$ with $\ker \varphi = H$.*

Proof. See [Sil09, proposition III.4.12 and remark III.4.13.1]. □

There are methods to construct specific isogenies given an elliptic curve, for example via application of Vélu's formulas (see [Was08, theorem 12.16]).

Proposition 3.1.7. *Let F be a field with algebraic closure $\overline{F}$, let E_1 and E_2 be elliptic curves over $\overline{F}$ and let $\varphi : E_1 \to E_2$ be an isogeny. If φ is separable, $\deg\varphi = \#\ker\varphi$. Otherwise, $\deg\varphi > \#\ker\varphi$.*

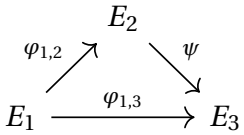
Proof. See [Was08, proposition 12.8]. □

The kernel of an isogeny $\varphi : E_1(K) \to E_2(K)$ is a finite subgroup of $E_1(K)$.

Proposition 3.1.8. *Let F be a field and E_1, E_2, E_3 elliptic curves over $\overline{F}$, for which there exist separable isogenies $\varphi_{1,2} : E_1 \to E_2$ and $\varphi_{1,3} : E_1 \to E_3$ defined over $\overline{F}$. If $\ker\varphi_{1,2} = \ker\varphi_{1,3}$, E_2 and E_3 are isomorphic.*

Proof. See [Was08, proposition 12.12]. □

The isomorphism in proposition 3.1.8 is given by an isogeny $\psi : E_2 \to E_3$, which gives that $\psi \circ \varphi_{1,2} = \varphi_{1,3}$. This is illustrated by commutativity of the following diagram:



In fact proposition 3.1.8 can be formulated as an if and only if statement.

Proposition 3.1.9. *If $E_2 \cong E_3$, then $\ker\varphi_{1,2} = \ker\varphi_{1,3}$.*

Proof. Let $E_2 \cong E_3$ again be given by isogeny $\psi : E_2 \to E_3$. Because the kernel of ψ is trivial,

$$\begin{aligned}\ker\varphi_{1,3} &= \ker(\psi \circ \varphi_{1,2}) \\ &= \deg(\psi \circ \varphi_{1,2}) \\ &= \deg\varphi_{1,2} \\ &= \ker\varphi_{1,2}.\end{aligned}$$

□

Definition 3.1.10 (Equivalent isogenies)**.** Let φ_1, φ_2 be separable isogenies. If $\ker\varphi_1 = \ker\varphi_2$, φ_1 and φ_2 are said to be *equivalent*. Otherwise they are called distinct.

By definition 3.1.10 it is possible to define equivalence classes of isogenies, where each class contains isogenies that have identical kernels.

Proposition 3.1.11. *Let E_1 and E_2 be elliptic curves over K, where K is an extension of the field F, and let $\varphi : E_1 \to E_2$ be an isogeny. Then φ is surjective.*

Proof. See [Was08, theorem 12.9]. □

Theorem 3.1.12 ([Feo17], theorem 13)**.** *Let p be a prime. Two elliptic curves E and E' defined over a finite field $\mathbb{F}_p$ are isogenous if and only if $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$.*

3.2. Isogeny graphs

Isogenous elliptic curves can be represented by isogeny graphs. This section will treat basic notions of graph theory, following [Wil96, chapter 2], and the construction of isogeny graphs.

Definition 3.2.1 (Graph)**.** A *graph* $\mathcal{G}$ consists of an ordered pair $(\mathcal{V},\mathcal{E})$, where $\mathcal{V}$ denotes a finite set of vertices and $\mathcal{E}$ a multiset of unordered pairs of vertices.

In definition 3.2.1 the elements of $\mathcal{E}$ are unordered pairs, in which case $\mathcal{G}$ is called an undirected graph. If $\mathcal{E}$ consists of ordered pairs of vertices, $\mathcal{G}$ is called a directed graph.
Vertices $v_i, v_j \in \mathcal{V}$ are called adjacent if they form a pair $\langle v_i, v_j\rangle = \langle v_j, v_i\rangle$ in $\mathcal{E}$. This determines the structure of the graph and can be represented in matrix form.

Definition 3.2.2 (Adjacency matrix)**.** Let $\mathcal{G} = (\mathcal{V},\mathcal{E})$ with $\mathcal{V} = \{v_1,\cdots,v_n\}$. The matrix $A \in \mathbb{Z}^{n\times n}$ with $A_{i,j}$ the number of pairs $\langle v_i, v_j\rangle \in \mathcal{E}$ is the *adjacency matrix* of $\mathcal{G}$.

If $\mathcal{G}$ is an undirected graph, its adjacency matrix is symmetric, because $\langle v_i, v_j\rangle = \langle v_j, v_i\rangle$ for all $\langle v_i, v_j\rangle \in \mathcal{E}$.

Definition 3.2.3 (Walk)**.** Let $\mathcal{G} = (\mathcal{V},\mathcal{E})$ be a graph with $\mathcal{V} = \{v_1,\cdots,v_n\}$. A *walk* of length $m \in \mathbb{Z}$ in $\mathcal{G}$ is represented by a finite sequence of vertices

$$\{v_{k_0}, v_{k_1},\cdots, v_{k_{m-1}}, v_{k_m}\}. \tag{3.3}$$

In this sequence any two consecutive vertices are adjacent.

Backtracking occurs in a walk if in a sequence of the form 3.3, $v_{k_{i+1}} = v_{k_{i-1}}$ for $i \in \{1,\cdots,m\}$.

Definition 3.2.4 (Isogeny graph)**.** Let $\mathcal{V}_{p,\ell}$ be the set of isomorphism classes of isogenous elliptic curves over the field $\overline{\mathbb{F}}_p$, where $\ell \in \mathbb{Z}_{>0}$. Such a class is denoted by $[E]$, where E is a representative and elliptic curves are in the same class if they are isomorphic. Let $\mathcal{E}_{p,\ell}$ be the multiset of distinct ℓ-isogenies between elements of $\mathcal{V}_{p,\ell}$. Then the graph $\mathcal{G}_{p,\ell} = (\mathcal{V}_{p,\ell},\mathcal{E}_{p,\ell})$ is an *ℓ-isogeny graph.*

By theorem 2.1.9, each vertex $[E]$ in an isogeny graph can be denoted by its unique j-invariant $j(E) \in \overline{\mathbb{F}}_p$.
Although the isogeny graph $\mathcal{G}_{p,\ell}$ depends on both p,ℓ, its vertex set $\mathcal{V}_{p,\ell}$ depends exclusively on p. Since $\mathcal{E}_{p,\ell}$ contains only distinct ℓ-isogenies, it is a multiset containing ℓ-isogeny classes.

Remark 3.2.5. In case $p \equiv 1 \mod 12$, ℓ-isogeny graph $\mathcal{G}_{p,\ell}$ is undirected. Here for any isogeny $\varphi \in \mathcal{E}_{p,\ell}$ also $\hat{\varphi} \in \mathcal{E}_{p,\ell}$. For other primes p it can happen that two non-equivalent isogenies have equivalent dual isogenies. For an isogeny $\varphi : E_1 \to E_2$, this occurs when $\#\mathrm{Aut}(E_2) > 2$. (see [Gal12, remark 25.3.2]).

Proposition 3.2.6. *Let E be an elliptic curve over $\overline{\mathbb{F}}_p$ and let $\ell \neq p$ be prime. Then there exist $\ell+1$ distinct ℓ-isogenies with domain $E(\overline{\mathbb{F}}_p)$.*

Proposition 3.2.6 implies that there are $\ell+1$ edges connected to each vertex in $\mathcal{G}_{p,\ell}$.
Isogeny graphs can be defined for both supersingular and ordinary elliptic curves. For the SIDH protocol only supersingular isogeny graphs are of interest, because here there is more algebraic structure on the endomorphism ring than in the case of ordinary isogeny graphs (see [Feo17, chapter 9]). In the remainder of this paper the explicit mention of supersingularity will be omitted and 'isogeny graph' will refer to a supersingular isogeny graph only.

4. Supersingular isogeny Diffie-Hellman

A potential candidate for a quantum resistant key exchange is supersingular isogeny Diffie-Hellman (SIDH), first described in [JF11]. In section 4.1 the details of SIDH will be discussed, followed by its security in terms of uniformity of the distribution of the secret key in section 4.2.
By theorem 2.2.6 and proposition 2.2.7, any supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ used in SIDH is isomorphic to a supersingular elliptic curve over $\mathbb{F}_{p^2}$. Therefore, this chapter considers such curves over $\mathbb{F}_{p^2}$ rather than over $\overline{\mathbb{F}}_p$. Furthermore, all isogenies mentioned here are assumed to be separable. By theorem 3.1.7 this implies that for any such isogeny φ, $\deg\varphi = \#\ker\varphi$.

4.1. Key exchange

In this section supersingular isogeny Diffie-Hellman (SIDH) will be discussed, following [JF11], [FJP14] and [Feo17]. First some preliminaries and a general overview of the protocol will be given, followed by a discussion of its details.
SIDH is based on making non-backtracking random walks of length e over the edges of an ℓ-isogeny graph. This yields a unique composition $\varphi = \varphi_1 \circ \cdots \circ \varphi_e$ of e ℓ-isogenies, where φ_i represents the ith step in the walk (see [BCNE+18, proposition 4.3]). For a non-backtracking walk, φ is an ℓ^e-isogeny with $deg(\varphi) = \ell^e = \#\ker\varphi$. The kernel of an ℓ-isogeny corresponds to a cyclic subgroup in $E[\ell]$. So for φ there exists $\langle P\rangle \subset E[\ell^e]$ such that $\ker\varphi = \langle P\rangle$, where $P \in E[\ell^e]$. The kernel of isogeny φ is cyclic of order ℓ^e if and only if the walk is non-backtracking.
The goal of the protocol is for Alice and Bob to compute a shared secret key, to which they both contribute. They each use their own isogeny graph with the same set of vertices (j-invariants), where Alice uses isogenies of degree ℓ_A as edges and Bob isogenies of degree $\ell_B \neq \ell_A$. Here the numbers ℓ_A, ℓ_B are primes, which are chosen small to increase security. Denote the graph of Alice by $\mathcal{G}_{p,\ell_A}$ and the graph of Bob by $\mathcal{G}_{p,\ell_B}$. Alice makes e_A non-backtracking random walks in $\mathcal{G}_{p,\ell_A}$ by choosing a random cyclic subgroup $\langle A\rangle \subset E[\ell_A^{e_A}]$. Similarly, Bob makes a walk of length e_B in $\mathcal{G}_{p,\ell_B}$ by choosing $\langle B\rangle \subset E[\ell_B^{e_B}]$. This is done so that $\ell_A^{e_A} \approx \ell_B^{e_B}$, making both sides of the protocol approximately equally resistant to attacks. They then compute respective corresponding separable isogenies α, β such that

$$\alpha : E \to E_A \coloneqq E/\langle A\rangle, \tag{4.1}$$
$$\beta : E \to E_B \coloneqq E/\langle B\rangle. \tag{4.2}$$

The goal is to let Alice compute a new isogeny $\tilde{\alpha}$ and Bob isogeny $\tilde{\beta}$ such that

$$\tilde{\alpha} : E_B \to E/\langle A, B\rangle, \tag{4.3}$$
$$\tilde{\beta} : E_A \to E/\langle A, B\rangle. \tag{4.4}$$

Then the j-invariant $j(E/\langle A, B\rangle)$ can be used as secret key. The remainder of this section will discuss the details of this process.
Alice and Bob start the protocol by picking public parameters. The first is a prime of the form

$$p = \ell_A^{e_A}\ell_B^{e_B} f \pm 1. \tag{4.5}$$

The number f is an additional factor to ensure that p is prime, while f remains as small as possible. Alice and Bob also choose a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ such that

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(\ell_A^{e_A}\ell_B^{e_B}f)\mathbb{Z} \oplus \mathbb{Z}/(\ell_A^{e_A}\ell_B^{e_B}f)\mathbb{Z}. \tag{4.6}$$

Such a curve exists by [Feo17, theorem 54]. Then $j(E)$ is the starting vertex in the isogeny graphs. By theorem 2.2.2,

$$E[\ell_A^{e_A}] \cong \mathbb{Z}/\ell_A^{e_a}\mathbb{Z} \oplus \mathbb{Z}/\ell_A^{e_a}\mathbb{Z},$$
$$E[\ell_B^{e_B}] \cong \mathbb{Z}/\ell_B^{e_B}\mathbb{Z} \oplus \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}.$$

So there exist points $P_A, Q_A \in E(\mathbb{F}_{p^2})$ and $P_B, Q_B \in E(\mathbb{F}_{p^2})$ such that

$$\langle P_A, Q_A\rangle = E[\ell_A^{e_A}],$$
$$\langle P_B, Q_B\rangle = E[\ell_B^{e_B}].$$

Summarized, Alice and Bob now have publicly known parameters $p, E, (P_A, Q_A), (P_B, Q_B)$. The Diffie-Hellman key exchange then takes place as follows:

1. **Key generation.** Alice picks elements $m_A, n_A \in \mathbb{Z}_{\ell_A^{e_A}}$, not both divisible by ℓ_A, and Bob picks $m_B, n_B \in \mathbb{Z}_{\ell_B^{e_B}}$, not both divisible by ℓ_B. These elements are their respective private keys. They construct their own respective cyclic subgroups

   $$\langle A\rangle = \langle m_A P_A + n_A Q_A\rangle,$$
   $$\langle B\rangle = \langle m_B P_B + n_B Q_B\rangle.$$

   Alice then computes the isogeny α of equation 4.1. She also computes $\alpha(P_B), \alpha(Q_B) \in E_A$ and shares these and E_A with Bob. In turn, Bob computes the isogeny β of equation 4.2 and shares E_B and $\beta(P_A), \beta(Q_A) \in E_B$ with Alice. The 3-tuples $(E_A, \alpha(P_B), \alpha(Q_B))$, $(E_B, \beta(P_A), \beta(Q_A))$ are the public keys.

2. **Encryption.** With E_B Alice can compute a new isogeny

   $$\tilde{\alpha} : E_B \to E_{BA} \coloneqq E_B/\langle\beta(A)\rangle,$$

   where $\ker\alpha = \langle\beta(A)\rangle = \langle m_A\beta(P_A) + n_A\beta(Q_A)\rangle$. Similarly, Bob computes isogeny

   $$\tilde{\beta} : E_A \to E_{AB} \coloneqq E_A/\langle\alpha(B)\rangle,$$

   where $\ker\tilde{\beta} = \langle\alpha(B)\rangle = \langle m_B\alpha(P_B) + n_B\alpha(Q_B)\rangle$.
   Since $E_{BA} \cong E/\langle A, B\rangle \cong E_{AB}$ (see [Tho17, section 6.2, remark 5]), the shared key is $j(E_{BA}) = j(E/\langle A, B\rangle) = j(E_{AB})$.

A schematic overview of SIDH is shown in table 4.1.

	Alice	**Public**	**Bob**
Pick public parameters		$p, E, (P_A, Q_A), (P_B, Q_B)$	
Pick secret keys	$m_A, n_A \in \mathbb{Z}_{\ell_A^{e_A}}$		$m_B, n_B \in \mathbb{Z}_{\ell_B^{e_B}}$
Exchange public keys		$(E_A, \alpha(P_B), \alpha(Q_B))$, $(E_B, \beta(P_A), \beta(Q_A))$	
Compute shared key	$j(E_{BA}) = j(E/\langle A, B\rangle)$		$j(E_{AB}) = j(E/\langle A, B\rangle)$

Table 4.1: Schematic overview of the SIDH protocol. The columns represent to whom the data are known.

It is believed that SIDH is a good candidate for a quantum-resistant key exchange protocol. Its safety relies on the supersingular isogeny problem, which is allegedly difficult to solve. This problem is formulated in problem 2.

Problem 2 ([GPST16], definition 1)**.** Given a finite field F and supersingular elliptic curves E_1, E_2 over F such that $\#E_1(F) = \#E_2(F)$, compute an isogeny $\varphi : E_1 \to E_2$.

By theorem 3.1.12, the condition $\#E_1(F) = \#E_2(F)$ in problem 2 implies that E_1 and E_2 are isogenous.
Another problem involves computation of the endomorphism ring of a supersingular elliptic curve. Once this ring is known, the isogeny problem can be solved (see [GPST16]).
An important factor that contributes to the security of SIDH is uniformity of the distribution of the secret key. This will be discussed in section 4.2.

4.2. Security

For security of the SIDH protocol, it is important that $j(E_A)$, $j(E_B)$ and the shared key $j(E_{AB})$ are uniformly distributed in the shared key space. A uniform distribution ensures optimal security, as it makes it equally likely for any j-invariant to be chosen as the secret key. Although it has not been proven theoretically that these distributions are uniform, there exist heuristics that show that this is the case. In [Tho17] these heuristics have been verified by simulation for $l_A = 2$, $l_B = 3$ and $p = 2^{e_A}3^{e_B}f - 1$. This section will discuss these results.
Let E be a randomly chosen starting curve such that $j(E)$ is a vertex in $\mathcal{G}_{p,\ell_A}$ and $\mathcal{G}_{p,\ell_B}$. According to the SIDH protocol, first a non-backtracking random walk of length e_A is made by Alice from $j(E)$ to $j(E_A)$ via 2-power isogeny α. Similarly, Bob makes a walk of length e_B from $j(E)$ to $j(E_B)$ via 3-power isogeny β.

Estimation 4.2.1 ([Tho17], estimation 7.3.1)**.** Construct multisets S_A and S_B as follows:

- Pick $\ell_A^{e_A-1}(\ell_A+1)$ vertices (j-invariants) in $\mathcal{G}_{p,\ell_A}$ uniformly at random, allowing repetition. Each time a vertex is picked, store it in S_A.
- Pick $\ell_B^{e_B-1}(\ell_B+1)$ vertices in $\mathcal{G}_{p,\ell_B}$ uniformly at random, allowing repetition. Each time a vertex is picked, store it in S_B.

The distribution of $j(E_A)$ and $j(E_B)$ in SIDH are estimated to be the same as when respectively picking an element from S_A and S_B uniformly at random.

In [Tho17] estimation 4.2.1 is tested by simulation in the following way. First a procedure is started to obtain a random starting vertex $j(E_0)$. Then 500 random walks of length e_A are simulated, recording the number of distinct end vertices $j(E_A)$. The same is done for $j(E_B)$ by simulating 500 random walks of length e_B.
To obtain shared secret key $j(E_{AB})$, the random walk of length e_A from $j(E_0)$ to $j(E_A)$ by Alice via 2^{e_A}-isogeny α is followed by a random walk of length e_B from $j(E_A)$ to $j(E_{AB})$ by Bob via 3^{e_B}-isogeny $\tilde{\beta}$. The above is analogous for first letting Bob make a random walk of length e_B from $j(E_0)$ to $j(E_B)$ via β and then letting Alice make a random walk of length e_A from $j(E_B)$ to $j(E_{BA})$ via $\tilde{\alpha}$. This results in secret key $j(E_{BA}) = j(E_{AB})$. Estimation 4.2.2 estimates the distribution of $j(E_{AB})$, which was verified by simulation.

Estimation 4.2.2 ([Tho17], estimation 7.4.1)**.** A multiset S is constructed as follows:

1. Randomly pick $\ell_A^{e_A-1}(\ell_A+1)$ vertices in $\mathcal{G}_{p,\ell_A}$. Call the number of times each j-invariant corresponding to the vertices is picked z.
2. Randomly pick $\ell_B^{e_B-1}(\ell_B+1)$ vertices in $\mathcal{G}_{p,\ell_B}$. Each time a vertex is picked, put z copies of its j-invariant in set S.

The distribution of $j(E_{AB})$ in SIDH is estimated to be the same as when picking an element from S uniformly at random.

In [Tho17] strong heuristic evidence is given for estimations 4.2.1 and 4.2.2 by conducting simulations. This was done for $\ell_A = 2$ and $\ell_B = 3$ in three cases:

- $e_A = 8, e_B = 5, f = 1, p = 2^8 3^5 - 1$
- $e_A = 9, e_B = 6, f = 5, p = 2^9 3^6 5 - 1$
- $e_A = 10, e_B = 6, f = 7, p = 2^{10} 3^6 7 - 1$

In all cases the walks are short and the primes relatively small, but the distributions are relatively uniform and coincide with the results obtained from the heuristic estimations.

5. Quaternion algebras

This chapter treats preliminaries on quaternion algebras in section 5.1, followed by section 5.2 on orders in a quaternion algebra and section 5.3 on quaternion ideals. The contents of this chapter follow [Voi17, chapter 2, 16 and 17].

5.1. Preliminaries

Definition 5.1.1 (Algebra)**.** An *algebra* B over a field F is a ring with a homomorphism

$$\phi : F \to B,$$

where

$$\phi(F) \subseteq Z(B) = \{\alpha \in B : \alpha\beta = \beta\alpha \ \forall \beta \in B\}.$$

Definition 5.1.2 (Quaternion algebra)**.** Let F be a field such that $\mathrm{char}(F) \neq 2$ and B an algebra over F. For $a, b \in F^\times$, let $(a, b \mid F)$ denote an F-vector space with basis $\{1, i, j, k\}$, where

$$\begin{aligned} i^2 &= a, \\ j^2 &= b, \\ k &= ij = -ji. \end{aligned}$$

If $B \cong (a, b \mid F)$, B is called a *quaternion algebra over* F.

The dimension of an F-algebra B is the dimension of B as an F-vector space, denoted by $\dim_F B$. If B is a quaternion algebra, $\dim_F B = 4$.

Definition 5.1.3 (Involution)**.** Let B be an F-algebra with multiplicative identity element 1. An involution $\bar{} : B \to B$ is an F-linear map such that

1. $\overline{1} = 1$;
2. $\overline{\overline{\alpha}} = \alpha$ for all $\alpha \in B$;
3. $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$ for all $\alpha, \beta \in B$.

If $\alpha\overline{\alpha} \in F$ for all $\alpha \in B$, $\bar{}$ is called the *standard involution.*

Definition 5.1.4. (Reduced norm) Let $\bar{}$ be the standard involution on F-algebra B. The *reduced norm* is defined by

$$\begin{aligned} \mathrm{nrd} : B &\to F, \\ \alpha &\mapsto \alpha\overline{\alpha}. \end{aligned}$$

5.2. Orders

This section will treat the theory necessary to understand the relation between elliptic curves and quaternion algebras, stated explicitly in theorem 5.2.5. Let B denote a quaternion algebra over $\mathbb{Q}$.

Definition 5.2.1 (Lattice)**.** Let V be a finite-dimensional $\mathbb{Q}$-vector space. A finitely generated $\mathbb{Z}$-submodule $M \subset V$ such that M contains a basis for V, is called a *lattice*.

Definition 5.2.2 (Order)**.** Let $O \subseteq B$ be a subring of B. If O is a lattice, it is called an *order* in B.

Definition 5.2.3 (Left/right order)**.** Let $I \subseteq B$ be a lattice. The *left order* and *right order* of I are defined by respectively

$$O_L(I) = \{\alpha \in B : \alpha I \subseteq I\},$$
$$O_R(I) = \{\alpha \in B : I\alpha \subseteq I\}.$$

Left and right orders are lattices of B, while also being subrings of B (see [Voi17, paragraph 10.2.5]). For lattices $I, J \subset B$, I is called compatible with J when $O_R(J) = O_L(I)$.

Definition 5.2.4 (Maximal order)**.** Let $O \subseteq B$. Then O is called *maximal* if for any order $O' \subseteq B$ such that $O \subseteq O'$, it is the case that $O = O'$.

The following theorem specifies the relation hinted at by theorem 2.2.5 and provides an alternate definition of a supersingular elliptic curve.

Theorem 5.2.5. *Let F be a field of characteristic p and let E/F be an elliptic curve. Then one of the following holds:*

- *End(E) is isomorphic to an order in a number field $\mathbb{Q}[\sqrt{-D}]$ for $D > 0$, in which case E is ordinary.*
- *End(E) is isomorphic to a maximal order in a quaternion algebra B over F, in which case E is supersingular.*

Proof. See [Sil09, corollary III.9.4]. □

Remark 5.2.6. If an elliptic curve E is supersingular, the maximal order to which $\mathrm{End}(E)$ is isomorphic is ramified at p and ∞. For more on ramification in terms of elliptic curves, see [Was08, section 10.2].

5.3. Quaternion ideals

Let B again denote a quaternion algebra over $\mathbb{Q}$ and O an order in B. This section will study ideals of O.

Definition 5.3.1. (Invertibility) Let $I \subset B$ be a lattice. If there exists a lattice $I' \subset B$ such that

$$II' = O_L(I),$$

I is called *right invertible* with right inverse I'.
Similarly, if there exists a left inverse $I^* \subset B$ such that

$$I^* I = O_R(I),$$

I is called *left invertible* with left inverse I^*. If there exists a two-sided inverse J of I such that

$$IJ = O_L(I) = O_R(J),$$
$$JI = O_L(J) = O_R(I),$$

I is called *invertible*. Its inverse J is then uniquely defined as

$$J = \{\alpha \in B : I\alpha I \subseteq I\}.$$

Definition 5.3.2. (Principal lattice) A lattice $I \subset B$ is *principal* if there exists $\alpha \in B$ such that I is generated by α. That is,

$$I = O_L(I)\alpha = \alpha O_R(I).$$

Definition 5.3.3. (Fractional ideal) Let $O \subseteq B$ be an order and $I \subset B$ a lattice. If $O \subseteq O_L(I)$, I is called a *left fractional O-ideal* and if $O \subseteq O_R(I)$, I is called a *right fractional O-ideal*.

By definition 5.3.3, any fractional ideal in a quaternion algebra is a lattice. In the rest of this chapter a fractional ideal will simply be referred to as 'ideal'.
The following definitions mention lattices and are therefore specifically applicable to O-ideals.

Definition 5.3.4. (Reduced norm of I) The *reduced norm* of a lattice $I \subset B$ is the $\mathbb{Z}$-module $\mathrm{nrd}(I) \subset \mathbb{Q}$ that is generated by $\{\mathrm{nrd}(\alpha) : \alpha \in I\}$.

For a lattice $I \subset B$, $\mathrm{nrd}(I)$ is an ideal of $\mathbb{Q}$ (see [Voi17, lemma 16.3.2]).
An equivalence relation between lattices $I, J \subseteq B$ is given by $\sim_R$, where $I \sim_R J$ if $\alpha I = J$ for some $\alpha \in B^\times$.

Definition 5.3.5. (Class) Let $I \subseteq B$ be a lattice. The set

$$[I]_R = \{J \subseteq B : I \sim_R J\}$$

is called a *right class* of lattices.

Definition 5.3.6. (Right class set) Let $O \subset B$ be an order. The set

$$\mathrm{Cls}_R\, O \coloneqq \{[I]_R : \text{I an invertible right } O\text{-ideal}\}$$

is the *right class set* of O.

Left classes $[I]_L$ and the left class set Cls_L are defined analogously to their right equivalents in definitions 5.3.5 and 5.3.6. In the rest of this paper only right classes and the right class set will be considered. For a lattice I, this is denoted by $[I] \coloneqq [I]_R$ and $\mathrm{Cls}\, O \coloneqq \mathrm{Cls}_R\, O$.

Proposition 5.3.7 ([Voi17], proposition 17.5.6)**.** *The right class set Cls O is finite.*

Proof. See [Voi17], proposition 17.5.6 and corollary 27.6.17. □

The following generalization can be made for ideals $I \subset O$ when O is a maximal order.

Theorem 5.3.8 ([Voi17], theorem 18.1.2.(a))**.** *Let $O \subseteq B$ be a maximal order. If $I \subseteq B$ is a lattice for which $O_R(I) = O$ or $O_L(I) = O$, then I is an invertible O-ideal.*

6. Equivalence of categories and Brandt matrices

To use Brandt matrices to represent walks on isogeny graphs, it must be shown that they can be interpreted as adjacency matrices for such graphs. There exists an equivalence of categories that can be used to prove that this is the case. Section 6.1 contains background theory on categories. The equivalence of categories is then made explicit in section 6.2, in particular by theorem 6.2.9. In section 6.3 Brandt matrices are defined and identified as adjacency matrices for isogeny graphs.

6.1. Preliminaries of category theory

This section will treat basic notions of category theory, following [Awo06] and [AHS04].

Definition 6.1.1 (Category)**.** A *category* is a quadruple $\mathbf{C} = (\mathrm{Ob}_{\mathbf{C}}, \mathrm{Hom}_{\mathbf{C}}, \circ, 1_{Ob})$, that satisfies the following properties:

- The class $\mathrm{Ob}_{\mathbf{C}}$ contains elements that are called objects.
- For any pair $A, B \in \mathrm{Ob}_{\mathbf{C}}$ there is a set of morphisms from A to B, denoted by $\mathrm{Hom}_{\mathbf{C}}(A, B)$. For $f \in \mathrm{Hom}_{\mathbf{C}}(A, B)$, then $A = \mathrm{dom}(f)$ and $B = \mathrm{cod}(f)$. The set of all morphisms in $\mathbf{C}$ is denoted by $\mathrm{Hom}_{\mathbf{C}}$, of which the elements are all pairwise disjoint.
- For any $A \in \mathrm{Ob}_{\mathbf{C}}$ there exists an identity morphism $1_A \in \mathrm{Hom}_{\mathbf{C}}$.
- For any $f, g \in \mathrm{Hom}_{\mathbf{C}}$ such that $\mathrm{dom}(g) = \mathrm{cod}(f)$, the composition map is given by

$$\begin{aligned} \circ : \mathrm{Hom}_{\mathbf{C}} \times \mathrm{Hom}_{\mathbf{C}} &\to \mathrm{Hom}_{\mathbf{C}} \\ (f, g) &\mapsto g \circ f. \end{aligned}$$

And this quadruple satisfies the following laws:

- Associativity: for any $f, g, h \in \mathrm{Hom}_{\mathbf{C}}$ such that $\mathrm{dom}(g) = \mathrm{cod}(f)$ and dom(h) = cod(g), the map $\circ$ satisfies
$$h \circ (g \circ f) = (h \circ g) \circ f.$$
- Identity: for any $f : A \to B \in \mathrm{Hom}_{\mathbf{C}}$,
$$f \circ 1_A = f = 1_B \circ f.$$

Definition 6.1.2 (Functor)**.** Let $\mathbf{C}$ and $\mathbf{D}$ be categories. Define the map

$$F : \mathbf{C} \to \mathbf{D}$$

which maps from $\mathrm{Ob}_{\mathbf{C}}$ to $\mathrm{Ob}_{\mathbf{D}}$ and from $\mathrm{Hom}_{\mathbf{C}}$ to $\mathrm{Hom}_{\mathbf{D}}$. For any $A, B \in Ob_{\mathbf{C}}$ and $f, g \in Hom_{\mathbf{C}}(A, B)$. If F satisfies the following conditions:

1. $F(f) : F(A) \to F(B)$,
2. $F(g \circ f) = F(g) \circ F(f)$,
3. $F(1_A) = 1_{F(A)}$,

then it is called a *covariant functor*. If $F(f) : F(B) \to F(A)$ instead of property 1, then F is called *contravariant*.
The identity functor on a category $\mathbf{C}$ is denoted by $\mathbb{1}_{\mathbf{C}}$.

The category of categories is denoted by **Cat**, where $\mathrm{Ob}_{\mathbf{Cat}}$ contains categories and $\mathrm{Hom}_{\mathbf{Cat}}$ functors between categories.

Definition 6.1.3 (Isomorphic objects)**.** Let $\mathbf{C}$ be a category and $A, B \in Ob_{\mathbf{C}}$ and let $f \in Hom_{\mathbf{C}}(A, B)$. If there exists $g : B \to A \in Hom_{\mathbf{C}}$ such that

$$g \circ f = 1_A,$$
$$f \circ g = 1_B,$$

then f is an *isomorphism*. In this case f and g are each others inverses and objects A and B are called *isomorphic*. This is denoted by $A \cong B$.

As for other algebraic structures, inverses of morphisms in categories are unique.

Definition 6.1.4 (Faithful, full, essentially surjective)**.** Let $F : \mathbf{C} \to \mathbf{D}$ be a functor between categories $\mathbf{C}$ and $\mathbf{D}$.

- If the map

$$\mathbf{F}_{A,B} : \mathrm{Hom}_{\mathbf{C}}(A, B) \to \mathrm{Hom}_{\mathbf{D}}(F(A), F(B)),$$
$$f \mapsto F(f)$$

  is injective for all $A, B \in Ob_{\mathbf{C}}$, F is *faithful*.

- If $\mathbf{F}_{A,B}$ is surjective for all $A, B \in Ob_{\mathbf{C}}$, F is *full*.

- If for all $A_{\mathbf{D}} \in Ob_{\mathbf{D}}$ there exists some $A_{\mathbf{C}} \in Ob_{\mathbf{C}}$ such that $F(A_{\mathbf{C}}) \cong A_{\mathbf{D}}$, F is *essentially surjective*.

While functors between categories are the morphisms in **Cat**, they can also be considered as the objects. Functors between two specific categories form the set of objects in a new category, in which the morphisms between the functors are called natural transformations.

Definition 6.1.5 (Natural transformation)**.** Let $\mathbf{C}$ and $\mathbf{D}$ be categories with covariant functors $F : \mathbf{C} \to \mathbf{D}$ and $G : \mathbf{C} \to \mathbf{D}$. A *natural transformation* $\eta : F \mapsto G$ is a family of morphisms such that

- To every $A \in Ob_{\mathbf{C}}$, η associates a morphism $\eta_A : F(A) \to G(A)$.
- For every $f : A \to B \in Hom_{\mathbf{C}}$,

$$\eta_B \circ F(f) = G(f) \circ \eta_A.$$

If the morphism $\eta_A \in Hom_{\mathbf{C}}$ is an isomorphism for every $A \in Ob_{\mathbf{C}}$, η is called a natural isomorphism.

The second condition in definition 6.1.5 is equivalent to commutativity of the following diagram:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ {\scriptstyle \eta_A}\downarrow & & \downarrow{\scriptstyle \eta_B} \\ G(A) & \xrightarrow{G(f)} & G(B) \end{array}$$

If F and G are contravariant functors, the arrows in the diagram are reversed.
For the two functors F and E, their compositions are denoted by EF and FE.

Definition 6.1.6 (Equivalence of categories)**.** An *equivalence of categories* **C** and **D** consists of functors

$$E : \mathbf{C} \to \mathbf{D},$$
$$F : \mathbf{D} \to \mathbf{C},$$

and natural isomorphisms

$$\alpha : \mathbb{1}_{\mathbf{C}} \to FE,$$
$$\beta : \mathbb{1}_{\mathbf{D}} \to EF.$$

The categories **C** and **D** are then said to be equivalent.

The following proposition provides provides a criterion to check if a functor is part of an equivalence of categories.

Proposition 6.1.7. *Let **C** and **D** be categories and $F : \mathbf{C} \to \mathbf{D}$ a functor. The following are equivalent:*

1. *F belongs to an equivalence of categories;*
2. *F is full, faithful and essentially surjective.*

Proof. See [Awo06, proposition 7.25]. □

The notion of skeletons of a category provides a second criterion to check for the existence of an equivalence of categories, given in corollary 6.1.11.

Definition 6.1.8 (Skeleton)**.** Let **C** and **C'** be categories such that the following hold:

- **C'** is a subcategory of **C**. That is,

  $$\mathrm{Ob}_{\mathbf{C}'} \subseteq \mathrm{Ob}_{\mathbf{C}},$$
  $$\mathrm{Hom}_{\mathbf{C}'}(A, B) \subseteq \mathrm{Hom}_{\mathbf{C}}(A, B),$$

  for all $A, B \in \mathrm{Ob}_{\mathbf{C}'}$. The composition operation and identities on **C'** are the same as on **C**, under restriction.

- The inclusion functor **C'** $\hookrightarrow$ **C** is full and essentially surjective.
- No distinct objects in **C'** are isomorphic.

Then **C'** is called a *skeleton* of **C**.

The last condition in definition 6.1.8 implies that in a skeleton, each isomorphism class contains just one object.

Definition 6.1.9 (Isomorphic categories)**.** Let **C** and **D** be categories. If there exists functors $F : \mathbf{C} \to \mathbf{D}$ and $G : \mathbf{D} \to \mathbf{C}$ such that $GF = \mathbb{1}_{\mathbf{C}}$ and $FG = \mathbb{1}_{\mathbf{D}}$, then **C** and **D** are *isomorphic as categories.*

Proposition 6.1.10. *The following properties hold:*

1. *Every category has a skeleton.*
2. *If* $\mathbf{C}'_1$ *and* $\mathbf{C}'_2$ *are both skeletons of the same category then they are isomorphic.*
3. *Let* **C** *be a category. For any skeleton* $\mathbf{C}'$ *of* **C***, there exists an equivalence relation between* $\mathbf{C}'$ *and* **C** *under the inclusion functor.*

Proof. See [AHS04, remark 4.10.3 and proposition 4.14]. □

Corollary 6.1.11 ([AHS04], corollary 4.15)**.** *Two categories are equivalent if and only if their skeletons are isomorphic.*

6.2. Supersingular isogenous elliptic curves and modules of maximal orders in quaternion algebras

The relation between supersingular isogenous elliptic curves and modules of maximal orders in a quaternion algebra can be made explicit by an equivalence of categories, defined in theorem 6.2.9. The theorem, its proof and the preliminaries discussed in this section mainly follow [Voi17, chapter 42].
For supersingular elliptic curves E and E_0 over $\overline{\mathbb{F}}_p$, define $O \coloneqq \mathrm{End}(E)$, $O_0 \coloneqq \mathrm{End}(E_0)$ and quaternion algebras $B \coloneqq O \otimes \mathbb{Q}$ and $B_0 \coloneqq O_0 \otimes \mathbb{Q}$. The set of homomorphisms between E and E_0 is denoted by $\mathrm{Hom}(E, E_0)$.

Theorem 6.2.1 ([Gal12], theorem 25.3.17)**.** *Let* E, E' *be elliptic curves over* $\overline{\mathbb{F}}_p$ *and let* $\ell \neq p$ *be a prime. Then there exists an* ℓ*-power isogeny from* E *to* E'*.*

Lemma 6.2.2 ([Voi17], lemma 42.1.11)**.** *Let* E, E_0 *be supersingular elliptic curves over* $\overline{\mathbb{F}}_p$*. Then* $Hom(E, E_0)$ *is a free* $\mathbb{Z}$*-module of rank 4, which is invertible as a right* O*-module and as a left* O_0*-module.*

Proof. This proof is in part based on the proof given in [Voi17, lemma 42.1.11].
The first part of the proof will show that $\mathrm{Hom}(E, E_0)$ is a free $\mathbb{Z}$-module of rank 4. By theorem 6.2.1, for a prime n there exists a nonzero n-isogeny $\psi \in \mathrm{Hom}(E, E_0)$ with $\ker \psi = n$. Its dual isogeny is $\hat{\psi} \in \mathrm{Hom}(E_0, E)$, such that $\psi \circ \hat{\psi} = [n]$. Define the map

$$\begin{aligned} \iota_\psi : \mathrm{Hom}(E, E_0) &\to O_0, \\ \varphi &\mapsto \varphi \circ \hat{\psi}. \end{aligned}$$

Let $\varphi_1, \varphi_2 \in \mathrm{Hom}(E, E_0)$ and suppose

$$\iota_\psi(\varphi_1) = \varphi_1 \circ \hat{\psi} = \varphi_2 \circ \hat{\psi} = \iota_\psi(\varphi_2).$$

Then

$$\varphi_1|_{\hat{\psi}(E_0)} = \varphi_2|_{\hat{\psi}(E_0)},$$

which implies that $\varphi_1 = \varphi_2$, because $\hat{\psi}(E_0)$ contains infinitely many points. So ι_ψ is injective and therefore bijective. It is also a homomorphism of $\mathbb{Z}$-modules, which then makes it isomorphic to its image:

$$\mathrm{Hom}(E, E_0) \cong \iota_\psi(\mathrm{Hom}(E, E_0)) = \mathrm{Hom}(E, E_0)\hat{\psi}.$$

Here $\mathrm{Hom}(E, E_0)\hat{\psi} \subseteq O_0$. Here O_0 is a free $\mathbb{Z}$-module that is of rank 4 by definition 5.2.1. The submodule $[n](O_0) = nO_0 \subseteq O_0$ is then also a free $\mathbb{Z}$-module of rank 4. Define the map

$$\begin{aligned} \tau_\psi : O_0 &\to \mathrm{Hom}(E, E_0), \\ \varphi' &\mapsto \varphi' \circ \psi. \end{aligned}$$

Then for $\varphi' \in O_0$,

$$\begin{aligned} \iota_\psi \circ \tau_\psi(\varphi') &= \iota_\psi(\varphi' \circ \psi) \\ &= \varphi' \circ \psi \circ \hat{\psi} \\ &= \varphi' \circ [n] \\ &= [n] \circ \varphi', \end{aligned}$$

where the last equality follows from the fact that φ' is an isogeny and therefore a homomorphism. This means that

$$\iota_\psi \circ \tau_\psi(O_0) = nO_0 \subseteq \mathrm{Hom}(E, E_0)\hat{\psi} \subseteq O_0.$$

Since nO_0 and O_0 are free $\mathbb{Z}$-modules of rank 4, $\mathrm{Hom}(E, E_0)$ is as well.
Left to prove is invertibility of $\mathrm{Hom}(E, E_0)$ as a right O-module and a left O_0-module. Let again $\psi \in \mathrm{Hom}(E, E_0)$ be nonzero and let $\hat{\psi} \in \mathrm{Hom}(E_0, E)$ be its dual. Since $\mathrm{Hom}(E, E_0)\hat{\psi} \subseteq O_0$ was shown to be a free $\mathbb{Z}$-module of rank 4, it is a left O_0-ideal. As O_0 is a maximal order, $\mathrm{Hom}(E, E_0)\hat{\psi}$ is invertible by theorem 5.3.8. This argument can be repeated to show that $\mathrm{Hom}(E, E_0)\hat{\psi}$ is a right O-module, which concludes the proof. □

Definition 6.2.3. Let $I \subseteq O$ be a nonzero left ideal and $\alpha \in I$, with $E[\alpha] \coloneqq \ker \alpha$. Define

$$E[I] \coloneqq \bigcap_{\alpha \in I} E[\alpha].$$

Lemma 6.2.4 ([Voi17], paragraph 42.2.1)**.** *Because $E[I] \subset E$ is a finite subgroup, there exists an isogeny*

$$\varphi_I : E \to E/E[I].$$

Throughout this section, let $E_I \coloneqq E/E[I]$. For a separable isogeny $\varphi \in I$, definition 6.2.3 implies that

$$E[I](F) = \{P \in E(\overline{\mathbb{F}}_p) : \varphi(P) = 0 \ \forall \varphi \in I\}.$$

As a result, φ_I is also a separable isogeny. In this chapter only separable isogenies will be considered. For more background theory and the case of inseparable isogenies, see [Voi17, paragraph 42.2.4].

Lemma 6.2.5 ([Voi17], lemma 42.2.7)**.** *Let $I \subseteq O$ be a nonzero left ideal. The map*

$$\begin{aligned} \varphi_I^* : Hom(E_I, E) &\to I, \\ \psi &\mapsto \psi\varphi_I \end{aligned}$$

is an isomorphism between left O-modules.

Proof. See [Voi17, lemma 42.2.7]. □

Proposition 6.2.6. *Let $I \subseteq O_0$ and define isogeny φ_I as in definition 6.2.3. Then $\deg \varphi_I = nrd(I)$.*

Proof. See [Voi17, proposition 42.2.16.(a)]. □

Corollary 6.2.7 ([Voi17], corollary 42.2.21)**.** *For every isogeny $\varphi : E \to E'$, there exists a left O-ideal I and an isomorphism $\rho : E_I \to E'$ such that $\varphi = \rho\varphi_I$.*

Proof. See [Voi17, corollary 42.2.21]. □

Lemma 6.2.8 ([Voi17], lemma 42.2.22)**.** *Let $I, I' \subseteq O$ be nonzero left ideals. The map*

$$Hom(E_I, E) \times Hom(E_{I'}, E_I) \to Hom(E_{I'}, E)$$

is a natural map, which is bijective. It gives rise to a further bijection

$$\begin{aligned} Hom(E_{I'}, E_I) &\to I^{-1}I', \\ \psi &\mapsto \varphi_I^{-1}\psi\varphi_{I'}. \end{aligned}$$

Proof. See [Voi17, lemma 42.2.22]. □

Theorem 6.2.9. *Let $\boldsymbol{C}_{EC}$ be the category of supersingular elliptic curves under isogenies and $\boldsymbol{C}_{O_0}$ the category of invertible left O_0-modules under left O_0-module homomorphisms. The functor given by*

$$\begin{aligned} G : \boldsymbol{C}_{EC} &\to \boldsymbol{C}_{O_0} \\ E &\mapsto Hom(E, E_0) \end{aligned}$$

defines an equivalence of categories between $\boldsymbol{C}_{EC}$ and $\boldsymbol{C}_{O_0}$.

Proof. The proof follows the proof given for [Voi17, theorem 42.3.2]. It will be shown that G is indeed a functor and subsequently that it is essentially surjective and fully faithful.
The first step is to prove that G is a functor between categories. By lemma 6.2.2, the class of

objects $\mathrm{Ob}_{\mathbf{C}_{O_0}}$ contains left O_0-modules of the form $\mathrm{Hom}(E, E_0)$. As $\mathrm{Ob}_{\mathbf{C}_{EC}}$ contains all elliptic curves E, association $G : E \mapsto \mathrm{Hom}(E, E_0)$ is indeed functorial on the classes of objects of both categories. For an isogeny $\varphi \in \mathrm{Hom}_{\mathbf{C}_{EC}}(E, E')$, let $G(\varphi) = \varphi*$ which is defined by

$$\begin{aligned} \varphi^* : \mathrm{Hom}(E', E_0) &\to \mathrm{Hom}(E, E_0), \\ \psi &\mapsto \psi \circ \varphi. \end{aligned}$$

Because φ^* is a left O_0-module homomorphism, $\varphi^* \in \mathrm{Hom}_{\mathbf{C}_{O_0}}(\mathrm{Hom}(E', E_0), \mathrm{Hom}(E, E_0))$. This implies that G is also functorial on morphisms of both categories and therefore a functor.
The next step is to show that G is essentially surjective. Let $I \in \mathrm{Ob}_{O_0}$ and tensor by $\mathbb{Q}$ to obtain injection $I \hookrightarrow I \otimes \mathbb{Q}$. Since I is a 4-dimensional $\mathbb{Z}$-lattice, this injection is given by

$$\begin{aligned} \mathbb{Z}^4 &\hookrightarrow \mathbb{Z}^4 \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}^4, \\ (w, x, y, z) &\mapsto (\frac{w}{1}, \frac{x}{1}, \frac{y}{1}, \frac{z}{1}). \end{aligned}$$

Use notation $M \coloneqq \mathbb{Z}^4 \otimes_{\mathbb{Z}} \mathbb{Q}$. It can be shown that there exists an isomorphism between M and B_0 as B_0-modules. To this end, let $m \in M$ be nonzero and define the map

$$\begin{aligned} \varphi : B_0 &\to M, \\ b &\mapsto bm. \end{aligned}$$

Then φ is a B_0-module homomorphism. Since B_0 is a division ring, $\ker(\varphi)$ as an ideal is either trivial or B_0. If $\ker(\varphi) = B_0$, then ϕ is the trivial map. Since $m \neq 0$ this cannot be the case, so $\ker(\varphi) = \{0\}$. This makes φ injective as a B_0-homomorphism and therefore bijective. So $M \simeq B_0$ and by map $I \hookrightarrow I \otimes \mathbb{Q}$, $I \subseteq B_0$ up to isomorphism. After scaling with an integer, $I \subseteq O_0$ is a left O_0-ideal. By lemma 6.2.5, $I \cong \mathrm{Hom}(E_I, E_0)$ under the pullback map. For any such I, define $E_I \coloneqq E/E[I]$. So for any $I \in \mathrm{Ob}_{O_0}$, there exists an $E_I \in \mathrm{Ob}_{EC}$ such that $G(E_I) = \mathrm{Hom}(E_I, E_0) \cong I$. This makes G is essentially surjective.
The last step is to show that G is fully faithful. Define the map

$$\begin{aligned} \mathbf{G}_{E,E'} : \mathrm{Hom}(E, E') &\to \mathrm{Hom}(\mathrm{Hom}(E, E_0), \mathrm{Hom}(E', E_0)), \\ \varphi &\mapsto \varphi^*. \end{aligned}$$

Showing that G is fully faithful is equivalent to showing that $\mathbf{G}_{E,E'}$ is bijective. By corollary 6.2.7, there exist left O_0-ideals I, I' such that $E \simeq E_{0,I} \coloneqq E_0/E_0[I]$ and $E' \simeq E_{0,I'} \coloneqq E_0/E_0[I']$. By lemma 6.2.4, there exist isogenies

$$\begin{aligned} \varphi_{0,I} &: E_0 \to E_{0,I}, \\ \varphi_{0,I'} &: E_0 \to E_{0,I'}. \end{aligned}$$

So by lemma 6.2.5, $I = \mathrm{Hom}(E_{0,I}, E_0)\varphi_{0,I}$ and $I' = \mathrm{Hom}(E_{0,I'}, E_0)\varphi_{0,I'}$. This reduces $\mathbf{G}_{E,E'}$ to the map

$$\begin{aligned} \mathrm{Hom}(E_{0,I}, E_{0,I'}) &\to (I' : I)_R = I'^{-1} I, \\ \psi &\mapsto \varphi_{0,I'}^{-1} \psi \varphi_{0,I}. \end{aligned}$$

So by lemma 6.2.8, $\mathbf{G}_{E,E'}$ is bijective.
Because G is essentially surjective and fully faithful, property 6.1.7 implies that it defines an equivalence of categories. □

6.3. Brandt matrices as adjacency matrices of supersingular isogeny graphs

This section contains a justification for the use of Brandt matrices as adjacency matrices for supersingular isogeny graphs. Such graphs will from here on be referred to as 'isogeny graphs'.
Throughout this section, fix p to be a prime and let all elliptic curves be defined over $\overline{\mathbb{F}}_p$. For the elliptic curve E_0 as a starting curve, define $O_0 \coloneqq \mathrm{End}(E_0)$ so that O_0 is an order in the quaternion algebra $B_0 \coloneqq O_0 \otimes \mathbb{Q}$. Let I_i, I_j be representatives of distinct classes of invertible O_0-ideals. That is, $[I_i], [I_j] \in \mathrm{Cls}\, O_0$ with $[I_i] \neq [I_j]$. Let E_i, E_j be elliptic curves. Define the sets

$$\mathcal{S}_{n,i,j} \coloneqq \{H \subseteq E_j(\overline{\mathbb{F}}_p) : E_j/H \simeq E_i, \#H = n\},$$
$$\mathcal{T}_{n,i,j} \coloneqq \{J \subseteq I_j : \mathrm{nrd}(J) = n \cdot \mathrm{nrd}(I_j), [J] = [I_i]\}.$$

Remark 6.3.1. The sets $\mathcal{S}_{n,i,j}$ and $\mathcal{T}_{n,i,j}$ also depend on the prime p. Since this number was fixed earlier, this won't be denoted explicitly.

Let k be a positive integer and let $S(n) \in M_k(\mathbb{Z})$ such that $S(n)_{i,j} = \#\mathcal{S}_{n,i,j}$, where $i, j = 1, ..., k$. The matrix $S(n)$ counts distinct isogenies between classes of elliptic curves, which makes it the adjacency matrix of the n-isogeny graph.

Definition 6.3.2 (Brandt matrix)**.** Let $T(n) \in M_k(\mathbb{Z})$ such that $T(n)_{i,j} = \#\mathcal{T}_{n,i,j}$ for $i, j = 1, ..., k$. Then $T(n)$ is called the n-Brandt matrix.

The n-Brandt matrix $T(n)$ is the adjacency matrix for a directed graph $\mathcal{G}_{p,n} = (\mathcal{V}_{p,n}, \mathcal{E}_{p,n})$, where

$$\mathcal{V}_{p,n} = \mathrm{Cls}\, O,$$
$$\mathcal{E}_{p,n} = \{\langle [I_i], [J] \rangle : n \cdot \mathrm{nrd}(I) = \mathrm{nrd}(J), J \subseteq I_i\}.$$

Remark 6.3.3. The matrices $S(n)$ and $T(n)$ depend on the distinct ordering of rows $i = 1, ..., k$ and columns $j = 1, ..., k$, which in turn depends on the choice of E_0. However, this does not affect the properties of the matrices as adjacency matrices; the graphs that they represent do not change with E_0.

By the result stated in [Voi17, paragraph 42.3.13], there exists a bijection between $\mathcal{T}_{n,i,j}$ and $\mathcal{S}_{n,i,j}$. Because the result includes no proof of this fact, one will be given in the remainder of this section.
To this end, let $I \subseteq O_0$ be a nonzero left O_0-ideal with $J \subset I$ such that

$$\mathrm{nrd}(J) = n \cdot \mathrm{nrd}(I). \tag{6.1}$$

Denote $E_{0,I} \coloneqq E_0/E_0[I]$ and $E_{0,J} \coloneqq E_0/E_0[J]$. By lemma 6.2.4, there exist isogenies

$$\phi_I : E_0 \to E_{0,I},$$
$$\phi_J : E_0 \to E_{0,J},$$

with $\ker \phi_I = E_0[I]$ and $\ker \phi_J = E_0[J]$. Recalling definition 6.2.3, $J \subset I$ implies that $E_0[I] \subseteq E_0[J]$. Then the homomorphism theorem implies that there exists an isogeny

$$\phi_{IJ} : E_{0,I} \to E_{0,J} \tag{6.2}$$

such that $\phi_J = \phi_{IJ} \circ \phi_I$. This is equivalent to commutativity of the following diagram:

$$\begin{array}{ccccc} & & E_{0,I} & & \\ & \overset{\phi_I}{\nearrow} & & \overset{\phi_{IJ}}{\searrow} & \\ E_0 & & \xrightarrow{\quad\phi_J\quad} & & E_{0,J} \end{array}$$

By proposition 6.2.6 and by (6.1), the degree of isogeny ϕ_{IJ} is given by

$$\deg \phi_{IJ} = \frac{\deg \phi_J}{\deg \phi_I} = \frac{\mathrm{nrd}(J)}{\mathrm{nrd}(I)} = n,$$

so $\#\ker \phi_{IJ} = n$. A map τ_n can then be defined as follows.

Definition 6.3.4. For $J \in \mathcal{T}_{n,i,j}$ such that $J \subseteq I_j \subseteq O_0$, let

$$\begin{aligned} \tau_n : \mathcal{T}_{n,i,j} &\to \mathcal{S}_{n,i,j}, \\ J &\mapsto \ker \phi_{I_j J}. \end{aligned} \tag{6.3}$$

To prove that τ_n is a bijection, which is formulated in proposition 6.3.7, the following lemma's will be needed.

Lemma 6.3.5. *If* $[I] = [J]$, *then* $E_{0,I} \cong E_{0,J}$.

Proof. Let $\mathbf{C}_{EC}$ denote the category of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ under isogenies and $\mathbf{C}_{O_0}$ the category of left O_0-modules under left O_0-module homomorphisms. By theorem 6.2.9, these categories are equivalent under the functor $G : E \mapsto \mathrm{Hom}(E, E_0)$. For $I, J \in \mathrm{Ob}_{\mathbf{C}_{O_0}}$, suppose that $[I] = [J]$.
Construct a skeleton $\mathbf{C}'_{O_0,I}$ containing I and a skeleton $\mathbf{C}'_{O_0,J}$ containing J which are both isomorphic to $\mathbf{C}_{O_0}$ under respective inclusion functors ι_I and ι_J. By corollary 6.1.11, skeletons of $\mathbf{C}_{EC}$ and $\mathbf{C}_{O_0}$ are isomorphic under F. So there exist (not necessarily distinct) skeletons of $\mathbf{C}_{EC}$ containing $E_{0,I}$ and $E_{0,J}$, so that

$$\begin{aligned} E_{0,I} &\cong I, \\ E_{0,J} &\cong J. \end{aligned}$$

These skeletons are isomorphic to $\mathbf{C}_{EC}$ under inclusion functors $\iota_{E_{0,I}}$ and $\iota_{E_{0,J}}$. Since skeletons of the same category are isomorphic by proposition 6.1.10.2, $[I] = [J]$ implies that $I \cong J$. This gives that

$$E_{0,I} \cong I \cong J \cong E_{0,J}.$$

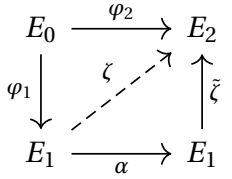
This is illustrated by the following diagram, where all isomorphic relations are denoted by G_i, $i = 1, \ldots, 6$:

$$\begin{array}{ccccccc} E_{0,I} & \xhookrightarrow{\iota_{E_{0,I}}} & E_{0,I} & \xrightarrow{G_2} & I & \xhookleftarrow{\iota_I} & I \\ \downarrow{\scriptstyle G_1} & & \downarrow{\scriptstyle G_3} & & \downarrow{\scriptstyle G_4} & & \downarrow{\scriptstyle G_5} \\ E_{0,J} & \xhookrightarrow{\iota_{E_{0,J}}} & E_{0,J} & \xrightarrow{G_6} & J & \xhookleftarrow{\iota_J} & J \end{array}$$

□

Lemma 6.3.6. *Let E_0, E_1 and E_2 be elliptic curves over $\overline{\mathbb{F}}_p$ such that $E_1 \cong E_2$. Suppose there exist isogenies $\varphi_1 : E_0 \to E_1$ and $\varphi_2 : E_0 \to E_2$. Then there exists an isomorphism $\zeta : E_1 \to E_2$ such that $\varphi_2 = \zeta \circ \varphi_1$.*

Proof. Suppose the isomorphism $E_1 \cong E_2$ is given by isogeny $\tilde{\zeta} : E_1 \to E_2$. Because φ_1 and φ_2 are isogenies, they are surjective by proposition 3.1.11. By comparing automorphisms on E_1, it is then possible to find $\alpha \in \mathrm{Aut}(E_1)$ such that $\varphi_1 \circ \alpha \circ \tilde{\zeta} = \varphi_2$. Choose $\zeta = \alpha \circ \tilde{\zeta}$ to obtain the desired isomorphism. This is equivalent to commutativity of the following diagram:



□

Proposition 6.3.7. *The map τ_n is a bijection.*

Proof. To prove the proposition, it suffices to construct a map $\sigma_n : \mathcal{S}_{n,i,j} \to \mathcal{T}_{n,i,j}$ such that $\sigma_n = \tau_n^{-1}$.
Let I_i and I_j be right invertible O_0-ideals (from here on referred to as 'O_0-ideals') and use notation $E_i \coloneqq E_{0,I_i}$, $E_j \coloneqq E_{0,I_j}$. By lemma 6.2.4, there exist isogenies

$$\varphi_{I_i} : E_0 \to E_i,$$
$$\varphi_{I_j} : E_0 \to E_j.$$

By lemma 6.2.5, then $I_i = \mathrm{Hom}(E_i, E_0)\varphi_{I_i}$ and $I_j = \mathrm{Hom}(E_j, E_0)\varphi_{I_j}$.
The goal of this proof is to first define σ_n and then show that $\sigma_n = \tau_n^{-1}$, which will be done in three steps.

1. As the first step the map σ_n will be defined.
   Let $H \in \mathcal{S}_n$, so that $\#H = n$ and $E_j/H \cong E_i$. By proposition 3.1.6, there exists an isogeny

   $$\varphi_H : E_j \to E_j/H$$

   with $\ker \varphi_H = H$. Now define the map σ_n as follows:

   $$\begin{aligned} \sigma_n : \mathcal{S}_n &\to \mathcal{T}_n, \\ H &\mapsto \mathrm{Hom}(E_j/H, E_0)(\varphi_H \circ \varphi_{I_j}) =: J'. \end{aligned} \tag{6.4}$$

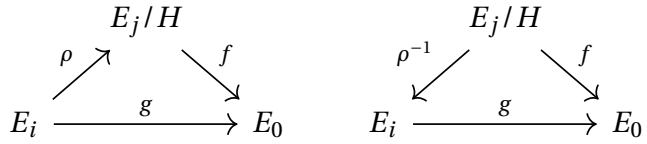
   For this map to be properly defined, it must be the case that $J' \in \mathcal{T}_{n,i,j}$.

   (a) First it must be shown that $J' \subseteq I_j$.
   Let $f \in \mathrm{Hom}(E_j/H, E_0)$. Then $f \circ \varphi_H : E_j \to E_0$, so $f \circ \varphi_H \in \mathrm{Hom}(E_j, E_0)$. For $f \circ \varphi_H \circ \varphi_{I_j} \in \mathrm{Hom}(E_j/H, E_0)(\varphi_H \circ \varphi_{I_j})$, then also $f \circ \varphi_H \circ \varphi_{I_j} \in \mathrm{Hom}(E_j, E_0)\varphi_{I_j}$. This indeed implies that $J' \subseteq I_j$.

   (b) This step will show that $[J'] = [I_i]$.
   Construct a map $\varphi_H \circ \varphi_{I_j} : E_0 \to E_j/H$. Since $E_j/H \cong E_i$, by lemma 6.3.6 there exists an isomorphism $\rho : E_i \to E_j/H$ such that

   $$\varphi_H \circ \varphi_{I_j} = \rho \circ \varphi_{I_i}. \tag{6.5}$$

Now let $f \in \mathrm{Hom}(E_j/H, E_0)$ and $g \in \mathrm{Hom}(E_i, E_0)$. Then $f \circ \rho \in \mathrm{Hom}(E_i, E_0)$ and $g \circ \rho^{-1} \in \mathrm{Hom}(E_j/H, E_0)$. The situation is illustrated by the following (not necessarily commutative) diagrams:



This gives that

$$\mathrm{Hom}(E_i, E_0) = \mathrm{Hom}(E_j/H, E_0)\rho. \tag{6.6}$$

Combining (6.5) and (6.6) results in

$$\begin{aligned} I_i &= \mathrm{Hom}(E_i, E_0)\varphi_{I_i} \\ &= \mathrm{Hom}(E_j/H, E_0)(\rho \circ \varphi_{I_i}) \\ &= \mathrm{Hom}(E_j/H, E_0)(\varphi_H \circ \varphi_{I_j}) \\ &= J'. \end{aligned}$$

By the above, $[J'] = [I_i]$.

(c) This step will prove that $\mathrm{nrd}(J') = n \cdot \mathrm{nrd}(I_j)$.
Since J' is an O_0-ideal by step 1a, use notation $E_{0,J'} \coloneqq E_0/E_0[J']$. By lemma 6.2.4, there exists an isogeny

$$\varphi_{J'} : E_0 \to E_{0,J'}.$$

In step 1b it was shown that $[J'] = [I_i]$, so by lemma 6.3.5 $E_{0,J'} \cong E_{I_i}$. Then it follows from proposition 3.1.9 that

$$\deg \varphi J' = \ker \varphi_{J'} = \ker \varphi_{I_i} = \deg \varphi_{I_i}.$$

Applying (1a) then gives that

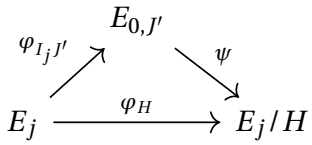
$$\begin{aligned} \deg \varphi_{J'} &= \deg \varphi_{I_i} \\ &= \deg \varphi_\rho \cdot \deg \varphi_{I_i} \\ &= \deg \varphi_H \cdot \deg \varphi_{I_j} \\ &= n \cdot \deg \varphi_{I_j}. \end{aligned}$$

The last equality follows from the fact that $\ker \varphi_H = H$. By finally applying theorem 6.2.6, the above implies that $\mathrm{nrd}\,(J') = n \cdot \mathrm{nrd}(I_j)$.

Steps 1a, 1b and 1c confirm that $J' \in \mathcal{T}_{n,i,j}$.

2. In this step it will be shown that $\tau_n \circ \sigma_n = id_{\mathcal{S}_{n,i,j}}$.
Let $H \in \mathcal{S}_{n,i,j}$ so that $\sigma_n(H) = J'$, where J' is defined as in (6.4). Following the reasoning preceding (6.2), there exists an isogeny $\varphi_{I_j J'} : E_j \to E_{0,J'}$. This gives that $\tau_n(J') = \ker \varphi_{I_j J'}$. It will now be shown that $\ker \varphi_{I_j J'} = H$.
Because $H \in \mathcal{S}_{n,i,j}$, it is known that $E_j/H \cong E_i$. In step 1b it was shown that $[J'] = [I_i]$, so $E_{0,J'} \cong E_i$. This also implies that $E_{0,J'} \cong E_j/H$. By lemma 6.3.6 there then exists an

isomorphism $\psi : E_{0,J'} \to E_j/H$ such that $\varphi_H = \psi \circ \varphi_{I_j J'}$. This is equivalent to commutativity of the following diagram:



Finally, this gives that

$$\begin{aligned} H &= \ker \varphi_H \\ &= \ker \psi \circ \varphi_{I_j J'} \\ &= \ker \varphi_{I_j J'}, \end{aligned}$$

where the last equality follows from the fact that $\ker \psi$ is trivial. This proves that $(\tau_n \circ \sigma_n)(H) = H$ and therefore that $\tau_n \circ \sigma_n = id_{\mathcal{S}_{n,i,j}}$.

3. In this step it will be shown that $\sigma_n \circ \tau_n = id_{\mathcal{T}_{n,i,j}}$.
Let $J \in \mathcal{T}_{n,i,j}$, so that $\mathrm{nrd} J = n \cdot \mathrm{nrd} I_j$ and $[J] = [I_i]$. The latter implies by lemma 6.3.5 that $E_{0,J} \cong E_i$. Because J is an O_0-ideal, use notation $E_{0,J} \coloneqq E_0/E_0[J]$. By lemma 6.2.4, there exists isogeny

$$\varphi_J : E_0 \to E_{0,J}.$$

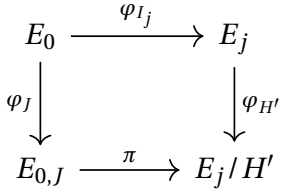
Following lemma 6.2.5, ideal J can also be written as $J = \mathrm{Hom}(E_{0,J}, E_0)\varphi_J$. Define a map $\varphi_{I_j J} : E_j \to E_{0,J}$ as in (6.2). Then $\tau_n(J) = \ker \varphi_{I_j J} \coloneqq H'$. It will now be shown that $\sigma_n(H') = J$.
Since H' is a finite subgroup of E_j, by proposition 3.1.6 there exists an isogeny

$$\varphi_{H'} : E_j \to E_j/H'$$

where $\ker \varphi_{H'} = H' = \ker \varphi_{I_j J}$. Then proposition 3.1.8 implies that $E_j/H' \cong E_{0,J}$ and therefore that $E_j/H' \cong E_i$. By lemma 6.3.6, there exists an isomorphism
$\pi : E_{0,J} \to E_j/H'$ such that

$$\varphi_{H'} \circ \varphi_{I_j} = \pi \circ \varphi_J. \tag{6.7}$$

This is equivalent to commutativity of the following diagram:



A similar argument as given in step 1b to justify (6.6), implies here that

$$\mathrm{Hom}(E_{0,J}, E_0) = \mathrm{Hom}(E_j/H, E_0)\pi. \tag{6.8}$$

Applying (6.7) and (6.8) then gives that

$$\begin{aligned} \mathrm{Hom}(E_j/H', E_0)(\varphi_{H'} \circ \varphi_{I_j}) &= \mathrm{Hom}(E_j/H, E_0)(\pi \circ \varphi_J) \\ &= \mathrm{Hom}(E_{0,J}, E_0)\varphi_J \\ &= J. \end{aligned}$$

This proves that $(\sigma_n \circ \tau_n)(J) = J$ and therefore that $\sigma_n \circ \tau_n = id_{\mathcal{T}_{n,i,j}}$.

Steps 2 and 3 prove that $\sigma_n = \tau_n^{-1}$, so τ_n is a bijection. □

Proposition 6.3.7 implies that $\mathcal{T}_{n,i,j} \cong \mathcal{S}_{n,i,j}$ and therefore $T(n) = \#\mathcal{T}_{n,i,j} = \#\mathcal{S}_{n,i,j} = S(n)$. This means that for an n-Brandt matrix $T(n)$, entry $T(n)_{i,j}$ is the number of isogenies from vertex $j(E_i)$ to vertex $j(E_j)$ in an n-isogeny graph.

7. Non-backtracking walks on supersingular isogeny graphs

In chapter 6 it was shown that Brandt matrices are adjacency matrices of supersingular isogeny graphs. The current chapter describes how they can be used to recreate the results in [Tho17, section 7.3 and 7.4]. The efficiency of this method is tested by timing the generation of Brandt matrices and adjacency matrices for supersingular isogeny graphs (referred to as 'isogeny graphs'). Section 7.1 discusses preliminaries regarding the procedure in Sage and a recurrence relation for non-backtracking matrices. This is followed by the results for distributions of $j(E_A)$, $j(E_B)$ and $j(E_{AB})$ in sections 7.2 and 7.3. A discussion of the results and concluding remarks follow in chapter 8.

7.1. Preliminaries

Where [Tho17] simulates 500 walks on isogeny graphs to approximate the distribution of $j(E_A)$, $j(E_B)$ and $j(E_{AB})$, Brandt matrices can be used to compute a matrix containing the exact distribution. The details and results of this are discussed in sections 7.2 and 7.3.
The following code creates the Brandt module B for a finite field $\mathbb{F}_p$ (see [Koh]) and then computes the Hecke matrix for this module and prime n (see [hec]).

```
B = Brandtmodule(p)
B.hecke_matrix(n)
```

Here the Hecke matrix is the n-Brandt matrix given a finite field $\mathbb{F}_p$. Similarly, the following code creates a supersingular module M (see [sup]) for the supersingular elliptic curve case followed by generating the Hecke matrix for this module and prime n.

```
M = Supersingular(p)
M.hecke_matrix(n)
```

Here the Hecke matrix is the adjacency matrix of the n-isogeny graph given a finite field $\mathbb{F}_p$. The choice for E_0 is made within the command that generates the Hecke matrix and is therefore not explicitly mentioned in this chapter. Since E_0 is not the same for each generated matrix, it can happen that $T(n) \neq S(n)$. However, they can still be considered equal as adjacency matrices of supersingular isogeny graphs (see also remark 6.3.3).
Fixing E_0 for the above reason and continuing the notation of section 6.3, let

$$S(n)_{i,j} = \#\{H \subseteq E_j(\overline{\mathbb{F}}_p) : E_j/H \simeq E_i, \#H = n\}.$$

The matrix $S(n)$ is the adjacency matrix of a supersingular n-isogeny graph. In the SIDH protocol only non-backtracking walks are of interest, so only cyclic subgroups H will be taken into account. To count just the non-backtracking walks, define a new matrix

$$S'(n)_{i,j} = \#\{H \subseteq E_i(\overline{\mathbb{F}}_p) : E_i/H \cong E_j, \#H = n, H \text{ cyclic}\}. \tag{7.1}$$

For any prime ℓ then $S'(\ell) = S(\ell)$, because subgroups of prime order are always cyclic. Where $S'(\ell)^e_{i,j} = S(\ell)^e_{i,j}$ is the number of walks of length e from a vertex i to a vertex j, then $S'(\ell^e)_{i,j}$

is the number of non-backtracking walks of length e between i and j. For Alice the matrix $S'(\ell_A^{e_A})$ gives the distribution of all possible non-backtracking walks of length e_A in ℓ_A-isogeny graph $\mathcal{G}_{\ell_A}$, which is equal to the distribution of $j(E_A)$. Similarly, for Bob the matrix $S'(\ell_B^{e_B})$ gives the distribution of $j(E_B)$. The distribution of $j(E_{AB})$ is given by the matrix $S'(\ell_A^{e_A})S'(\ell_B^{e_B}) = S'(\ell_B^{e_B})S'(\ell_A^{e_A})$.
It is possible to construct a recurrence relation to obtain such a matrix $S'(\ell^e)$. Recall that for $e = 1$, simply $S'(\ell^1) = S(\ell)$. For $e = 2$, the only possible backtracking walk starting from any vertex is to an arbitrary adjacent vertex and back to itself. By proposition 3.2.6, for each vertex in an ℓ-isogeny graph this is possible in $\ell + 1$ different ways. In terms of adjacency matrices this is represented by $(\ell + 1)I$, where I is the identity matrix. The matrix of non-backtracking walks of length 2 is then given by

$$S'(\ell^2) = S'(\ell)^2 - (\ell + 1)I. \tag{7.2}$$

For $e \geq 3$, the following theorem and corollary give a recurrence relation to obtain $S'(\ell^e)$.

Theorem 7.1.1. *Let a, b be positive integers and let $(a, b) \coloneqq gcd(a, b)$. Then*

$$S'(a)S'(b) = \sum_{d|(a,b)} dS'(\frac{ab}{d^2}).$$

Proof. See [Apo90, theorem 6.13]. □

Corollary 7.1.2. *The matrix containing all non-backtracking walks of length e on ℓ-isogeny graph $\mathcal{G}_{p,\ell}$ is given by*

$$S'(\ell^e) = S'(\ell^{e-1}) \cdot S'(\ell) - \ell \cdot S'(\ell^{e-2}). \tag{7.3}$$

Proof. Choose $a = \ell^{e-1}$, $b = \ell$ and apply theorem 7.1.1. □

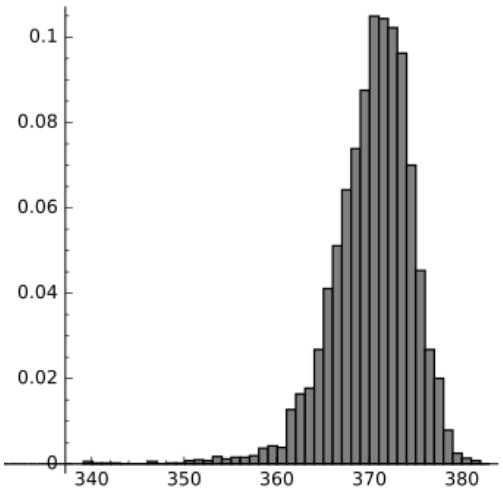
The results of section 6.3 imply that $T'(\ell^e) = S'(\ell^e)$, where $T'(\ell^e)$ is the non-backtracking version of $T(\ell)^e$. To obtain the results in sections 7.2 and 7.3, $T'(\ell_A^{e_A})$ and $T'(\ell_B^{e_B})$ were computed using the recurrence relation in equation 7.3.
To compare efficiency of the quaternion algebra method and the supersingular elliptic curve method, the generation of matrices $T'(\ell_A)$ and $T'(\ell_B)$ by both methods was timed for $\ell_A = 2, \ell_B = 3$ and $p = 2^8 3^5 - 1$. This was done by timing the generation of the Hecke matrix 10 times for both modules, giving the results in table 7.1. The results show that the Brandt matrix is not generated faster than the matrix based on supersingular elliptic curves (SSEC). The Brandt matrix for Bob is computed faster than the one for Alice, while the opposite occurs for the SSEC matrix.

	Brandt matrix	SSEC matrix
Alice ($\ell = 2$)	438.42961	14.82953
Bob ($\ell = 3$)	286.90380	55.34492

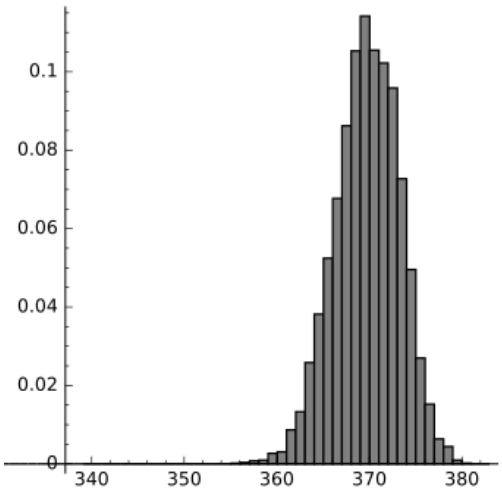
Table 7.1: The time taken (in seconds) to generate Brandt matrices and supersingular elliptic curve (SSEC) matrices for Alice and Bob. The table shows the mean results of 10 repetitions.

7.2. Distribution of $j(E_A)$ and $j(E_B)$

Let $\mathcal{G}_{p,\ell_A}$ be the ℓ_A-isogeny graph for Alice and let $p = \ell_A^{e_A}\ell_B^{e_B} - 1$. Computing the matrix $T'(\ell_A^{e_A})$ results in the distribution of all possible non-backtracking walks of length e_A in $\mathcal{G}_{p,\ell_A}$. From a single starting vertex there are $(\ell_A+1)\ell_A^{e_A-1}$ such walks. The entries in each column j sum up to $(\ell_A+1)\ell_A^{e_A-1}$. By remark 3.2.5, the entries in each row i will sum up to $(\ell_A+1)\ell_A^{e_A-1}$ only if $p \equiv 1 \mod 12$, in which case $T'(\ell_A^{e_A})$ is symmetric.
The heuristic estimation is given by 4.2.1, following [Tho17, estimation 7.3.1]. This estimation was tested by computing $T'(\ell_A^{e_A})$ for $\ell_A = 2, \ell_B = 3, e_A = 8, e_B = 5$. Here $p = 2^8 3^5 - 1$, for which $T'(\ell_A^{e_A}) \in M_{5185}(\mathbb{Z})$. For each column in $T'(\ell_A^{e_A})$ the nonzero entries are counted, indicating the number of distinct end points of the walk. The results are shown in figure 7.1. This process is repeated for Bob's non-backtracking walks of length e_B on ℓ_B-isogeny graph $\mathcal{G}_{p,\ell_B}$, by generating $T'(\ell_B^{e_B}) \in M_{5185}(\mathbb{Z})$. Bob's results are shown in figure 7.2.
Similar to what was found in [Tho17], comparing figure 7.1b to figure 7.1a and figure 7.2b to figure 7.2a, the results for heuristic estimation 4.2.1 approximate the distributions well, even for a relatively small prime.

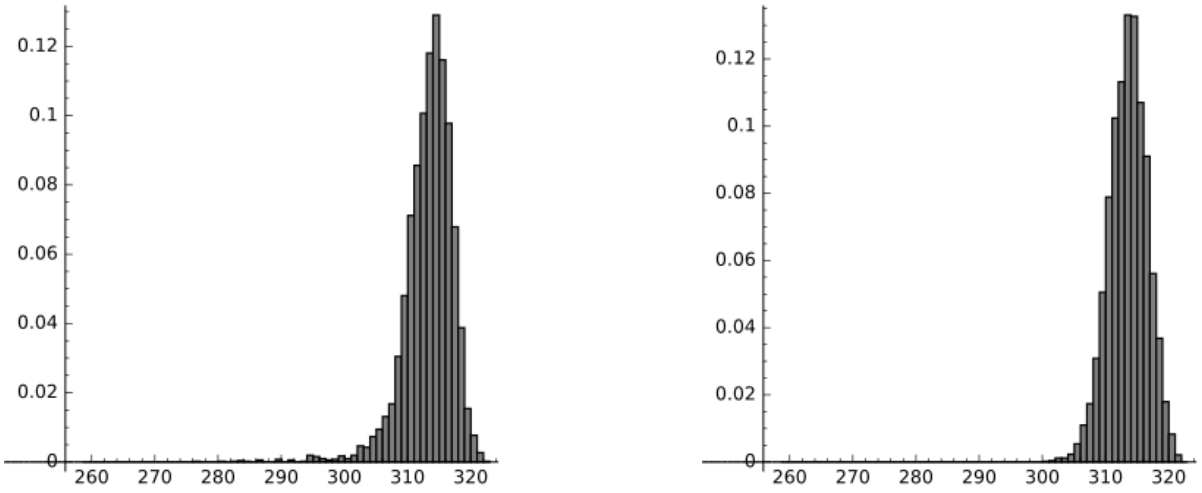


(a) Results for $j(E_A)$.



(b) Results for S_A (see estimation 4.2.1).

Figure 7.1: Alice's results for $p = 2^8 3^5 - 1$. The histograms shows the fraction of starting vertices $j(E_0)$ (vertical axis) that result in x distinct vertices $j(E_A)$ (horizontal axis). These results are equivalent to [Tho17], figures 2 and 3 in section 7.3.



(a) Results for $j(E_B)$.

(b) Results for S_B (see estimation 4.2.1)

Figure 7.2: Bob's results for $p = 2^8 3^5 - 1$. The histograms show which fraction of vertices (vertical axis) has been chosen x times (horizontal axis). These results are compared to [Tho17, figures 2, 3, 4 and 5, section 7.3].

7.3. Distribution of $j(E_{AB})$

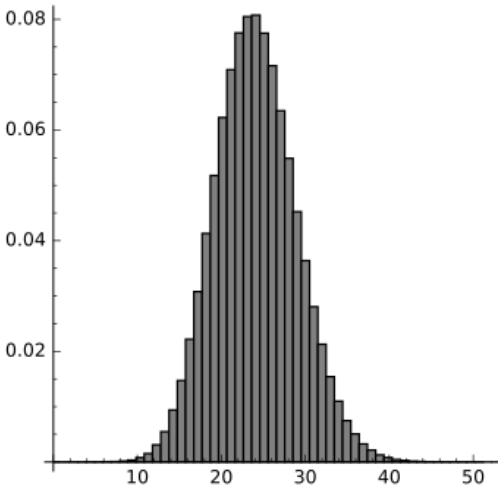
Let $\mathcal{G}_{p,\ell_A}$ be the ℓ_A-isogeny graph for Alice and $\mathcal{G}_{p,\ell_B}$ the ℓ_B-isogeny graph for Bob. For respective non-backtracking walks of length e_A and e_B, as in section 7.2 the distribution of these walks are represented by matrices $T'(\ell_A^{e_A})$ and $T'(\ell_B^{e_B})$. The matrix $T'(\ell_A^{e_A})T'(\ell_B^{e_B})$, represents all possible walks by Alice from starting vertex E_0 to E_A and then by Bob from E_A to E_{AB}. Since $T'(\ell_A^{e_A})T'(\ell_B^{e_B}) = T'(\ell_B^{e_B})T'(\ell_A^{e_A})$, this is the same as Bob first walking from E_0 to E_B and Alice walking from E_B to E_{BA}. The resulting matrix gives the distribution of $j(E_{AB}) = j(E_{BA})$.
The heuristic estimation is given by 4.2.2, following [Tho17, estimation 7.4.1]. This estimation was also tested for $\ell_A = 2, \ell_B = 3, e_A = 8, e_B = 5$, for which $p = 2^8 3^5 - 1$. To be able to comment on the accuracy of estimation 4.2.2, it is compared to the following naive estimation.

Estimation 7.3.1. Construct multiset S^* as follows:

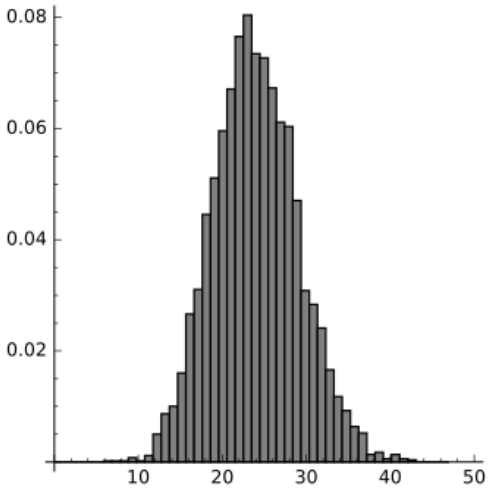
- Pick $\ell_A^{e_A-1}(\ell_A+1)\ell_B^{e_B-1}(\ell_B+1)$ vertices (j-invariants) uniformly at random. Each time a vertex is picked, store it in S^*.

In a naive sense, the distribution of $j(E_{AB})$ is estimated to be the same as when picking an element from S^* uniformly at random.

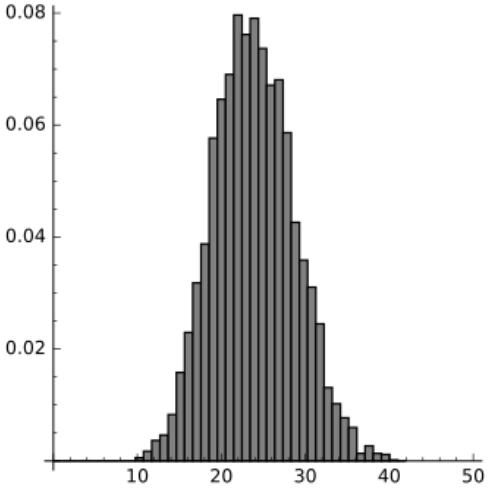
For each distinct entry x in $T'(\ell_A^{e_A})T'(\ell_B^{e_B})$ it was counted how many end nodes $j(E_{AB})$ occur x times. The results are shown in figure 7.3. When comparing figure 7.3a to figure 7.3b, the estimation approximates the distribution quite well. Moreover, figure 7.3c also approximates figure 7.3a well.



(a) Results for $j(E_{AB})$.



(b) Results for S (see estimation 4.2.2).



(c) Results for S^* (see estimation 7.3.1).

Figure 7.3: The results for the secret key for $p = 2^8 3^5 - 1$. The histograms show the fraction of possible vertices $j(E_{AB})$ (vertical axis) that occurs x times (horizontal axis). Figures (a) and (b) are compared to [Tho17, figures 14 and 15, section 7.4].

8. Conclusion

The theoretical background in chapters 2 to 5 and in particular chapter 6 allow the experiments in chapter 7. The results in sections 7.2 and 7.3 show that in case $p = 2^8 3^5 - 1$, finding the distributions of $j(E_A), j(E_B), j(E_{AB})$ through computation of Brandt matrices gives approximately equally strong results as found in [Tho17] by simulating walks on supersingular isogeny graphs. Generating Brandt matrices was also attempted for larger primes, where $T'(2^9), T'(3^6) \in M_{155521}(\mathbb{Z})$ for $p = 2^9 3^6 5 - 1$ and $T'(2^{10}), T'(3^6) \in M_{435457}(\mathbb{Z})$ for $p = 2^{10} 3^6 7 - 1$. The available memory capacity was not sufficient to compute and store dense matrices of these sizes. In the first case, a rough estimation of the necessary amount of memory is given by 8 bits times 155521^2 entries, which would amount to approximately 180 GB. It is possible that additional data besides the matrix is stored by the Sage command that generates the Hecke matrix, which causes it to increase memory usage even more. If all information stored in a Brandt matrix of size k would be computed via simulation of walks on isogeny graphs, in Alice's case this is equivalent to performing $k(\ell_A + 1)\ell^{e_A}$ random walks in a simulation. This is much more than necessary. Instead of finding the complete distribution by computing an entire matrix, it may be possible to simulate a lower number of "walks" via quaternion algebras, as was done for walks on supersingular isogeny graphs by [Tho17]. A topic for further research is to look into the code for the Sage commands that were used and how to optimize this for such a simulation.

The mean times taken to generate Brandt and supersingular elliptic curve (SSEC) matrices, shown in table 7.1, suggest that finding the distribution through Brandt matrices is slower than through SSEC's. A notable difference in both cases is whether the matrix is generated faster for Alice or Bob. In the Brandt case this is Bob, but in the SSEC case this is Alice. A possible explanation for this is that a different amount of preparatory computations is made and cached by Sage. For example, in the SSEC case first all j-invariants could be computed and stored. Finding out where this difference comes from by again studying the code of the built-in commands would make a good topic for further investigation. Furthermore, the efficiency of both methods has now only been tested by timing the matrix generation process. Although it is a good indication of mutual differences between the methods (specially since the difference between the Brandt and SSEC case is so large), the exact result depends on the used hardware. The efficiency of both methods could be researched further and more accurately, for example by tracking which and how much data is saved intermittently.

When improving the experiments in such a way that it is possible to use larger primes than $p = 2^8 3^5 - 1$, naive estimation 7.3.1 should be compared to estimation 4.2.2 to see if it produces notable differences. In section 7.3 it was shown that this does not truly happen for $p = 2^8 3^5 - 1$. If this is also not the case for larger primes, that may indicate both estimations work equally well.

References

[AHS04] Jiří Adámek, Horst Herrlich, and George E. Strecker. Abstract and Concrete Categories. http://katmat.math.uni-bremen.de/acc/, 2004. [Online; accessed May 2018].

[Apo90] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, New York, 1990.

[Awo06] Steve Awodey. *Category Theory*. Clarendon Press, Oxford, 2006.

[BCNE+18] Efrat Bank, Catalina Camacho-Navarro, Kirsten Eisenträger, Travis Morrison, and Jennifer Park. Cycles in the supersingular l-isogeny graph and corresponding endomorphisms. *ArXiv e-prints*, 2018.

[DPV06] Sanjoy Dasgupta, Christos H. Papadimitriou, and Umesh Vazirani. *Algorithms*. McGraw-Hill, Inc., 2006.

[Feo17] Luca De Feo. Mathematics of Isogeny Based Cryptography. 2017.

[FJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[Gal12] Stephen D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, New York, 2012.

[GPST16] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the Security of Supersingular Isogeny Cryptosystems. Cryptology ePrint Archive, Report 2016/859, 2016. https://eprint.iacr.org/2016/859.

[hec] Sage documentation: Modular forms and hecke operators. http://doc.sagemath.org/html/en/thematic_tutorials/explicit_methods_in_number_theory/modular_forms_and_hecke_operators.html. [Online; accessed June 2018].

[His14] Jordan Hisel. Addition Law on Elliptic Curves. http://math.uchicago.edu/~may/REU2014/REUPapers/Hisel.pdf, 2014. [Online; accessed July 2018].

[JF11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Post-Quantum Cryptography Lecture Notes in Computer Science*, page 19âĂŞ34, 2011.

[Koh] David R. Kohel. Brandt Modules. http://iml.univ-mrs.fr/~kohel/alg/index.html. [Online; accessed June 2018].

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484âĂŞ1509, 1997.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Science & Business Media, 2009.

[sup] Sage documentation: Module of supersingular points. `http://doc.sagemath.org/html/en/reference/modmisc/sage/modular/ssmod/ssmod.html`. [Online; accessed June 2018].

[Tho17] Erik Thormarker. Post-Quantum Cryptography: Supersingular Isogeny Diffie-Hellman Key Exchange. Master's thesis, 2017.

[Voi17] John Voight. Quaternion Algebras. `https://math.dartmouth.edu/~jvoight/quat.html`, 2017. [Online; accessed April 2018].

[Was08] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Taylor & Francis Group, 2008.

[Wil96] Robin J. Wilson. *Introduction to Graph Theory*. Longman Group Ltd, 4 edition, 1996.