Random sampling of supersingular elliptic curves

Marzio Mula Nadir Murru Federico Pintore

May 3, 2022

Abstract

We consider the problem of uniformly sampling supersingular elliptic curves over finite fields of cryptographic size (SRS problem). The currently best-known method combines the reduction of a suitable CM j-invariant and a random walk over some isogeny graph. Unfortunately, this method is not suitable for cryptographic applications because it leaks too much information about the endomorphism ring of the generated curve. This fact motivates a stricter version of the SRS problem, requiring that the sampling algorithm gives no extra information about the endomorphism ring of the output curve (cSRS problem). The known cSRS algorithms work only for small finite fields, since they involve the computation of polynomials of large degree. In this work we formally define the SRS and cSRS problems, we discuss the relevance of cSRS for cryptographic applications, and we provide a self-contained survey of the known approaches to both the problems. Afterwards, we describe and analyse some alternative techniques, based either on Hasse invariant or division polynomials, and we explain the reasons why these techniques do not readily lead to efficient cSRS algorithms.

1 Introduction

The problem of sampling supersingular elliptic curves over $\overline{\mathbb{F}}_p$, or *SRS problem*, is not as easy as drawing marbles from a bag: when p is large, the best known algorithms are only able to extract a negligible fraction of all the existing supersingular elliptic curves. The others can be sampled 'indirectly' as the endpoints of random walks. In other words, they cannot be reached without first passing through one of those few supersingular elliptic curves which we are able to sample directly. Surprisingly enough, this would not be a problem if our only purpose was to efficiently sample uniformly random supersingular elliptic curves. However, cryptographic applications require more: the curve should be sampled in such a way that its endomorphism ring remains unknown. In fact, this further requirement rules out any known efficient method for sampling supersingular elliptic curves, leaving us with an open problem that we call *cSRS problem*.

Although the cSRS problem is well-known in literature [Vit19, p. 71; CPV20, p. 3], we believe that its importance is not stressed enough: therefore, the first goal of this article is to provide a short and essentially self-contained introduction to the problem, motivating its appeal from both a mathematical and cryptographic point of view. In particular, Section 2.5 recalls the main features of supersingular isogeny graphs following [AAM19] and [DFJP14], while Section 3.2 gathers some cryptographic protocols that could benefit from an efficient solution of the SRS problem, ranging from CGL hash function to SIDH [CLG09; DFJP14; Pet17].

Our second goal consists in surveying some known approaches to the SRS and cSRS problems: this is done in Section 4. We first give a thorough theoretical explanation of Bröker's algorithm [Brö09]. It is based on the the deep connection, already observed by Deuring in [Deu41], between CM elliptic curves over number fields and elliptic curves over finite fields. In fact, the only known way to sample a supersingular elliptic curve modulo large primes consists in reducing modulo p some suitably chosen CM curve. Later on, we consider some standard characterizations of supersingular elliptic curves, which lead to two highly inefficient methods for sampling supersingular elliptic curves: exhaustive search over randomly sampled elliptic curves, and root-finding on a polynomial of large degree (Hasse invariant). In Sections 4.2 and 4.3 we explain why the reduction of CM curves is not a good approach to the SRS problem, since it ends up either requiring an excessive computational cost or revealing the endomorphism ring of the output [LB20; CPV20]. We would like to highlight that a comprehensive and clarifying explanation of these issues is still lacking.

Finally, we make a step further, exploring other ways to sample supersingular elliptic curves without making use of CM curves, with the hope of opening new research directions:

- In Section 5, we compute the Hasse invariant of other models of elliptic curves. In Theorem 4.17, a classic result about the Hasse invariant is extended to elliptic curves in Jacobi form. In Proposition 5.10 we also prove a special property of the Hasse invariant of a supersingular elliptic curve in Montgomery form: namely, it splits completely over $\mathbb{F}_{p^2}$.
- In Section 6.2, we prove a slight generalization of a result in [Dol18] (Proposition 6.7), from which we deduce another explicit characterization of supersingular elliptic curves in terms of their p-th division polynomial.
- In Section 6.3, under further assumptions on the prime p, we formulate another characterization of supersingular elliptic curves based on $\mathbb{F}_p$-rational points of small torsion.

2 Preliminaries

2.1 Elliptic curves

Let K be a perfect field with $\operatorname{char} K \notin \{2, 3\}$. An *elliptic curve* over K is a projective curve that can be written, up to birational equivalence, as a cubic in $\mathbb{A}^2(K)$ in *(short) Weierstrass form*

$$y^2 = x^3 + Ax + B \qquad \text{with } A, B \in K \tag{1}$$

having a base point at infinity O and such that the *discriminant*, $\Delta(E) = -16(4A^3 + 27B^2)$, is not 0.

Every isomorphism class of elliptic curves over K can be uniquely identified with an element $j \in K$, called j-*invariant*. The value of j can be easily retrieved from the coefficients of any curve $E\colon y^2 = x^3 + Ax + B$ in the isomorphism class as

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)}.$$

We recall from [Sil09, Prop. 1.4.b-c] the fundamental properties of the j-invariant.

Proposition 2.1.

(a) Two elliptic curves over K are isomorphic if and only if they have the same j-invariant.

(b) Let $j_0 \in \overline{K}$. There exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.

Every elliptic curve E can be endowed with the structure of an abelian group $(E, +)$ [Sil09, § III.2] whose zero element is O.

Since elliptic curves are defined up to birational equivalence, there exist various representations other than the Weierstrass model considered above. In Table 1, we summarise the form of the affine equation and the corresponding definition of the j-invariant for some of these alternative models. We also provide the values of the coefficients A and B of a birationally equivalent Weierstrass model.

2.2 Isogenies

An *isogeny* between two elliptic curves E_1, E_2 over K is a morphism

$$\varphi\colon E_1 \to E_2$$

such that $\varphi(O) = O$. We say that φ is a K-*isogeny*, or that φ is *defined over* K, if the rational functions defining φ can be chosen with coefficients in K. We refer to [Sil09, § III.4] for the basic properties of isogenies and the definition of degree.

For each positive integer m, let $[m]$ denote the 'multiplication-by-m' map

$$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}}.$$

The above definition easily extends to negative integers, setting $[-m]P = -([m]P)$. For each $m \in \mathbb{Z}$, the m-*torsion* of E is the subgroup $E[m] = \ker[m]$.

Table 1: Other models of elliptic curves

Model	Affine equation	j-invariant	Equivalent Weierstrass model
Legendre [Sil09, p. 49]	$y^2 = x(x-1)(x-\lambda)$	$2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$	$\begin{cases} A = \frac{-\lambda^2+\lambda-1}{3} \\ B = \frac{-2\lambda^3+3\lambda^2+3\lambda-2}{27} \end{cases}$
Montgomery [CS17, § 2.4]	$B'y^2 = x^3 + A'x^2 + x$	$\frac{256(A'^2-3)^3}{A'^2-4}$	$\begin{cases} A = B'^2 \left(1 - \frac{A'^2}{3}\right) \\ B = \frac{B'^3 A'}{3} \left(\frac{2A'^2}{9} - 1\right) \end{cases}$
Jacobi [BJ03, § 3]	$y^2 = \epsilon x^4 - 2\delta x^2 + 1$	$64 \frac{(\delta^2+3\epsilon)^3}{\epsilon(\delta^2-\epsilon)^2}$	$\begin{cases} A = -4\epsilon - \frac{4}{3}\delta^2 \\ B = -\frac{16}{27}\delta(\delta^2 - 9\epsilon) \end{cases}$

Denote by $\operatorname{End}(E)$ the set of endomorphisms (that is, isogenies $E \to E$) of an elliptic curve E. Since $\operatorname{End}(E)$ is torsion-free, the map

$$\begin{aligned} [\ ]\colon \mathbb{Z} &\to \operatorname{End}(E) \\ m &\mapsto [m] \end{aligned}$$

is injective. Endomorphisms in the image of the injective map $[\ ]$ are called *trivial*. Whenever the map $[\ ]$ is *not* surjective, that is, there exists some non-trivial endomorphism, we say that E is a *CM curve*, or, equivalently, that E has *complex multiplication*. CM curves defined over number fields can be used as a starting point for generating supersingular elliptic curves, as we are going to see in Section 4.

Proposition 2.2. *Let $\varphi\colon E_1 \to E_2$ be a nonconstant isogeny of degree m. Then there exists a unique isogeny*

$$\hat{\varphi}\colon E_2 \to E_1$$

such that $\hat{\varphi} \circ \varphi = [m]$.

Proof. See [Sil09, Thm. 6.1.a]. □

The isogeny $\hat{\varphi}$ is called *dual isogeny*. We also define $\widehat{[0]} = [0]$.

2.3 Endomorphism rings

In this section we gather the fundamental facts about the structure of $\operatorname{End}(E)$ for an elliptic curve E. We first recall the following definitions:

- An algebra B over a field K (with $\operatorname{char} K \neq 2$) is a *quaternion algebra* if there exist $i, j \in B$ such that $1, i, j, ij$ form a basis for B and
$$i^2 = a, \qquad j^2 = b, \qquad ji = -ij \tag{2}$$
for some $a, b \in K^*$.
- Let B be an algebra of finite dimension n over $\mathbb{Q}$. An *order* $\mathcal{O} \subset B$ is a $\mathbb{Z}$-module of rank n which is also a subring.

For example, if we take $B = K$, where K is a quadratic extension of $\mathbb{Q}$, and denote by $\mathcal{O}_K$ its ring of integers, one can prove that the orders in K are exactly the rings $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, where f is a positive integer called the *conductor* of $\mathcal{O}$ [Cox13, Lemma 7.2].

Theorem 2.3 (Structure of $\operatorname{End}(E)$)**.** *Let E be an elliptic curve over K. Then $\operatorname{End}(E)$ is either $\mathbb{Z}$, an order in an imaginary quadratic extension of $\mathbb{Q}$, or an order in a quaternion algebra over $\mathbb{Q}$. If K has characteristic 0, the last case never occurs.*

Proof. [Sil09, Cor. III.9.4]. ☐

Corollary 2.4 (Characteristic polynomial of an endomorphism)**.** *Let φ be an endomorphism of an elliptic curve E over K, and define*

$$d = \deg \varphi \qquad \textit{and} \qquad a = 1 + \deg \varphi - \deg(1 - \varphi).$$

Then

$$\varphi^2 - [a] \circ \varphi + [d] = [0]. \tag{3}$$

Proof. This can be checked directly using the properties of dual isogenies. ☐

The integer a from Corollary 2.4 is called the *trace* of φ and denoted by $\mathrm{tr}(\varphi)$. In particular, when E is defined over a finite field $\mathbb{F}_q$ of characteristic p, the map

$$\begin{aligned} \varphi_q \colon E &\to E \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

is called the *q-th power Frobenius endomorphism E*, and its trace is the *trace of E* over $\mathbb{F}_q$. Moreover, its degree equals q [Sil09, Prop. II.2.11], so that (3) yields

$$\left(x^{q^2}, y^{q^2}\right) - [\mathrm{tr}(\varphi_q)](x^q, y^q) + [q](x, y) = O$$

for each $(x, y) \in E(\overline{\mathbb{F}_q})$.

2.4 Supersingular elliptic curves

We will now recall some characterizations of supersingular elliptic curves. Such criteria for supersingularity will be employed in Sections 4,5 and 6 to generate supersingular curves. In the following, we will use p for a prime number and q for a generic power of p.

Theorem 2.5 (Definitions of supersingular elliptic curve)**.** *Let K be a perfect field of characteristic p, and let E be an elliptic curve over K. For each $r \geq 1$ let*

$$\varphi_r \colon E \to E^{(p^r)}$$

be the p^r-th power Frobenius map. Then the following are equivalent:

(a) $E[p^r] = 0$ *for each $r \geq 1$.*

(b) The endomorphism $[p] \colon E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.

(c) $\mathrm{End}(E)$ *is an order in a quaternion algebra.*

If an elliptic curve satisfies one of the previous conditions, it is called supersingular.

Proof. See [Sil09, Thm. 3.1]. ☐

Corollary 2.6. *Every supersingular curve defined over a field of characteristic p is isomorphic to a supersingular curve defined over $\mathbb{F}_{p^2}$.*

Proof. This is an immediate consequence of part (b) of the previous Theorem and the properties of j-invariants in Proposition 2.1. ☐

For supersingular elliptic curves there is also another characterization which takes into account the number of $\mathbb{F}_q$-rational points:

Theorem 2.7. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and $\varphi \colon E \to E$ the q-th power Frobenius endomorphism. Then E is supersingular if and only if*

$$\mathrm{tr}(\varphi) \equiv 0 \mod p$$

or, equivalently,

$$\#E(\mathbb{F}_q) \equiv 1 \mod p.$$

Proof. See [Was08, Prop. 4.31]. ☐

2.5 Isogeny graphs

Supersingular isogeny graphs are a major object of study in isogeny-based cryptography. Their peculiar structure allows 'walking' from an elliptic curve to another in such a way that

- each step can be performed quickly (via Vélu's formulae: see [Gal18, § 25.1.1; Vél71]);
- starting from a given supersingular elliptic curve, every other supersingular elliptic curve can be reached within a small number of steps;
- the endpoints of random walks have an 'almost uniform' distribution (*rapid mixing*).

In this section, we provide a general introduction to random walks over graphs, showing the relation between the 'randomness' of a random walk and the structure of the corresponding graph. Finally, referring to a famous result due to Pizer in [Piz98], we show that random walks on suitably chosen isogeny graphs of supersingular elliptic curves actually land on 'random' vertices.

2.5.1 Random walks

In this section we mainly follow [Lov96, § 1; Ter99, § 6].

Let G be a graph with set of vertices V and set of vertices E. A *random walk* on G is the stochastic process $(X_t)_{t\geq 0}$ defined as follows:

- each state X_t is a vertex of G;
- the starting node X_0 is any vertex of G;
- for each pair of vertices $i, j \in V$,

$$\mathbb{P}_{i\to j} = \begin{cases} \frac{\#\{\text{ edges between } i \text{ and } j\ \}}{\#\{\text{edges starting from } i\}} & \text{if there is an edge between } i \text{ and } j, \\ \\ 0 & \text{otherwise,} \end{cases}$$

  where $\mathbb{P}_{i\to j}$ denotes the probability that, given $X_t = i$ for some $t \geq 0$, the next state X_{t+1} equals j.

The *length* of a random walk is the (possibly infinite) number of its states.

The above definition implies that a random walk is a Markov chain. Its transition matrix T is closely related to the adjacency matrix of the graph.

Proposition 2.8. *Let G be a graph, A its adjacency matrix and T the transition matrix of a random walk on G. Then, if G is a k-regular graph,*

$$T = \frac{1}{k}A.$$

Since the adjacency matrix encloses every information about the structure of G, it is natural to ask which assumptions on G ensure that a random walk on G approaches the uniform distribution, no matter how the starting vertex is chosen. To address this question, we name *probability function* on $G = (V, E)$ any non-negative map $p\colon V \to \mathbb{R}$ such that $\sum_{x\in V} p(x) = 1$.

Remark 2.9. Let n be the number of vertices of G, and suppose that we are able to sample vertices of G according to a certain probability distribution $p = (p_1, p_2, \ldots, p_n)$. Then, a random walk of length t on G allows us to sample vertices with probability distribution $T^t p$.

Theorem 2.10. *Suppose that $G = (V, E)$ is connected, non-bipartite and k-regular with n vertices. Let A be its adjacency operator and $T = (1/k)A$ the Markov transition operator. Then, for every probability function p on G we have*

$$\lim_{t\to\infty} T^t p = u$$

where u is the uniform distribution, *i.e.* $u(x) = 1/n$ *for each* $x \in V$.

Proof. See [Ter99, Thm. 6.1]. ☐

Moreover, the convergence of a random walk to the uniform distribution is particularly fast if the eigenvalues of the adjacency matrix are small (in absolute value).

Theorem 2.11. *Let G be a connected non-bipartite k-regular graph with n vertices. Denote by A its adjacency matrix, and by $T = (1/k)A$ its Markov transition matrix. Define*

$$\mu = \frac{\max(|\lambda_2|, |\lambda_n|)}{k},$$

where $\lambda_1 = k > \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of A. Then, for every probability function p on G and every positive integer t,

$$\|T^t p - u\|_1 \leq \sqrt{n}\mu^t,$$

where u is the uniform probability distribution and $\|\cdot\|_1$ is defined as $\|f\|_1 = \sum_{x\in V} |f(x)|$ for each $f\colon V \to \mathbb{R}$.

Proof. See [Ter99, Thm. 6.2]. □

2.5.2 Ramanujan property

Theorem 2.11 suggests that the 'speed of expansion' of random walks is related to the absolute value of the eigenvalues of the adjacency matrix.

A k-regular graph is *Ramanujan* if

$$\max(|\lambda_2|, |\lambda_n|) \leq 2\sqrt{k-1},$$

where λ_2 and λ_n are the second and the least eigenvalue of its adjacency matrix respectively.

Lemma 2.12 (Rapid mixing on Ramanujan graphs)**.** *Let G be a k-regular Ramanujan graph on n vertices, S be any subset of s vertices, and v be any vertex of G. Then, a random walk of length at least*

$$\frac{\log\left(\frac{n}{\sqrt{s}}\right)}{\log\left(\frac{k}{2\sqrt{k-1}}\right)}$$

starting from v ends in S with probability between $\frac{1}{2}\frac{s}{n}$ and $\frac{3}{2}\frac{s}{n}$.

Proof. See [JMV09, Lem. 2.1]. □

Corollary 2.13. *Let G be a k-regular Ramanujan graph on n vertices. The diameter of G, i.e. the maximal distance between any pair of its vertices, is $O(\log(n))$.*

Proof. Fix two vertices v and w. Then, setting $S = \{w\}$ in Lemma 2.12, we can conclude that a random walk of length $\log(n)/\log\big(k/(2\sqrt{k-1})\big)$ starting from v ends in w with non-zero probability. In particular, the distance between v and w is $O(\log(n))$. □

2.5.3 Supersingular isogeny graphs

Let ℓ and p be two distinct primes, $p \geq 5$ and $q = p^r$ for some $r \geq 1$. By Tate's theorem [Tat66, § 3], two elliptic curves over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogeneous if and only if they have the same trace over $\mathbb{F}_q$. We can thus define the *ℓ-isogeny graph* $\mathcal{G}_\ell(\mathbb{F}_q, a)$ as follows:

- its vertices are the elliptic curves with trace a over $\mathbb{F}_q$ modulo isomorphism over $\mathbb{F}_q$;
- its edges are the isogenies over $\mathbb{F}_q$ of degree ℓ between vertices.

An easy consequence of Tate's theorem is that two curves in the same isogeny graph are either both supersingular or both ordinary, depending on their trace over $\mathbb{F}_q$ being or not a multiple of p. From now on we will focus on supersingular isogeny graphs[1].

In order to represent the set of supersingular j-invariants in $\mathbb{F}_{p^2}$ (see Theorem 2.5) in terms of an ℓ-isogeny graph, we wonder if the trace a can be chosen in such a way that the vertices of $\mathcal{G}_\ell(\mathbb{F}_{p^2}, a)$ are in bijection with the supersingular j-invariants. We address this question by rephrasing a result in [AAM19].

Proposition 2.14. *Let $a \in \{2p, -2p\}$. Then, for each supersingular j-invariant $j_0 \in \mathbb{F}_{p^2}$ there is exactly one vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, a)$ composed by supersingular elliptic curves with j-invariant j_0.*

[1]More information about the ordinary case can be found in [Sut13; Koh96].

Proof. See [AAM19, pp. 5–6]. $\square$

Another ℓ-isogeny graph, denoted by $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$, can be defined as follows:

- its vertices are the supersingular j-invariants in $\mathbb{F}_{p^2}$;
- its edges are the isogenies of degree ℓ between vertices.

Working with $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ or with $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ is actually the same.

Theorem 2.15. *$\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ are isomorphic.*

Proof. See [AAM19, Thm. 6]. $\square$

$\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$, or equivalently $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$, enjoys the very properties which ensure 'good randomicity' of random walks. First of all, we consider the regularity of the graph.

Proposition 2.16. *Every vertex of $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ has outdegree $\ell + 1$.*

Proof. Let E be a vertex and α be a degree-ℓ isogeny starting from E. Then [Sil09, Thm. III.4.10] $\ker \alpha$ has order ℓ; in particular,

$$\ker \alpha \subseteq E[\ell].$$

By [Sil09, Cor. III.6.4], the ℓ-torsion of E is

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z},$$

and so it has exactly $\ell + 1$ subgroups of order ℓ. For each finite group G, the quotient curve $E' = E/G$ (i.e. the image of the isogeny with kernel G) is unique up to isomorphism [Sil09, Prop. 4.12]. $\square$

Actually, with the possible exception of the vertices 0 and 1728 and their neighbours (see [AAM19, Thm. 7], we can consider $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ as an undirected $(\ell + 1)$-regular graph. In [Piz98], a fairly stronger result is proven.

Theorem 2.17. *$\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ is Ramanujan.*

Therefore, $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ enjoys the rapid mixing property stated in Lemma 2.12. Moreover, since the number of supersingular j-invariants is at most $\lfloor p/12 \rfloor + 2$ (see Corollary 5.4), from Corollary 2.13 we conclude that the diameter of $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ is $O(\log p)$.

3 Motivation

The mathematical properties of supersingular elliptic curves go far beyond the results in the previous section. We believe that the appeal of this topic, from a theoretical perspective, needs no further evidence. However, there are also practical reasons for considering supersingular elliptic curves, since they are widely used in isogeny-based cryptography: we detail this fact in Section 3.1, and provide two examples in Section 3.2. Finally, in Section 3.3, we come to the formulation of the SRS and cSRS problems, to which the remainder of this article is devoted.

3.1 Hard problems for supersingular elliptic curves

Fix a fixed prime p of cryptographic size, the following problems are considered computationally hard [Gal+16, § 2.2].

Problem 1 (ℓ-ISOGENYPATH). *Given two supersingular elliptic curves E and E' over $\mathbb{F}_{p^2}$, find an ℓ-isogeny path between them, i.e. a path*

$$E \to E_1 \to \cdots \to E'$$

on $\mathcal{G}_\ell(\mathbb{F}_{p^2}, 2p)$.

Problem 2 (ENDRING). *Given a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, compute $\mathrm{End}(E)$ (i.e., find four endomorphisms that generate $\mathrm{End}(E)$ as a $\mathbb{Z}$-module).*

Not every instance of EndRing is computationally hard, though. There exist supersingular elliptic curves whose endomorphism ring can be easily computed: namely, those having non-trivial endomorphisms of small degree. We will detail this in Section 4.3.2.

Solving either ℓ-IsogenyPath or EndRing turns out to be the same.

Theorem 3.1. *ℓ-IsogenyPath and EndRing are computationally equivalent. More precisely:*

- *if $E, E', \mathrm{End}(E)$ and $\mathrm{End}(E')$ are given, an ℓ-isogeny path $E \to E'$ can be computed in polynomial time;*
- *if E, E', an ℓ-isogeny path $E \to E'$ and $\mathrm{End}(E)$ are given, $\mathrm{End}(E')$ can be computed in polynomial time.*

Proof. This was proven first under heuristic assumptions in [PL17, § 3.3], and later formally in [Wes21; Gha+21, § 7.1]. □

3.2 Two cryptographic applications

Hard mathematical problems can often be exploited to construct secure cryptographic protocols, and ℓ-IsogenyPath is no exception. Here we provide two examples, whose main purpose is to motivate our formulation of the cSRS problem in Section 3.3.

CGL hash function As a first example, we present a hash function based on the isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}_{p^2}})$ for some small prime $\ell \neq p$: the *CGL function* [CLG09]. The CGL function is outlined in Algorithm 1 for the case $\ell = 2$. Figure 1 depicts the paths in $\mathcal{G}_2(\overline{\mathbb{F}_{p^2}})$ that are followed throughout the computation of the CGL hash of the message 101.

Algorithm 1: CGL hash function

Input: A message m of n bits: $m = b_1 b_2 \cdots b_n$.
Output: $\mathsf{CGL}(m)$.
Choose a supersingular curve E_0 over $\mathbb{F}_{p^2}$;
Choose a 2-torsion point P of E_0;
Compute the isogeny $\varphi_0 \colon E_0 \to E_0/\langle P \rangle$ with kernel $\langle P \rangle$;
Set $E_1 = E_0/\langle P \rangle$;
for $i \in \{1, \ldots, n\}$ **do**
  Find the 2-torsion points of E_i, other than O;
  Rule out the 2-torsion point P such that map $E_i \to E_i/\langle P \rangle$ with kernel $\langle P \rangle$ is the dual of φ_{i-1};
  Label the other 2-torsion points by P_0, P_1 (according to some convention);
  Compute the isogeny $\varphi_i \colon E_i \to E_i/\langle P_{b_i} \rangle$ with kernel $\langle P_{b_i} \rangle$;
  Set $E_{i+1} = E_i/\langle P_{b_i} \rangle$;
end
Set $\mathsf{CGL}(m) = j\,(E_{n+1})$;

In this setting, a collision happens whenever the same curve E_{n+1} can be reached through two distinct ℓ-isogeny paths starting from E_1. Therefore, the hardness of ℓ-IsogenyPath ensures that the CGL function is, in general, collision resistant and preimage resistant: see [CLG09, § 5].

However, Theorem 3.1 suggests that the starting curve E_0 for the CGL hash function should be chosen carefully. Namely, if computing $\mathrm{End}(E_0)$ is by any chance easy, then finding a collision becomes easy as well.

SIDH key-exchange As a second example, we consider an algorithm designed by Petit [Pet17] to attack SIDH [DFJP14]. SIDH is a key-exchange protocol between two players, say Alice and Bob. Below we recall its construction.

Public parameters:

- A prime p of the form $p = \ell_A^{e_A} \ell_B^{e_B} \cdot f \pm 1$, where ℓ_A and ℓ_B are 'small' primes.
- A supersingular elliptic curve E_0 defined over $\mathbb{F}_{p^2}$.

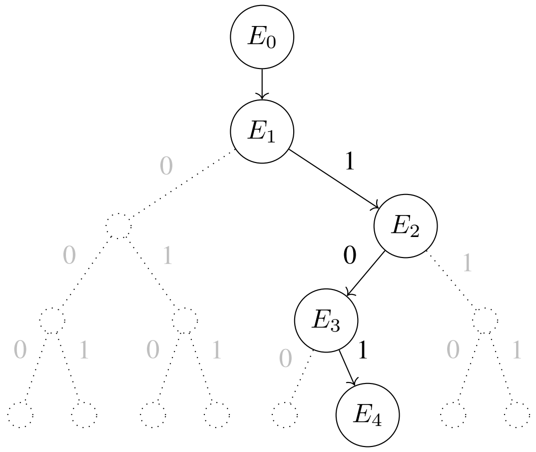

Figure 1: The path followed by the CGL function along the graph $\mathcal{G}_2(\overline{\mathbb{F}_{p^2}})$ for the message 101.

- Two bases $\{P_A, Q_A\}$ and $\{P_B, Q_B\}$ which generate $E_0[\ell_A^{e_A}]$ and $E_0[\ell_B^{e_B}]$ respectively.

Key exchange:

- Alice chooses two random integers $m_A, n_A \in [1 \dots \ell_A^{e_A}]$, not both divisible by ℓ_A. Then she computes an isogeny $\varphi_A \colon E_0 \to E_A$ with kernel $\langle [m_A]P_A + [n_A]Q_A \rangle$, and sends $(E_A, \varphi_A(P_B), \varphi_A(Q_B))$ to Bob.
- Bob acts similarly: he chooses two random integers $m_B, n_B \in [1 \dots \ell_B^{e_B}]$, not both divisible by ℓ_B. Then he computes an isogeny $\varphi_B \colon E_0 \to E_B$ with kernel $\langle [m_B]P_B + [n_B]Q_B \rangle$, and sends $(E_B, \varphi_B(P_A), \varphi_B(Q_A))$ to Alice.
- Alice computes an isogeny $\varphi'_A \colon E_B \to E_{BA}$ with kernel $\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle$.
- Bob computes an isogeny $\varphi'_B \colon E_A \to E_{AB}$ with kernel $\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle$.
- The shared secret is the j-invariant of E_{AB}, which is the same as the j-invariant of E_{BA}.

The security of SIDH relies on the following problem:

Problem 3 (CSSI (Computational supersingular isogeny))**.** *Given Alice's output* $(E_A, \varphi_A(P_B), \varphi_A(Q_B))$ *as above, find* φ_A *(equivalently: find its kernel* $\langle [m_A]P_A + [n_A]Q_A \rangle$*).*

Since the degree of φ_A is by construction $\ell_A^{e_A}$, CSSI can be seen as a variant of ℓ_A-ISOGENYPATH where some extra information is given about the isogeny to be found (namely, its action on $E_0[\ell_A^{e_A}]$).

In [Pet17, p. 4], however, it is shown that the knowledge of any non-trivial small-degree endomorphism of E_0 leads to dramatic speed-ups in the solution of CSSI: in this case, under further assumption on the starting parameters, CSSI can be even solved in polynomial time in the size of p.

Therefore, as in the previous case, the supersingular elliptic curve E_0 should be chosen carefully.

3.3 SRS and cSRS problems

In this section we formalise the problem of sampling uniformly random supersingular elliptic curves over $\mathbb{F}_{p^2}$, in two different versions:

- the first, weaker version is solely focused on the mathematical problem;
- the second, stronger version adds some further request in the light of cryptographic applications.

Let A be an algorithm. We say that A is a *superisingular random sampler* if, on input a prime p, A produces a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ and the sets

$$\{E \mid E \leftarrow \mathsf{A}(p)\} \qquad \text{and} \qquad \left\{E \;\middle|\; E \leftarrow_{\$} \{\text{Supersingular elliptic curves over } \mathbb{F}_{p^2}\}\right\}$$

have the same distribution.

Remark 3.2. Suppose that A' is a deterministic algorithm that, on input a prime p, produces a supersingular elliptic curve E over $\mathbb{F}_{p^2}$. Then, A' can be easily turned into a supersingular random sampler A thanks to the rapid mixing property (Lemma 2.12). Namely, on input p, A simply performs a random walk starting from $E \leftarrow \mathsf{A}'(p)$, and outputs the endpoint of the random walk.

Supersingular Random Sampling (SRS) problem
Construct a supersingular random sampler whose time complexity is $O(p)$.

In order to formulate a stronger version of the SRS problem, for any supersingular random sampler A we define a slight variation of Problem 2.

Problem 4 (ENDRING$_\mathsf{A}$). *Given $E \leftarrow \mathsf{A}(p)$ and the randomness used by A to sample E, compute* $\mathrm{End}(E)$.

Let A be a supersingular random sampler. We say that A is a *crypto-sampler* if ENDRING$_\mathsf{A}$ is computationally equivalent to ENDRING.

Crypto Supersingular Random Sampling (cSRS) problem
Construct a crypto-sampler whose time complexity is $O(p)$.

Remark 3.3. Let A be a supersingular random sampler consisting of a random walk $E \to E'$ that starts from the output of a deterministic algorithm A', as described in Remark 3.2. In this case, the randomness used by A is the random walk itself. It is then clear, in the light of Theorem 3.1, that computing $\mathrm{End}(E')$ using the randomness of A is equivalent to computing $\mathrm{End}(E)$. Therefore, A is a crypto-sampler if and only if ENDRING *on input E* is hard.

4 Known approaches

We now survey some known SRS methods, showing that none of them leads to an efficient cSRS algorithm.

First, we provide a detailed description of the most efficient SRS algorithm, to the best of our knowledge. It consists of the combination of two building blocks:

- an algorithm due to Bröker, described in Section 4.1;
- a random walk over $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, described in Section 4.3.

In Section 4.3.2 we will see why the resulting algorithm is not a cSRS algorithm.

Finally, in Section 4.4 we present some actual cSRS algorithms. They are mainly of theoretical interest, though, since their computational cost is at least sub-exponential in the size of p.

4.1 Bröker's algorithm

For any given prime $p \geq 5$, at least one supersingular j-invariant can be efficiently found thanks to Bröker's algorithm [Brö09], which heavily relies on the following result by Deuring.

Theorem 4.1 (Deuring). *Fix a prime $p \geq 5$. Let E be an elliptic curve over a number field K, with* $\mathrm{End}(E)$ *isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field k. Let $\mathfrak{P}$ be a prime of K over p, and suppose that E has a good reduction*[2] *modulo $\mathfrak{P}$, which we denote by $\tilde{E}$. Then $\tilde{E}$ is supersingular if and only if p has only one prime of k above it (that is, p does not split over k).*
Moreover, let $\mathscr{E}$ be an elliptic curve over a field of characteristic p with a non-trivial endomorphism α_0. Then there exists an elliptic curve E defined over a number field K, an endomorphism α of E and a good reduction $\tilde{E}$ of E at a prime $\mathfrak{P}$ of K over p, such that $\mathscr{E}$ is isomorphic to $\tilde{E}$ and α_0 corresponds to $\tilde{\alpha}$ (the reduction of α at $\mathfrak{P}$) under the isomorphism.

Proof. See [Deu41; Lan87, Thm. 13.12 and 13.14]. □

The first part of Deuring's theorem provides a criterion for determining whether the reduction modulo a prime ideal $\mathfrak{P}$ of a CM curve is supersingular or not, while the second part ensures that *every* supersingular elliptic curve can be expressed as the reduction modulo a prime ideal $\mathfrak{P}$ of a suitable CM curve.

[2] We say that *E has a good reduction* modulo $\mathfrak{P}$ if the $\mathfrak{P}$-adic valuation of $\Delta(E)$ equals 0. See [Sil09, § VII.5] for more details. In particular, this means that the coefficients of E can be seen as elements of some finite extension of $\mathbb{F}_p$, and they define an elliptic curve $\tilde{E}$ called the *reduction* of E modulo $\mathfrak{P}$.

4.1.1 Finding CM curves with supersingular reduction

By Deuring's Theorem, constructing a supersingular elliptic curve over $\overline{\mathbb{F}_p}$ is equivalent to constructing a CM curve E defined over some number field and such that p does not split in $\mathrm{End}(E)$. Equivalently, if we denote by k the imaginary quadratic field containing $\mathrm{End}(E)$, and by D the discriminant of k, we are imposing the condition

$$\left(\frac{D}{p}\right) \neq 1, \tag{4}$$

where the left-hand expression denotes the Legendre symbol [Cox13, Prop. 5.16, Cor. 5.17].

Once that a quadratic field k satisfying (4) is fixed, the goal is to determine the CM j-invariants whose endomorphism rings lie in k. To this end, a deeper insight of the link between elliptic curves and lattices over $\mathbb{C}$ is needed.

From complex lattices to complex elliptic curves Let x_1 and x_2 two $\mathbb{R}$-linearly independent vectors in the complex plane $\mathbb{C}$ (seen as a 2-dimensional $\mathbb{R}$-vector space). The *complex lattice generated by x_1 and x_2* is the set

$$\Lambda = \{z_1x_1 + z_2x_2 \mid z_1, z_2 \in \mathbb{Z}\}.$$

Two lattices Λ_1, Λ_2 are *homothetic* if there exists $\beta \in \mathbb{C} \setminus \{0\}$ such that $\Lambda_2 = \beta\Lambda_1$.

We will now recall how an elliptic curve E over $\mathbb{C}$ can be constructed from a complex lattice Λ, and also how $\mathrm{End}(E)$ can be retrieved from Λ. For this part we follow [Cox13, § 10; Sil09, § C.11; Was08, § 9.1-9.3, 10.1]; see also [Gal18, § 16.1] for a general overview on lattices in $\mathbb{R}^n$.

Let Λ be a complex lattice generated by $x_1, x_2 \in \mathbb{C}$; we call *complex torus* the quotient $\mathbb{C}/\Lambda$. For each integer $k \geq 3$, the *Eisenstein series*

$$G_k(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-k}$$

is defined. Each Eisenstein series converges: [Was08, Lem. 9.4]. In order to ease the notation, $60G_4(\Lambda)$ and $140G_6(\Lambda)$ are usually denoted by $g_2(\Lambda)$ and $g_3(\Lambda)$, respectively.

Finally, the *j-invariant* of a complex lattice is

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}. \tag{5}$$

Theorem 4.2. *Two complex lattices are homothetic if and only if they have the same j-invariant.*

Proof. See [Cox13, Thm. 10.9] □

As the use of the word 'j-invariant' suggests, complex lattices and elliptic curves over $\mathbb{C}$ are closely related.

Theorem 4.3. *Let Λ be a complex lattice, and define the elliptic curve*

$$E_\Lambda : \quad y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda).$$

Then the groups $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$ are isomorphic. Moreover, the map

$$\begin{aligned}\{\text{Homothety classes of complex lattices}\} &\to \{\text{Isomorphism classes of elliptic curves over } \mathbb{C}\} \\ \Lambda &\mapsto E_\Lambda\end{aligned}$$

is one-to-one, and $j(\Lambda) = j(E_\Lambda)$.

Proof. See [Was08, § 9.2 and 9.3]. □

The following proposition clarifies the connection between Λ and the endomorphism ring of E_Λ.

Proposition 4.4. *Let Λ be a complex lattice, and E_Λ the corresponding elliptic curve as in Theorem 4.3. Then*

$$\mathrm{End}(E_\Lambda) \cong \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}. \tag{6}$$

Proof. See [Was08, Theorem 10.1]. $\square$

Thus, if a complex lattice Λ such that $\mathbb{Z} \subsetneq \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}$ is considered, the corresponding elliptic curve E_Λ has complex multiplication. If fact, every such Λ is homothetic to a fractional ideal in some imaginary quadratic field, as we are going to prove in Corollary 4.9.

Proposition 4.5. *Let $\mathcal{O}$ be an order in an imaginary quadratic field k. Then every non-zero fractional ideal of $\mathcal{O}$ is a complex lattice.*

Proof. See [Cox13, § 10.C]. $\square$

Remark 4.6. On the contrary, a complex sublattice of an imaginary order $\mathcal{O}$ is not, in general, an ideal, nor even a subring, of $\mathcal{O}$. For example, consider $k = \mathbb{Q}(\sqrt{i})$ and the sublattice Λ generated by 2 and i in the ring of integers of k. The square of the second generator is -1, which does not lie in Λ. Therefore, Λ is not closed under multiplication.

Let S be the right-hand side of (6), i.e.

$$S = \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\},$$

and assume that Λ is a fractional ideal of an order $\mathcal{O}$ in a quadratic imaginary field. The inclusion $\mathcal{O} \subset S$ holds trivially. The other inclusion needs not to be true, though: see[Cox13, § 7.A]. When it does (that is: Λ is *not* an ideal in any order greater than $\mathcal{O}$), Λ is called a *proper* ideal.

Proposition 4.7. *Let $\mathcal{O}$ be an order in an imaginary quadratic field k, and Λ a proper non-zero ideal in $\mathcal{O}$. Then $\mathrm{End}(E_\Lambda) \cong \mathcal{O}$.*

Proof. It follows immediately from the definition of proper ideal and Proposition 4.4. $\square$

The above result provides a class of complex elliptic curves whose endomorphism ring is exactly $\mathcal{O}$: those of the form E_Λ, where Λ is a proper fractional ideal of $\mathcal{O}$. Actually, up to isomorphism, there are no other complex elliptic curves with endomorphism ring $\mathcal{O}$.

Theorem 4.8. *Let Λ be a complex lattice, and $\alpha \in \mathbb{C} \setminus \mathbb{Z}$. Then, the inclusion $\alpha\Lambda \subset \Lambda$ holds if and only if there exists an order $\mathcal{O}$ in an imaginary quadratic field k such that $\alpha \in \mathcal{O}$ and Λ is homothetic to a proper fractional $\mathcal{O}$-ideal.*

Proof. See [Cox13, Thm. 10.14]. $\square$

Corollary 4.9. *Let $\mathcal{O}$ be an imaginary quadratic order and E a complex elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}$. Then there exists a proper fractional $\mathcal{O}$-ideal Λ such that $E \cong E_\Lambda$.*

Proof. Theorem 4.3 ensures that $E \cong E_{\Lambda'}$ for some complex lattice Λ'. Since we are assuming that E is a CM curve, by (6) there exists $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ such that $\alpha\Lambda' \subseteq \Lambda'$. From Theorem 4.8 we know that there exists an imaginary quadratic order $\mathcal{O}'$ containing α and Λ' is homothetic to a proper fractional $\mathcal{O}'$-ideal Λ. By Proposition 4.7, $\mathrm{End}(E_\Lambda) = \mathcal{O}'$. Moreover, since Λ and Λ' are homothetic, the curves E_Λ and $E_{\Lambda'}$ are isomorphic. Hence, their endomorphism rings are isomorphic too, i.e. $\mathcal{O} = \mathcal{O}'$. $\square$

Corollary 4.10. *Let $\mathcal{O}$ be an order in an imaginary quadratic field. Then the map $f \colon \Lambda \mapsto j(E_\Lambda)$ yields a one-to-one correspondence between the ideal class group $\mathscr{C}(\mathcal{O})$ and the j-invariants of CM curves with endomorphism ring $\mathcal{O}$.*

Proof. It is easy to prove that two proper fractional ideals of $\mathcal{O}$ determine the same class if and only if they are homothetic as complex lattices. Therefore, f is well-defined on equivalence classes of ideals, and by Theorem 4.2 it is also injective. Proposition 4.7 ensures that $f(\Lambda)$ is actually a CM j-invariant. Finally, surjectivity follows from Corollary 4.9. $\square$

Hilbert class polynomials Corollary 4.10 alone does not provide an explicit strategy to compute CM j-invariants: even though a suitable complex lattice Λ can be easily determined, the infinite sums $g_2(\Lambda)$ and $g_3(\Lambda)$ involved in (5) make any direct computation quite impractical. Furthermore, *a priori* it is not ensured that the CM j-invariants considered in Corollary 4.10 are algebraic over $\mathbb{Q}$. In fact, this is a necessary condition to apply Deuring's theorem, since the CM curve (and therefore its j-invariant) is required to be defined over some number field. The latter problem is addressed in the following proposition.

Proposition 4.11. *Let $\mathcal{O}$ be an order in an imaginary quadratic field k, and denote by $\Lambda_1, \Lambda_2, \dots, \Lambda_h$ a complete set of representatives for $\mathscr{C}(\mathcal{O})$. Then the polynomial*

$$P_{\mathcal{O}} = \prod_{i=1}^{h} \big(X - j(E_{\Lambda_i})\big) \tag{7}$$

has integer coefficients. In particular, the CM j-invariants $j(E_{\Lambda_1}), \dots, j(E_{\Lambda_h})$ are algebraic over $\mathbb{Q}$.

Proof. See [Cox13, Thm. 13.2]. □

The polynomial $P_{\mathcal{O}}$ defined in (7) is called *Hilbert class polynomial* (or *ring class polynomial*, whenever $\mathcal{O}$ is not maximal) of the quadratic order $\mathcal{O}$.

There exist several algorithms to compute the Hilbert class polynomial of a given imaginary quadratic order $\mathcal{O}$ in time $\tilde{O}(\operatorname{disc}\mathcal{O})$. For the sake of completeness we sketch below the classical approach from [Coh93, p. 7.6.2]:

1) compute a set of representatives $\Lambda_1, \Lambda_2, \dots, \Lambda_h$ for $\mathscr{C}(\mathcal{O})$. Equivalently, following [Coh93, § 5.3.1], enumerate all the positive definite reduced integral binary quadratic forms $aX^2 + bXY + cY^2$ of discriminant $D = \operatorname{disc}(\mathcal{O})$, i.e. the triples of integers (a, b, c) such that
   - $|b| \le a \le c$,
   - if $|b| = a$ or $a = c$, then $b \ge 0$,
   - $b^2 - 4ac = D$.
2) Let (a, b, c) be one of the triples from the previous step. Then the corresponding representative is $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ with $\tau = \frac{-b+\sqrt{D}}{2a}$, and $j(\Lambda)$ can be approximated via the expansion

$$j(\tau) = 1728 \frac{\Big(1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k}\Big)^3}{\Big(1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k}\Big)^3 - \Big(1 - 504 \sum_{k=1}^{\infty} \frac{k^5 q^k}{1-q^k}\Big)^2}, \tag{8}$$

   where $q = e^{2\pi i \tau}$: see e.g. [Was08, Prop. 9.12].
3) If the approximations $\tilde{j}_1, \dots, \tilde{j}_h$ from the previous step are 'good enough', thanks to Proposition 4.11 the exact Hilbert class polynomial of $\mathcal{O}$ can be found by rounding the coefficients of $\prod_{i=1}^{h}(X - \tilde{j}_i)$ to the nearest integers. More precisely, the closeness of $\tilde{j}_i$ to $j(\Lambda_i)$ depends on both the partial sums from (8) considered for the approximation, and the precision used for numerical computations. While the impact of the first choice is limited by the rapid convergence of (8), the second one requires a deeper analysis of the coefficients of $P_{\mathcal{O}}$ [Eng06, § 4].

4.1.2 The algorithm

To summarise, in Section 4.1.1 we have depicted the following strategy to generate a supersingular j-invariant in $\mathbb{F}_{p^2}$ for a fixed prime $p \ge 5$:

1) Choose an imaginary quadratic field k whose discriminant D satisfies equation (4);
2) Choose an order $\mathcal{O}$ in k;
3) Compute the Hilbert class polynomial $P_{\mathcal{O}}$;
4) Consider the reduction modulo p of $P_{\mathcal{O}}$ and find one of its roots.

Bröker's algorithm, which is summarised in Algorithm 2, is just a special case of the above strategy. In particular, it performs steps (1) and (2) in such a way that the computation time is polynomial in the size of p, and the j-invariant found lies in $\mathbb{F}_p$. This is achieved by

- computing the smallest prime $q \equiv 3 \mod 4$ such that $\left(\frac{-q}{p}\right) \ne 1$;
- setting $k = \mathbb{Q}(\sqrt{-q})$;
- setting $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-q})/2]$, that is the maximal order of $\mathbb{Q}(\sqrt{-q})$.

Algorithm 2: Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.
Set $q = 3$;
while $\left(\frac{-q}{p}\right) = 1$ **do**
  Assign q to the next prime equivalent to 3 modulo 4;
end
Compute the Hilbert class polynomial $P_{\mathcal{O}}$ relative to the quadratic order $\mathcal{O}$ of discriminant $-q$;
Find a root $\alpha \in \mathbb{F}_p$ of $P_{\mathcal{O}}$ modulo p;
Set $j = \alpha$.

In particular, the fact that q is the smallest possible ensures that $\mathcal{O}$ is uniquely determined by p. Thus, the output of Bröker's algorithm depends only on p and the root of $P_{\mathcal{O}}$ chosen at step (4).

According to Bröker's analysis in [Brö09, Lem. 2.5], the expected running time of Algorithm 2 is $\tilde{O}\big((\log p)^3\big)$ due to the following reasons:

- heuristically, q is likely to be below 50 for $p \sim 2^{256}$. This fact seems reasonable, since half the elements of $\mathbb{Z}/p\mathbb{Z}$ are quadratic non-residues. In fact, in [LO77] it is proven that, under GRH, q has size $O\big((\log p)^2\big)$.
- $P_{\mathcal{O}}$ can be computed in $\tilde{O}(\operatorname{disc}(\mathcal{O})) = \tilde{O}(q) = \tilde{O}\big((\log p)^2\big)$ time, as we have already pointed out in Section 4.1.1.
- a root of $P_{\mathcal{O}}$ in $\mathbb{F}_p$ can be found, as described e.g. in [GG13, § 14.5], in probabilistic time

$$\tilde{O}\big(\deg(P_{\mathcal{O}})(\log p)^2\big),$$

  that is $\tilde{O}\big((\log p)^3\big)$ because $\deg(P_{\mathcal{O}}) = h(\mathcal{O}) = \tilde{O}(\sqrt{q})$. The latter equality is a classical result from [Sie35].

4.2 Extending Bröker's algorithm

We have already observed that Bröker's algorithm does not sample uniformly random supersingular elliptic curves. In fact, for any p, the output belongs to a uniquely determined subset of all possible supersingular j-invariants: namely, the roots of $P_{\mathcal{O}}$ in $\mathbb{F}_p$, which are $\tilde{O}(\sqrt{q})$. Following [LB20], we now go back to the general strategy summarised at the beginning of Section 4.1.2, and see how it can be translated into an actual SRS algorithm.

4.2.1 Listing imaginary quadratic orders

Imaginary quadratic orders can be listed according to their discriminants:

Theorem 4.12. *Write every integer as f^2D, where D is square-free. There is a bijection*

$$\{\text{ Imaginary quadratic orders }\} \leftrightarrow \mathbb{Z}^{<0}$$

$$\mathcal{O} \subseteq \mathbb{Q}(\sqrt{D}) \mapsto \begin{cases} \operatorname{disc}\mathcal{O} & \text{if } D \equiv 1 \mod 4, \\ \frac{\operatorname{disc}\mathcal{O}}{4} & \text{if } D \equiv 2,3 \mod 4 \end{cases}$$

$$\text{Order of conductor } f \text{ in } \mathbb{Q}(\sqrt{D}) \leftarrow f^2D.$$

In particular, if we denote by $\mathcal{D}$ the set

$$\mathcal{D} = \{\operatorname{disc}\mathcal{O} \mid \mathcal{O} \text{ imaginary quadratic order }\},$$

we have

$$\mathcal{D} = \big\{f^2d \mid f, d \in \mathbb{Z},\ d < 0,\ d \text{ square-free and either } d \equiv 1 \bmod 4 \text{ or } f \text{ is even}\big\}. \tag{9}$$

Proof. We recall from [Cox13, § 5.B] that every imaginary quadratic field can be written as $\mathbb{Q}(\sqrt{D})$ with D square-free, and its discriminant is

$$d_{\mathbb{Q}(\sqrt{D})} = \begin{cases} D & \text{if } D \equiv 1 \mod 4, \\ 4D & \text{if } D \equiv 2, 3 \mod 4. \end{cases}$$

Let $\mathcal{O}_D$ be the ring of integers of $\mathbb{Q}(\sqrt{D})$. Any positive integer f yields a unique order $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_D$ of conductor f, and every imaginary quadratic order can be constructed in this way (see Section 2.3).
Finally, the discriminant of an order of conductor f in $\mathbb{Q}(\sqrt{D})$ is $f^2 d_{\mathbb{Q}(\sqrt{D})}$ (see [Cox13, p. 134]). Therefore, the maps defined above are one inverse to the other. □

4.2.2 Increasing the number of outputs

The general strategy outlined in Section 4.1.2 consists in choosing a random imaginary quadratic order $\mathcal{O}$ whose discriminant is not a square modulo p, and finding a root of $P_{\mathcal{O}}$ modulo p. Algorithm 3 exactly follows this strategy, setting a lower bound $-4M$ for $\operatorname{disc} \mathcal{O}$ (we use the same notation for M as in [LB20]).

Algorithm 3: Extended Bröker's algorithm

Input: A prime $p \geq 5$ and a positive integer M.
Output: A supersingular j-invariant $j \in \mathbb{F}_{p^2}$.
Choose a random negative integer $n \in \mathcal{D} \cap [-4M, -3]$, with $\mathcal{D}$ as in (9);
Write $n = f^2 d$ with d square-free;
while $\left(\frac{d}{p}\right) = 1$ **do**
    Choose a new n;
end
Let $\mathcal{O}$ be the quadratic order of discriminant $f^2 d$;
Compute the Hilbert class polynomial $P_{\mathcal{O}}$;
Compute any root $\alpha \in \mathbb{F}_{p^2}$ of $P_{\mathcal{O}}$ modulo p;
Set $j = \alpha$.

We stress that M should be large enough so that at least one quadratic discriminant $n \in [-4M, -3]$ is not a quadratic residue modulo p (otherwise the algorithm would run endlessly). Under GRH, it is enough to set $M = \tilde{O}\big((\log p)^2\big)$.

The analysis of Algorithm 2 can be straightforwardly adapted to show that the expected running time of Algorithm 3 is $\tilde{O}\big(\sqrt{M} \cdot (\log p)^2\big)$:

- $|n|$ is at most $4M$.
- $P_{\mathcal{O}}$ can be computed in $\tilde{O}(\operatorname{disc}(\mathcal{O})) = \tilde{O}(M)$ time.
- a root of $P_{\mathcal{O}}$ in $\mathbb{F}_p$ can be found in probabilistic time

$$\tilde{O}\big(\deg(P_{\mathcal{O}})(\log p)^2\big) = \tilde{O}\big(\sqrt{M} \cdot (\log p)^2\big).$$

In the light of Theorem 4.1, Algorithm 3 can generate any supersingular j-invariant in $\mathbb{F}_{p^2}$, provided that M is large enough. Therefore, it is natural to ask which is the minimum value of M for which this holds. A first, rough estimate immediately suggests that M must be quite large[3].

Proposition 4.13. *Let N be the number of possible outputs of Algorithm 3. Then $N = \tilde{O}(M^{3/2})$.*

Proof. Let $\mathcal{O}$ be any quadratic order whose discriminant lies in the range $[-4M, -3]$. We have already observed that the class number $h(\mathcal{O})$, which is equal to the number of distinct roots of $P_{\mathcal{O}}$ modulo p, is $\tilde{O}(M^{1/2})$. Denote by $h(n)$ the class number of the quadratic order of discriminant n; then

$$N = \sum_{\substack{n \in \mathcal{D} \\ -4M \leq n}} h(n) \leq 4M \cdot \tilde{O}(M^{1/2}) = \tilde{O}(M^{3/2}), \tag{10}$$

where $\mathcal{D}$ is defined as in (9). □

[3] A more precise estimate can be found in [LB20, Prop. A.5].

For N to be (close to) $p/12$, the previous proposition rules that the value of M must be $\tilde{O}(p^{2/3})$. In that case, though, the running time of Algorithm 3 is sub-exponential: namely, $\tilde{O}(p^{1/3})$.

4.3 Bröker's algorithm and random walks

We will now consider the extended Bröker's algorithm Algorithm 3 under the assumption that M is polynomial in the size of p (so that the running time is polynomial, too).

The only known algorithm for sampling over the set of all supersingular j-invariants over $\mathbb{F}_{p^2}$ [Vit19, p. 71] is constructed according to the strategy described in Remark 3.2: it performs a random walk in $\mathcal{G}_2(\overline{\mathbb{F}_{p^2}})$ starting from the output of Algorithm 3. This algorithm, though, does not solve the cSRS problem, as we are going to show in Section 4.3.2.

4.3.1 Efficiency

In Section 3.2 we have shown that a random walk in $\mathcal{G}_2(\overline{\mathbb{F}_{p^2}})$ can be performed computing the CGL hash function on a random message. How long should such message be, in order to ensure that *every* supersingular curve can be reached? This question is addressed by Section 2.5.3. Namely, starting from a given supersingular j-invariant in $\mathbb{F}_{p^2}$ (possibly, the output of Algorithm 3), every other supersingular j-invariant in $\mathbb{F}_{p^2}$ can be reached within $O(\log(p))$ steps in $\mathcal{G}_2(\overline{\mathbb{F}_{p^2}})$.

4.3.2 Non-minimal output

Thus, the combination of (extended) Bröker's algorithm and random walks solves the SRS problem. Unfortunately, though, it does not solve the cSRS problem.

Proposition 4.14. *If E is an output of Algorithm 3, then* $\mathrm{End}(E)$ *can be computed efficiently.*

Proof. The statement is remarked in [LB20, p. 1], but here we provide a more explicit explanation. Following [LB20], we say that a curve is *M-small* if it has a non-trivial endomorphism of degree at most M. Let $\mathcal{O}$ be the quadratic order selected at the end of the while loop in Algorithm 3.

- A copy of $\mathcal{O}$ is embedded in $\mathrm{End}(E)$. To prove this, we recall from Section 4.1.1 that $j(E)$ is the reduction modulo p of some complex CM j-invariant, say $\tilde{j}$, whose endomorphism ring is isomorphic to $\mathcal{O}$. Let $\tilde{E}$ be a complex CM curve with j-invariant $\tilde{j}$, and suppose that its reduction is E. The reduction map $\mathrm{End}(\tilde{E}) \to \mathrm{End}(E)$ is a degree-preserving injection: see e.g. [Sil94, Prop. 4.4]. Therefore, $\mathcal{O}$ embeds in $\mathrm{End}(E)$.
- In particular, as our notation suggested, E is M-small, i.e. $\mathrm{End}(E)$ contains a non-trivial endomorphism of degree $|\mathrm{disc}\,\mathcal{O}| \le M$, which can be found applying Vélu's formulae to every subgroup of E having order $|\mathrm{disc}\,\mathcal{O}|$. This can be done efficiently, since we are assuming that M is polynomial in the size of p.
- In fact, the whole structure of $\mathrm{End}(E)$ can be computed as follows:
  1) Depending on p, consider a 'special' order as in [Eis+18, Prop. 1]. By [Eis+18, Prop. 3], one can compute a j-invariant j_0 whose endomorphism ring is isomorphic to such order. Let E_0 be a curve of j-invariant j_0. By construction, assuming GRH, E_0 is $O(\log^2 p)$-small.
  2) [LB20, Thm. 1.3] shows that isogenies of power-smooth degree between M-small curves can be computed in polynomial time in the size of p. Thus, since $\mathrm{End}(E_0)$ and a power-smooth isogeny $E_0 \to E$ are known, $\mathrm{End}(E)$ can be retrieved by Theorem 3.1.

□

Corollary 4.15. *Let* A *be the algorithm that performs a random walk $E \to E'$ starting from the output of Algorithm 3. Then* $\textsc{EndRing}_{\mathsf{A}}$ *can be solved in polynomial time in the size of p. In particular,* A *is not a crypto-sampler.*

Proof. The argument is the same as in Remark 3.3: once $\mathrm{End}(E)$ and an ℓ-isogeny $E \to E'$ are known, $\mathrm{End}(E')$ can be computed efficiently by Theorem 3.1. □

4.4 Exponential-time algorithms

Here we present two alternative approaches to solve the cSRS problem, based on classic results: exhaustive search via Schoof's algorithm and computation of Hasse invariants. Within the section we will also explain why the computational cost of these two methods is exponential in the size of p.

4.4.1 Exhaustive search

There exist efficient algorithms to check whether a given elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular or not: one of them computes the number of $\mathbb{F}_{p^2}$-rational points of E via Schoof's algorithm [Sch85, § 3] and checks if it equals 1 modulo p. Therefore, it is natural to ask if an efficient algorithm to solve the cSRS problem might be as simple as an exhaustive search, i.e. sampling random elements in $\mathbb{F}_{p^2}$ until a supersingular j-invariant is found.

Unfortunately, exhaustive search over $\mathbb{F}_{p^2}$ is unfeasible because supersingular j-invariants are 'rare': about 1 out of p elements of $\mathbb{F}_{p^2}$ is a supersingular j-invariant, as we are going to show in Corollary 5.4.

One might wonder if the probability of finding a supersingular j-invariant increases when the sample space is restricted to the smaller set $\mathbb{F}_p$. The following estimate suggests that this is true, even though the probability of success is still sub-exponential in the size of p:

Theorem 4.16. *There are $O(\sqrt{p}\log p)$ supersingular j-invariants over $\mathbb{F}_p$.*

Proof. See [DG16, pp. 2–3]. □

Therefore, a random element in $\mathbb{F}_p$ is a supersingular j-invariant with probability about $\log p/\sqrt{p}$. This rules out exhaustive search over both $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$ as an efficient method for solving the cSRS problem.

4.4.2 Hasse invariant

Consider a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve E over $\mathbb{F}_q$ given by an equation

$$E\colon y^2 = f(x),$$

where $f(x)$ is a separable polynomial of degree 3 or 4 as in Table 1. For any $k > 0$, define

$$A_{p^k} = \text{coefficient of } x^{p^k-1} \text{ in } f(x)^{(p^k-1)/2}.$$

In particular, we call A_p the *Hasse invariant*[4] of E.

A precise characterization of the Hasse invariant when $f(x)$ has degree 3 is given in [Sil09, Thm. 4.1.a]. In sight of Section 5, we provide here a slight generalization of the same result.

Theorem 4.17. *Consider a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve E over $\mathbb{F}_q$ given by an equation*

$$E\colon y^2 = f(x),$$

where $f(x)$ is a separable polynomial of degree 3 or 4 as in Table 1. Then E is supersingular if and only if its Hasse invariant equals 0.

Proof. Since the case $\deg(f) = 3$ is already covered in Silverman's proof, we assume that E is in Jacobi form.
First of all, we count the $\mathbb{F}_q$-rational points of E. [BJ03, § 3] shows that the points of E are in one-to-one correspondence with triplets $(X : Y : Z)_{[1,2,1]}$ which satisfy

$$Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4, \tag{11}$$

where $(X : Y : Z)_{[1,2,1]}$, or simply $(X : Y : Z)$, denotes *weighted projective coordinates* defined by the equivalence relation

$$(X : Y : Z) = (X' : Y' : Z') \qquad \Longleftrightarrow \qquad \exists\, k \in \overline{\mathbb{F}_p}^* \text{ such that } \begin{cases} X' = kX, \\ Y' = k^2 Y, \\ Z' = kZ. \end{cases} \tag{12}$$

[4]For each elliptic curve over $\mathbb{F}_q$ of equation

$$y^2 = 4x^3 - g_2 x - g_3,$$

Hasse [Has35] defines a polynomial $A_q \in \mathbb{F}_q[g_2, g_3]$, such that $A_q = 0$ if and only if the corresponding curve is supersingular. Here we generalise Hasse's definition to other models of elliptic curves.

Thus, the affine points of E are the image of the bijection

$$\begin{aligned}\{(X:Y:Z)_{[1,2,1]} \mid Z\neq 0\} &\to \mathbb{A}^2(\overline{\mathbb{F}_p})\\ (X:Y:1) &\mapsto (x,y),\end{aligned}$$

that is, they are indeed the solutions of the affine equation $y^2 = \epsilon x^4 - 2\delta x^2 + 1$. In particular, if we let $\chi\colon \mathbb{F}_q^* \to \{-1,0,1\}$ be the map such that

$$\chi(z) = \begin{cases} -1 & \text{if } z \text{ is not a square,}\\ 0 & \text{if } z = 0,\\ 1 & \text{if } z \text{ is a non-zero square,}\end{cases}$$

we have

$$\#\left(E(\mathbb{F}_q)\cap \mathbb{A}^2(\mathbb{F}_q)\right) = \sum_{x\in\mathbb{F}_q}\left(1+\chi\big(f(x)\big)\right) = q + \sum_{x\in\mathbb{F}_q}\chi\big(f(x)\big).$$

The 'points at infinity' of E, on the other hand, are triplets $(X:Y:0)$ satisfying (11). Notice that X and Y must be non-zero since $\epsilon\neq 0$, so that the equation $Y^2=\epsilon X^4$ yields two $\mathbb{F}_q$-rational points if ϵ is a square, zero points otherwise. In conclusion,

$$\#\big(E(\mathbb{F}_q)\big) = 1+\chi(\epsilon)+q+\sum_{x\in\mathbb{F}_q}\chi\big(f(x)\big). \tag{13}$$

Since $\mathbb{F}_q^*$ is cyclic of order $q-1$, the equality

$$\chi(z) = z^{\frac{q-1}{2}}$$

holds for every $z\in\mathbb{F}_q$. In particular, (13) becomes

$$\#E(\mathbb{F}_q) = 1+\epsilon^{\frac{q-1}{2}}+q+\sum_{x\in\mathbb{F}_q}\big(f(x)\big)^{\frac{q-1}{2}}.$$

We stress that the latter equation holds on $\mathbb{Z}$, as long as we choose 1 and -1 to represent the equivalence classes of $\epsilon^{\frac{q-1}{2}}$ and $(f(x))^{\frac{q-1}{2}}$ modulo p.
Furthermore, one can prove the following equality [Was08, Lem. 4.35]:

$$\sum_{x\in\mathbb{F}_q} x^i = \begin{cases} -1 & \text{if } q-1\mid i,\\ 0 & \text{if } q-1\nmid i.\end{cases}$$

As a consequence, since $f(x)$ has degree 4, the only nonzero terms in $\sum_{x\in\mathbb{F}_q} f(x)^{(q-1)/2}$ are (up to a sign) the coefficients of x^{q-1} and $x^{2(q-1)}$ in $f(x)^{(q-1)/2}$. Namely, the coefficient of x^{q-1} is A_q by definition, while the coefficient of $x^{2(q-1)}$ actually is the leading coefficient of $f(x)^{(q-1)/2}$, which is $\epsilon^{\frac{q-1}{2}}$. Then we have

$$\#E(\mathbb{F}_q) \equiv 1+\epsilon^{\frac{q-1}{2}}-\epsilon^{\frac{q-1}{2}}-A_q \equiv 1-A_q \mod p.$$

Moreover, from [Sil09, Theorem 2.3.1] we know

$$\#E(\mathbb{F}_q) = q+1-a,$$

where a is the trace of the q-power Frobenius endomorphism. By Theorem 2.7 we can therefore conclude

$$E \text{ is supersingular} \iff a\equiv 0 \mod p \iff A_q = 0.$$

The implication $A_q = 0 \iff A_p = 0$ follows by induction from the relation

$$A_{p^{r+1}} = A_{p^r}A_p^{p^r},$$

which can be proven exactly as in the cubic case (see [Was08, Lemma 4.36]). □

It is common to consider the Hasse invariant for elliptic curves in Legendre form.

Proposition 4.18. *Let $y^2 = x(x-1)(x-\lambda)$ be the equation defining an elliptic curve in Legendre form. Then*

$$A_p = (-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i,$$

where $m = (p-1)/2$.

Proof. See [Deu41, p. 201; Was08, Thm. 4.34; Sil09, Thm. 4.1.b]. □

We focus on the construction of A_p as a polynomial in the variable λ. If we write down explicitly its coefficients (considered modulo p)[5]

$$c_i = \frac{(m!)^2}{(i!)^2\big((m-i)!\big)^2} \qquad \text{for } i = 0, \ldots, m,$$

it is easy to see that they can be computed recursively, starting from $c_0 = 1$, via the following formula:

$$c_{i+1} = c_i \cdot \frac{(m-i)^2}{(i+1)^2}.$$

This avoids the computation of any factorial modulo p, but does not suggest any easy way to find the roots of A_p. In terms of computational complexity, computing the zeroes of A_p appears actually worse than an exhaustive search of supersingular j-invariants over $\mathbb{F}_{p^2}$ as described in Section 4.4.1. We will say more on this subject in Section 5.

5 Hasse invariant of other models of elliptic curves

Section 2.4 gathers various characterizations of supersingular elliptic curves over finite fields. Throughout the next sections we do a step further, and see if these characterizations may lead to efficient solving algorithms for the SRS/cSRS problem.

In this section, the Hasse invariant A_p (defined in Section 4.4.2) is computed for elliptic curves in Weierstrass form and for the other elliptic-curve models in Table 1 (excluding Legendre, which has already been considered in Section 4.4.2): namely, for each model we construct A_p as a polynomial whose coefficients lie in $\mathbb{F}_q$, and whose roots are coefficients of supersingular elliptic curves over (some extension of) $\mathbb{F}_q$.

We make use of the same notation as in Section 4.4.2, i.e.:

$$m = \frac{p-1}{2}$$

where p is a prime ≥ 5.

5.1 Weierstrass

Consider the family of elliptic curves over $\mathbb{F}_q$ in Weierstrass form, i.e. the curves of equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_q$. Thus, the Hasse invariant A_p can be regarded as a polynomial in $\mathbb{F}_q[A, B]$.

Proposition 5.1. *The Hasse invariant of an elliptic curve $E\colon y^2 = x^3 + Ax + B$ in Weierstrass form is*

$$A_p = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} A^{2m-3i} B^{2i-m}. \tag{14}$$

Proof. Write

$$(x^3 + Ax + B)^m = \sum_{i=0}^{m} \binom{m}{i} x^{3i} (Ax+B)^{m-i}$$

[5] The factor $(-1)^m$ can be neglected, since we are interested in the zeroes of A_p.

$$= \sum_{i=0}^{m} \binom{m}{i} x^{3i} \left(\sum_{j=0}^{m-i} \binom{m-i}{j} (Ax)^j B^{m-i-j} \right).$$

In each term, the degree of x equals $p-1$ if and only if $j = p-1-3i$. Therefore

$$A_p = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} A^{2m-3i} B^{2i-m}.$$

□

Now, we wonder which values of $A, B \in \mathbb{F}_q$ annihilate A_p. The cases $A = 0$ or $B = 0$ can be ruled out since they yield elliptic curves with j-invariant 0 or 1728, which we have already considered in Section 4.4.2. A and B may therefore be regarded as elements in the multiplicative group $\mathbb{F}_{p^2}^*$. Namely, we can express A and B as powers of some primitive element $g \in \mathbb{F}_{p^2}^*$, say

$$A = g^k, \qquad B = g^\ell \qquad \text{with } k, \ell \in \{0, \dots, p^2-2\}.$$

Thus we can rewrite A_p as follows:

$$\begin{aligned} A_p &= \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} A^{2m-3i} B^{2i-m} \\ &= \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} g^{k(2m-3i)} g^{\ell(2i-m)} \\ &= \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} g^{m(2k-\ell)+i(2\ell-3k)} \end{aligned}$$

In order to find the coefficients A, B defining supersingular curves, it is necessary to look for values of k, ℓ such that the latter expression annihilates. Moreover, by multiplying the expression by the inverse of $g^{m(2k-\ell)}$, it is enough to consider

$$\sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} g^{i(2\ell-3k)}. \tag{15}$$

Notice that (15) can be seen as a polynomial over $\mathbb{F}_p$ in the variable $g^{2\ell-3k}$.

Lemma 5.2. *Let n be a positive integer and fix $C \in \mathbb{Z}/(p^n-1)\mathbb{Z}$. Then*

$$2L - 3K \equiv C \mod p^n - 1 \tag{16}$$

has $p^n - 1$ solutions in K and L.

Proof. Observe that

- if $k \equiv C \mod 2$, the following pairs

$$\left(k, \frac{3k+C}{2}\right) \qquad \text{and} \qquad \left(k, \frac{3k+C}{2} + \frac{p^n-1}{2}\right)$$

  are distinct solutions of (16);

- if $k \not\equiv C \mod 2$, no element $\ell \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ satisfies equation (16).

Therefore, equation (16) has

$$2 \cdot \frac{p^n-1}{2} = p^n - 1$$

solutions. □

The zeroes of (15), seen as a polynomial over $\mathbb{F}_p$ in the variable $g^{2\ell-3k}$, correspond to the superinsingular j-invariants as detailed in the following results.

Theorem 5.3. *Let g be a primitive element of $\mathbb{F}_{p^2}$, and fix $C = 2\ell' - 3k'$ such that* (15) *annihilates. In other words, g^C is a root of*

$$G(X) = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i}\binom{m-i}{2m-3i} X^i \in \mathbb{F}_p[X]. \tag{17}$$

Denote by

$$E'\colon y^2 = x^3 + A'x + B'$$

the corresponding supersingular elliptic curve having

$$A' = g^{k'}, \qquad B' = g^{\ell'}.$$

Then the curves defined over $\mathbb{F}_{p^2}$ and isomorphic to E' are exactly the curves whose coefficients written in the form

$$A = g^k, \qquad B = g^\ell$$

satisfy

$$C \equiv 2\ell - 3k \mod p^2 - 1.$$

Proof. Let E be a curve defined over $\mathbb{F}_{p^2}$ and isomorphic to E' over $\overline{\mathbb{F}_p}$. Therefore [Sil09, p. 45] the coefficients of E must satisfy

$$A = u^4 A', \qquad B = u^6 B' \tag{18}$$

for some $u \in \mathbb{F}_{p^4}^*$ such that $u^2 \in \mathbb{F}_{p^2}^*$. Notice that there are exactly $p^2 - 1$ values of u with such property[6]; that is, there are exactly $p^2 - 1$ curves defined over $\mathbb{F}_{p^2}$ and isomorphic to E. In terms of a given generator g of $\mathbb{F}_{p^2}^*$, we have

$$g^k = u^4 g^{k'} = g^{2r+k'} \qquad \text{and} \qquad g^\ell = u^6 g^{\ell'} = g^{3r+\ell'}$$

for some $r \in \{0, \dots, p^2 - 2\}$. Then

$$2\ell - 3k \equiv 2(3r + \ell') - 3(2r + k') \equiv 2\ell' - 3k' \equiv C \mod (p^2 - 1).$$

Thus, letting u vary, we have $p^2 - 1$ distinct solutions for the equation in L and C

$$2L - 3K \equiv C \mod (p^2 - 1). \tag{19}$$

Lemma 5.2 ensures that there is no other solution. ☐

Corollary 5.4. *Let $G(X)$ be the polynomial defined in* (17). *The non-zero roots of $G(X)$ are in bijection with the supersingular j-invariants $\notin \{0, 1728\}$.*

Proof. Let g be a primitive element of $\mathbb{F}_{p^2}$. We have already shown that every non-zero root g^C of $G(X)$ corresponds to some isomorphism class of supersingular curves. Namely, if

$$E\colon y^2 = x^3 + g^k x + g^\ell$$

is a representative of this class (in particular, $2k - 3\ell \equiv C \mod (p^2 - 1)$), its j-invariant is

$$\begin{aligned} j(E) &= 1728 \cdot \frac{4g^{3k}}{4g^{3k} + 27g^{2\ell}} \\ &= 1728 \cdot \frac{4g^{3k}}{4g^{3k} + 27g^{2\ell}} \cdot \frac{g^{-3k}}{g^{-3k}} \\ &= \frac{1728 \cdot 4}{4 + 27g^{2\ell-3k}}. \end{aligned}$$

[6] Namely, the elements

$$1, \gamma^{\frac{p^2+1}{2}}, \gamma^{2\frac{p^2+1}{2}}, \dots \gamma^{(p^2-2)\frac{p^2+1}{2}}$$

for some generator γ of $\mathbb{F}_{p^4}^*$.

Therefore the correspondence

$$\begin{array}{rcl} \{\text{non-zero roots of } G(X)\} & \leftrightarrow & \{\text{supersingular } j\text{-invariants} \notin \{0,1728\}\} \\ g^C & \mapsto & \dfrac{1728 \cdot 4}{4 + 27 g^C} \\ \dfrac{64 \cdot 4}{j} - \dfrac{4}{27} & \leftarrow\!\shortmid & j \end{array} \tag{20}$$

is one-to-one.

□

Let

$$\tilde{G}_p(X) = \sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \underbrace{\binom{m}{i}\binom{m-i}{2m-3i}}_{c_i} X^{i-\lceil \frac{p-1}{4} \rceil}$$

be the polynomial considered in the proof of Corollary 5.4, with $m = (p-1)/2$. So far, we have shown that the roots of $\tilde{G}_p(X)$ correspond to the supersingular j-invariants in $\mathbb{F}_{p^2} \setminus \{0, 1728\}$. Moreover, by (20), $\tilde{G}_p$ splits completely over $\mathbb{F}_{p^2}$ (since every supersingular j-invariant lies in $\mathbb{F}_{p^2}$: see Theorem 2.5.b).

The coefficients of $\tilde{G}_p$, for $i \in \left\{\lceil \frac{p-1}{4} \rceil, \ldots, \lfloor \frac{p-1}{3} \rfloor\right\}$, are

$$\begin{aligned} c_i &= \binom{m}{i}\binom{m-i}{2m-3i} \\ &= \frac{m!}{i!(m-i)!} \cdot \frac{(m-i)!}{(2m-3i)!(2i-m)!} \\ &= \frac{m!}{i!(2m-3i)!(2i-m)!}. \end{aligned}$$

We can assume that $\tilde{G}_p(X)$ is normalized with respect to its constant term; therefore, starting from $c_{\lceil \frac{p-1}{4} \rceil} = 1$, every other coefficient can be computed recursively via the following formula:

$$c_{i+1} = -12 \cdot \frac{(3i+1)(3i+2)}{(4i+3)(4i+5)} \cdot c_i. \tag{21}$$

As p does not appear within the factors of any coefficient, we conclude that every coefficient of $\tilde{G}_p(X)$ is different from 0.

5.2 Montgomery

Consider the family of elliptic curves over $\mathbb{F}_q$ in Montgomery form, i.e. the curves of equation $y^2 = (x^3 + Ax^2 + x)/B$ with $A, B \in \mathbb{F}_q$, $B \neq 0$ and $A^2 \neq 4$. Thus, the Hasse invariant A_p can be regarded as a polynomial in $\mathbb{F}_q[A, B]$.

Moreover, we note that the zeroes of A_p do not depend on B. This is actually coherent with the fact that j-invariants of Montgomery curves depend only on A (see Table 1). We can therefore assume $B = 1$ and compute A_p as a polynomial in the only variable A.

Proposition 5.5. *The Hasse invariant of an elliptic curve $E\colon y^2 = (x^3 + Ax^2 + x)/B$ in Montgomery form is*

$$A_p = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{i}\binom{m-i}{m-2i} A^{m-2i},$$

and its coefficients can be computed recursively starting from $c_0 = 1$ via the formula

$$c_{i+1} = c_i \cdot \frac{(m-2i)(m-2i-1)}{(i+1)^2}.$$

Proof. We start by observing that

$$(x^3 + Ax^2 + x)^m = x^m (x^2 + Ax + 1)^m$$

$$
\begin{aligned}
&= x^m \cdot \sum_{i=0}^{m} \binom{m}{i} x^{2i} (Ax+1)^{m-i} \\
&= x^m \cdot \sum_{i=0}^{m} \binom{m}{i} x^{2i} \left(\sum_{j=0}^{m-i} \binom{m-i}{j} A^j x^j \right).
\end{aligned}
$$

In each term, the degree of x equals $p-1$ if and only if $m + 2i + j = 2m$, or, equivalently, $j = m - 2i$. Therefore,

$$
A_p = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \underbrace{\binom{m}{i}\binom{m-i}{m-2i}}_{c_i} A^{m-2i}.
$$

Notice that $c_0 = 1$, defined above, is now the coefficient of the leading term; the other coefficients can be computed recursively via the formula

$$
c_{i+1} = c_i \cdot \frac{(m-2i)(m-2i-1)}{(i+1)^2}.
$$

□

Remark 5.6. The degrees of the terms in A_p have all the same parity. In particular, if A annihilates A_p, also $-A$ does. This is, again, coherent with the fact that isomorphism classes depend only on A^2.

5.2.1 Splitting field of the Hasse invariant

Since every supersingular j-invariant lies in $\mathbb{F}_{p^2}$ by Theorem 2.5.b, the equation for the j-invariant of Montgomery curves (see Table 1) suggests that the roots of A_p lie in $\mathbb{F}_{p^{12}}$. A stronger result actually holds, as we are going to show in Proposition 5.10, whose proof requires a few lemmata. The first one is just a special case of [Was08, Ex. 4.10]:

Lemma 5.7. *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve in Weierstrass form over $\mathbb{F}_{p^2}$ with trace t. Then one of its twists has trace $-t$.*

Proof. Let γ be a generator for $\mathbb{F}_{p^4}^*$. Define

$$
u = \gamma^{\frac{p^2+1}{2}}
$$

and consider the curve

$$
E'\colon \quad y^2 = x^3 + u^4 Ax + u^6 B.
$$

From [Sil09, p. 45] we know that

$$
\begin{aligned}
\varphi\colon \quad & E \to E' \\
& (x, y) \mapsto (u^2 x, u^3 y).
\end{aligned}
$$

is an isomorphism defined over $\mathbb{F}_{p^4}$ but *not* over $\mathbb{F}_{p^2}$; in other words, E' is a quadratic twist of E.
Let t' be the trace of E'. By [Sil09, Rem. V.2.6] and [Hus87, Prop. 4.1.10] we have

$$
\#E(\mathbb{F}_{p^2}) = 1 + p^2 - t, \qquad \#E'(\mathbb{F}_{p^2}) = 1 + p^2 - t', \qquad \#E(\mathbb{F}_{p^2}) + \#E'(\mathbb{F}_{p^2}) = 2p^2 + 2.
$$

The thesis follows immediately. □

Lemma 5.8. *Let $E\colon y^2 = x^3 + A'x + B'$ be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ in Weierstrass form with j-invariant different from 0 or 1728. Then every 4-torsion point of either E or its quadratic twist E' is $\mathbb{F}_{p^2}$-rational.*

Proof. It is well-known [Sil09, Ex. 3.32, Ex. 5.10] that the number of $\mathbb{F}_{p^2}$-rational points of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ is $p^2 - t + 1$, where

$$
t \in \{0, \pm p, \pm 2p\}.
$$

Furthermore, $t \in \{0, \pm p\}$ if and only if $j(E) \in \{0, 1728\}$ [AAM19, pp. 5–6]. We can therefore assume that E has trace $2p$, while its quadratic twist E' has trace $-2p$ by Lemma 5.7.

From [Sch87, Lemma 4.8.ii] we know the structure of $\mathbb{F}_{p^2}$-rational groups of the two curves:

$$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \qquad \text{and} \qquad E'(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}.$$

In particular,

- if $p \equiv 1 \mod 4$, then $\mathbb{Z}/(p-1)\mathbb{Z}$ has a subgroup of order 4 and such subgroup must be $\mathbb{Z}/4\mathbb{Z}$. Otherwise, E would have more than 4 points of 2-torsion, contradicting [Sil09, Cor. III.6.4]. Then $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is a subgroup of $E(\mathbb{F}_{p^2})$ (up to isomorphism). Equivalently, again from [Sil09, Cor. III.6.4], $E[4] \subseteq E(\mathbb{F}_{p^2})$.
- Similarly, if $p \equiv 3 \mod 4$, one can prove $E'[4] \subseteq E'(\mathbb{F}_{p^2})$.

□

Lemma 5.9. *Let $E'\colon y^2 = x^3 + A'x + B'$ be an elliptic curve over $\mathbb{F}_q$. Then E' is birationally equivalent to a Montgomery curve E* over $\mathbb{F}_q$ *if and only if*

(a) E' has an $\mathbb{F}_q$-rational 2-torsion point $(\alpha, 0)$.

(b) $3\alpha^2 + A' = s^2$ for some $s \in \mathbb{F}_q^*$.

The coefficients of E are

$$\begin{cases} A = 3\alpha s^{-1}, \\ B = s^{-1}. \end{cases}$$

Proof. See [OKS00, Prop. 4.1, 7.5]. □

Proposition 5.10. *A_p for Montgomery curves splits completely over $\mathbb{F}_{p^2}$. Equivalently, the coefficient A of every supersingular Montgomery curve lies in $\mathbb{F}_{p^2}$.*

Proof. First of all, notice that the j-invariant

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

of a Montgomery curve $E\colon By^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{p^2}$ equals 0 if and only if A is a square root of 3. Similarly, one can check that $j(E) = 1728$ if and only if either $A = 0$ or A is a square root of $2^{-1} \cdot 9$. In both cases, A lies in $\mathbb{F}_{p^2}$.

Let E be a representative of a supersingular j-invariant $j' \notin \{0, 1728\}$. By Proposition 2.1, E can be written in Weierstrass form over $\mathbb{F}_{p^2}$:

$$E\colon \quad y^2 = x^3 + A'x + B'.$$

By Lemma 5.8 we can also assume that the 4-torsion points of E are $\mathbb{F}_{p^2}$-rational. It particular, it has 2-torsion points $(\alpha_i, 0)$ for $i \in \{1, 2, 3\}$, with $\alpha_i \in \mathbb{F}_{p^2}^*$ (they are non-zero, otherwise $B' = 0$ and $j = 1728$ which contradicts our assumption). Notice that B' can be written as

$$B' = -\alpha_i^3 - A'\alpha_i \tag{22}$$

for every $i \in \{1, 2, 3\}$, and exploit such relation in order to factor the fourth division polynomial ψ_4 (see Section 6.1):

$$\begin{aligned}
\psi_4/2y &= 2x^6 + 10A'x^4 + 40B'x^3 - 10(A')^2x^2 - 8A'B'x - 2(A')^3 - 16(B')^2 \\
&= 2x^6 - 40x^3\alpha_i^3 - 16\alpha_i^6 + 10A'x^4 - 40A'x^3\alpha_i + \\
&\quad + 8A'x\alpha_i^3 - 32A'\alpha_i^4 - 10(A')^2x^2 + 8(A')^2x\alpha_i - 16(A')^2\alpha_i^2 - 2(A')^3 \\
&= -2(-x^2 + 2x\alpha_i + 2\alpha_i^2 + A')(x^4 + 2x^3\alpha_i + 6x^2\alpha_i^2 - 4x\alpha_i^3 + \\
&\quad + 4\alpha_i^4 + 6A'x^2 - 6A'x\alpha_i + 6A'\alpha_i^2 + (A')^2).
\end{aligned} \tag{23}$$

Since ψ_4 annihilates exactly on the 4-torsion points (see Proposition 6.5), for each i there exist two distinct values x_i and x'_i in $\mathbb{F}_{p^2}$ that annihilate the first factor of (23), i.e.

$$-x^2 + 2x\alpha_i + 2\alpha_i^2 + A',$$

or, equivalently, satisfy

$$A' + 3\alpha_i^2 = (x - \alpha_i)^2. \tag{24}$$

Notice that $x_i - \alpha_i$ is non-zero because $x_i \neq x'_i$. The conditions (a) and (b) from Proposition 5.9 are therefore verified, and E is birationally equivalent to Montgomery curves defined over $\mathbb{F}_{p^2}$ with coefficients

$$\begin{cases} A_i = 3\alpha_i(x_i - \alpha_i)^{-1} \\ B_i = (x_i - \alpha_i)^{-1} \end{cases}$$

for every $i \in \{1, 2, 3\}$.
We claim that $A_i^2 \neq A_j^2$ for $i \neq j$. Suppose, by contradiction, $A_i^2 = A_j^2$ for some $i \neq j$. By (24) we can write

$$\begin{aligned} 9\alpha_i^2(3\alpha_i^2 + A')^{-1} &= 9\alpha_j^2(3\alpha_j^2 + A')^{-1} \\ \alpha_i^2(3\alpha_j^2 + A') &= \alpha_j^2(3\alpha_i^2 + A') \\ \alpha_i^2 &= \alpha_j^2, \end{aligned}$$

but this cannot occur. In fact, $\alpha_i \neq \alpha_j$ by construction, and the assumption $B' \neq 0$ together with (22) implies $\alpha_i \neq -\alpha_j$.
To summarise, starting from a suitable supersingular elliptic curve in Weierstrass form with j-invariant $j' \notin \{0, 1728\}$, we have found three distinct solutions A_1^2, A_2^2, A_3^2 for the equation

$$j' = \frac{256(X-3)^3}{X-4}.$$

Since there is no other solution, the coefficient of x^2 of a Montgomery curve with j-invariant j' must be one of $\{\pm A_i \mid i = 1, 2, 3\}$, and all these values lie in $\mathbb{F}_{p^2}$.

□

5.3 Jacobi

Consider the family of elliptic curves over $\mathbb{F}_q$ in Jacobi form, i.e. the curves of equation $y^2 = \epsilon x^4 - 2\delta x^2 + 1$ with $\epsilon, \delta \in \mathbb{F}_q$, $\epsilon \neq 0$ and $\delta^2 \neq \epsilon$. Thus, the Hasse invariant A_p can be regarded as a polynomial in $\mathbb{F}_q[\epsilon, \delta]$.

Proposition 5.11. *The Hasse invariant of an elliptic curve $E\colon y^2 = \epsilon x^4 - 2\delta x^2 + 1$ in Jacobi form is*

$$A_p = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \underbrace{\binom{m}{i}\binom{m-i}{m-2i}}_{c_i} \epsilon^i (-2\delta)^{m-2i}$$

and its coefficients c_i can be computed recursively starting from $c_0 = 1$ via the formula

$$c_{i+1} = c_i \cdot \frac{(m-2i)(m-2i-1)}{(i+1)^2}.$$

Proof. Similar to the proof of Proposition 5.5. In particular, notice that the coefficients are the same. □

5.4 Efficiency analysis

We have found explicit formulas to construct the Hasse invariant A_p for several elliptic-curve models, but none of them allows for an *efficient* construction of A_p. From a computational point of view, even the storage of A_p becomes problematic when p is of cryptographic size.

However, the combination of Bröker's algorithm and random walks, as described in Section 4.3, provides an efficient method to find arbitrarily many roots of A_p. We cannot rule out that this fact, combined with the recursion formula for the coefficients of A_p, might lead to an efficient algorithm to solve the cSRS problem. We leave the investigation for future work.

6 Torsion points

In this section we provide two distinct characterizations of supersingular elliptic curves over finite fields in terms of suitably chosen torsion points.

6.1 Division polynomials

Following [Sil09, ex. 3.7; Was08, sec. 3.2], we introduce division polynomials, which constitute the main tool for our constructions. Let

$$E:\quad y^2 = x^3 + Ax + B$$

be an elliptic curve over a perfect field K with $\operatorname{char} K \notin \{2,3\}$. For $m = -1, 0, 1, 2, \dots$ we define the *division polynomials* $\psi_m \in K[A,B,x,y]$ as

$$\begin{aligned}
\psi_{-1} &= -1,\\
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 2y(2x^6 + 10Ax^4 + 40Bx^3 - 10A^2x^2 - 8ABx - 2A^3 - 16B^2),
\end{aligned}$$

and then recursively by means of the following relations:

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad \text{for } n \geq 2, \tag{25}$$

$$\psi_{2n} = \frac{\psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2}{\psi_2} \qquad \text{for } n \geq 3. \tag{26}$$

For ease of notation, we also define

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
2\psi_2\omega_m &= \psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

We now review some well-known results about division polynomials, which can be proven by induction (see e.g. [Was08, Lem. 3.3, 3.5]).

Proposition 6.1. *For each $m > 0$, the polynomial ψ_2 is an even-degree factor of*

$$\begin{cases} \psi_2\psi_m & \text{if } m \text{ is even},\\ \psi_m & \text{if } m \text{ is odd}. \end{cases}$$

In particular, ψ_m is a polynomial for each m.

Remark 6.2. If m is odd, ψ_m, ϕ_m and $\psi_2^{-1}\omega_m$ are polynomials in $K[A,B,x,\psi_2^2]$; the same holds, if m is even, for $\psi_2^{-1}\psi_m$, ϕ_m and ω_m. As a consequence, when evaluating these polynomials at points of E, ψ_2^2 can be substituted with $4(x^3 + Ax + B)$, so that the variable y no longer appears. Therefore, by a slight abuse of notation, we will often identify these polynomials with their representatives in the quotient ring

$$K[A,B,x,\psi_2^2]\big/(y^2 - x^3 - Ax - B) \cong K[A,B,x].$$

Proposition 6.3. *Consider ϕ_m and ψ_m^2 as elements in $K[A,B,x]$. Then*

$$\begin{aligned}
\phi_m(x) &= x^{m^2} + \textit{terms of lower degree}\\
\psi_m^2(x) &= m^2x^{m^2-1} + \textit{terms of lower degree}.
\end{aligned}$$

Theorem 6.4 (Computation of $[m]P$ via division polynomials)**.** *Consider an elliptic curve $E\colon y^2 = x^3 + Ax + B$ over K, a point $P = (x_0, y_0) \in E(\overline{K}) \setminus \{O\}$ and a positive integer m such that $[m]P \neq O$. Then, the point $[m]P$ can be calculated as follows:*

$$[m]P = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right) \tag{27}$$

or, equivalently,

$$[m]P = \left(x_0 - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y_0\psi_m^3}\right)$$

where we denote by ϕ_m*,* ψ_m *e* ω_m *the evaluations* $\phi_m(A,B,x_0,y_0)$*,* $\psi_m(A,B,x_0,y_0)$ *and* $\omega_m(A,B,x_0,y_0)$*.*

Proof. See [Was08, sec. 9.5]. □

Proposition 6.5 (Characterization of $E[m]$ via division polynomials)**.** *Let* $E\colon y^2 = x^3 + Ax + B$ *be an elliptic curve over* K*. Then*

$$E[m] = \{O\} \cup \{(x_0, y_0) \in E(\overline{K}) \mid \psi_m(A,B,x_0,y_0) = 0\}.$$

Proof. See [CR88, Prop. 9.10]. □

6.2 p-torsion points

Theorem 2.5 ensures that an elliptic curve E is supersingular if and only if $E[p] = \{O\}$. As in Section 4.4.2, in this section we construct a polynomial whose zeroes are exactly the coefficients A and B defining supersingular elliptic curves in Weierstrass form. In this case, though, the *coefficients* of such polynomial lie in a much bigger set, namely $\mathbb{F}_p[X]$.

Since any non-constant polynomial over $\mathbb{F}_p$ has its zeroes in $\overline{\mathbb{F}_p}$, Proposition 6.5 allows us to rephrase the characterization given in Theorem 2.5.(a) as follows:

Proposition 6.6. *Let* $E\colon y^2 = x^3 + Ax + B$ *be an elliptic curve over a field* $\mathbb{F}_q$ *of characteristic* p*. Then* E *is supersingular if and only if* $\psi_p(A,B,x)$ *is constant.*

A more refined result is given in [Dol18, Lemma 4]: we state it below in a more general fashion.

Proposition 6.7. *Let* $E\colon y^2 = x^3 + Ax + B$ *be a supersingular elliptic curve over* $\mathbb{F}_{p^2}$*. Then the polynomial*

$$\psi_{p^r} \quad \textit{with } r = \begin{cases} 1 & \textit{if } \operatorname{tr}(E) = \pm 2p \\ 2 & \textit{if } \operatorname{tr}(E) = 0 \\ 3 & \textit{if } \operatorname{tr}(E) = \pm p \end{cases}$$

is either 1 *or* -1 *in* $\mathbb{F}_p[A,B,x]$*.*

Proof. Doliskani's proof covers the case $\operatorname{tr}(E) = \pm 2p$, but it can be easily extended to the other cases. The characteristic polynomial of a supersingular curve E over $\mathbb{F}_{p^2}$ is

$$\begin{cases} X^2 \mp 2pX + p^2 & \text{if } \operatorname{tr}(E) = \pm 2p \\ X^2 + p^2 & \text{if } \operatorname{tr}(E) = 0 \\ X^2 \mp pX + p^2 & \text{if } \operatorname{tr}(E) = \pm p. \end{cases}$$

As a consequence, a suitable r-th power of Frobenius endomorphism φ_{p^2} equals $\pm[p^r]$, namely

$$\begin{cases} \varphi_{p^2} = \pm[p] & \text{if } \operatorname{tr}(E) = \pm 2p \\ \varphi_{p^2}^2 = -[p^2] & \text{if } \operatorname{tr}(E) = 0 \\ \varphi_{p^2}^3 = \mp[p^3] & \text{if } \operatorname{tr}(E) = \pm p. \end{cases}$$

Suppose $\operatorname{tr}(E) = -p$. From the latter equations we can write

$$[p^3](x,y) = \left(x^{p^6}, y^{p^6}\right) \tag{28}$$

for every $(x,y) \in E$, while from equation (27) and Proposition 6.3 we obtain

$$[p^3](x,y) = \left(\frac{\phi_{p^3}}{\psi_{p^3}^2}, \frac{\omega_{p^3}}{\psi_{p^3}^3}\right) = \left(\frac{x^{p^6} + \text{terms of lower degree}}{p^6 x^{p^6-1} + \text{terms of lower degree}}, \frac{\omega_{p^3}}{\psi_{p^3}^3}\right). \tag{29}$$

Comparing the first coordinates on the right-hand sides of (28) and (29) yields $\psi_{p^3}^2 = 1$. The other cases can be proven similarly. □

Proposition 6.7 suggests the following strategy to sample supersingular elliptic curves:

- compute $\psi_p^2 - 1$ as a polynomial in $\mathbb{F}_p[A, B, x]$;
- find values of A and B that annihilate $\psi_p^2 - 1$: these are parameters of a supersingular elliptic curve.

Some further assumptions can be made in order to diminish the number of monomials in ψ_p:

- restrict the root finding to $A, B \in \mathbb{F}_p$;
- assume $B = -1 - A$.

Equivalently, we consider $\psi_p^2 - 1$ as an element of the quotient ring $\mathbb{F}_p[A, B, x]/J$, where $J = (A + B + 1)(A^{p-1} - 1)$.
In fact, every $\mathbb{F}_{p^2}$-isomorphism class of supersingular curves over $\mathbb{F}_p$ contains at least one curve such that $B = -1 - A$.

Proposition 6.8. *For each supersingular j-invariant $j \in \mathbb{F}_p$ there is at least one elliptic curve in Weierstrass form that has j-invariant j, is defined over $\mathbb{F}_p$ and passes through $(1, 0)$.*

Proof. If $j = 1728$, the curve of equation $y^2 = x^3 - x$ has j-invariant 1728 and passes through $(1, 0)$. Assume $j \neq 1728$. Combining Theorem 2.7 and Hasse's inequality

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$$

(see e.g. [Was08, Thm. 4.2]), we know that any supersingular curve over $\mathbb{F}_p$ has exactly $p + 1$ points; in particular, it has an even number of points. Therefore, as O is one of them, and every $\mathbb{F}_p$-rational point (x, y) yields another point $(x, -y)$, every supersingular curve over $\mathbb{F}_p$ must intersect the horizontal axis an odd number of times. Let $(x_0, 0)$ be any point in the intersection of the horizontal axis with a supersingular curve $E\colon y^2 = x^3 + A'x + B'$ having j-invariant j. Thanks to Proposition 2.1.b, we can assume that E is defined over $\mathbb{F}_p$. Since j is non-zero, x_0 must be non-zero, too. Let $u \in \mathbb{F}_{p^2}^*$ be a square root of ${x_0}^{-1}$. Then [Sil09, p. 45] the curve defined by the coefficients

$$A = u^4 A', \qquad\qquad B = u^6 B'$$

is isomorphic to E and passes through $(1, 0)$ because we have

$$\begin{aligned} 1 + A' + B' &= 1 + \frac{A}{{x_0}^2} + \frac{B}{{x_0}^3} \\ &= \frac{1}{{x_0}^3}(x_0^3 + Ax_0 + B) \\ &= 0. \end{aligned}$$

□

6.2.1 Efficiency analysis

Even with the addition of extra assumptions on A and B, the computation of $\psi_{p^2} - 1$ remains unfeasible. The main obstacles are the recursive definition of division polynomials and their quickly-increasing degrees. Therefore, determining the coefficients of supersingular elliptic curves as roots of $\psi_{p^2} - 1$ seems an impractical method to solve the cSRS problem, despite the theoretical interest of Proposition 6.7.

6.3 Small-torsion points

In this section, we sketch a new method for sampling supersingular elliptic curves over $\mathbb{F}_p$, under the assumption that $p + 1$ has 'many' small factors.

Proposition 6.9. *Let $p = \prod_{i=1}^{r} \ell_i^{e_i} - 1$ be a prime such that*

$$\prod_{i=1}^{r} \ell_i > 2\sqrt{p}, \tag{30}$$

and let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve in Weierstrass form over $\mathbb{F}_p$. Denote by r' the minimum integer $\leq r$ satisfying (30)*. Then E is supersingular if and only if the division polynomial $\psi_{\ell_i}(A, B, x, y)$ has a root $(x_i, y_i) \in E(\mathbb{F}_p)$ for each $i \in \{1, \dots, r'\}$.*

Proof. Suppose that E be is supersingular. From Theorem 2.7 we know that the subgroup $E(\mathbb{F}_p)$ has $p+1$ elements. In particular, for any prime ℓ_i dividing $p+1$, Cauchy's theorem ensures that there exists a subgroup of $E(\mathbb{F}_p)$ having order ℓ_i. Equivalently, there exists an $\mathbb{F}_p$-rational ℓ_i-torsion point (x_i, y_i). Such point annihilates ψ_{ℓ_i} by Proposition 6.5.
For the converse, the bound (30) is needed. Suppose that there exists an $\mathbb{F}_p$-rational ℓ_i-torsion point for each $i \in \{1, \ldots, r'\}$. Then each ℓ_i divides $\#E(\mathbb{F}_p)$. Equivalently, by the CRT,

$$\#E(\mathbb{F}_p) \equiv 0 \mod \prod_{i=1}^{r} \ell_i. \tag{31}$$

Moreover, $\#E(\mathbb{F}_p)$ must satisfy Hasse's inequality

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}. \tag{32}$$

One can check that the only integer satisfying (30), (31) and (32) is $\#E(\mathbb{F}_p) = p + 1$. Therefore, E is supersingular by Theorem 2.7. $\square$

Remark 6.10. Some primes used in cryptographic applications do satisfy the hypotheses of Proposition 6.9: for example, the prime p in CSIDH-512 [Cas+18, § 8.1] is $p = 4 \cdot 587 \cdot \ell_1 \cdots \ell_{73} - 1$ where $\ell_1, \ldots, \ell_{73}$ are the first 73 odd primes.

Fix a prime $p = \prod_{i=1}^{r} \ell_i^{e_i} - 1$ such that (30) is satisfied for some (minimal) $r' \leq r$. Then, by Proposition 6.9, any solution of the system of equations

$$\begin{cases} \psi_{\ell_i}(A, B, x_i, y_i) = 0 & \text{for each } i \in \{1, \ldots r'\} \\ y_i^2 - x_i^3 - Ax_i - B = 0 & \text{for each } i \in \{1, \ldots r'\} \\ x_i^p - x_i = 0 & \text{for each } i \in \{1, \ldots r'\} \\ y_i^p - y_i = 0 & \text{for each } i \in \{1, \ldots r'\} \\ A^p - A = 0 \\ B^p - B = 0 \end{cases} \tag{33}$$

yields the coefficients of a supersingular elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$, together with the coordinates of $\mathbb{F}_p$-rational ℓ_i-torsion points (x_i, y_i) for $i \in \{1, \ldots, r'\}$.

6.3.1 Efficiency analysis

Despite working only for certain primes, the latter method seems promising. Indeed, the polynomials involved in system (33) have either low degree or sparse coefficients. An unsofisticated use of Groebner bases, though, is far from enough to turn this method into an efficient algorithm to solve the cSRS problem: in our experiments, it worked only for primes up to $12011 = 4 \cdot 3 \cdot 7 \cdot 11 \cdot 13 - 1$. We leave any improvement of this technique for future work.

7 Conclusions

We have provided a more precise framework for the SRS and cSRS problems, surveying a solution to the first, and presenting new approaches to the latter. A solution for the cSRS problem, though, is yet to be found. We hope that our formalisation of the problem, along with the analysis of the drawbacks in each method considered, will make a useful starting point for future research on the subject.

References

[AAM19] G. Adj, O. Ahmadi, and A. Menezes. "On Isogeny Graphs of Supersingular Elliptic Curves over Finite Fields". In: *Finite Fields and their Applications* 55 (2019), pp. 268–283.

[BJ03] O. Billet and M. Joye. "The Jacobi Model of an Elliptic Curve and Side-Channel Analysis". In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2003. Lecture Notes in Computer Science*. Vol. 2643. 2003, pp. 34–42.

[Brö09] R. Bröker. "Constructing supersingular elliptic curves". In: *Journal of Combinatorics and Number Theory* 1(3) (2009), pp. 269–273.

[Cas+18] W. Castryck et al. “CSIDH: An Efficient Post-Quantum Commutative Group Action”. In: *Advances in Cryptology – ASIACRYPT 2018*. Ed. by T. Peyrin and S. Galbraith. Cham: Springer International Publishing, 2018, pp. 395–427.

[CLG09] D. X. Charles, K. E. Lauter, and E. Z. Goren. “Cryptographic Hash Functions from Expander Graphs”. In: *Journal of Cryptology* 22 (1 2009), pp. 93–113.

[Coh93] H. Cohen. *A course in computational algebraic number theory*. Vol. 138. Graduate Texts in Mathematics. Berlin: Springer-Verlag, 1993.

[Cox13] D. A. Cox. *Primes of the Form* $x^2 + ny^2$. John Wiley & Sons, Ltd, 2013.

[CPV20] W. Castryck, L. Panny, and F. Vercauteren. “Rational Isogenies from Irrational Endomorphisms”. In: *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*. Ed. by A. Canteaut and Y. Ishai. Vol. 12106. Lecture Notes in Computer Science. Springer, 2020, pp. 523–548.

[CR88] L. S. Charlap and D. P. Robbins. *An elementary introduction to elliptic curves*. 1988. URL: `https://cs.nyu.edu/courses/spring05/G22.3220-001/ec-intro1.pdf`.

[CS17] C. Costello and B. Smith. “Montgomery curves and their arithmetic: The case of large characteristic fields”. In: *Journal of Cryptographic Engineering* 8 (2017), pp. 227–240.

[Deu41] M. Deuring. “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14.1 (1941), pp. 197–272.

[DFJP14] L. De Feo, D. Jao, and J. Plût. “Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies”. In: *J. Mathematical Cryptology* 8.3 (2014), pp. 209–247. URL: `https://doi.org/10.1515/jmc-2012-0015`.

[DG16] C. Delfs and S. D. Galbraith. “Computing isogenies between supersingular elliptic curves over F_p”. In: *Designs, Codes and Cryptography* 78 (2016), pp. 425–440.

[Dol18] J. Doliskani. “On Division Polynomial PIT and Supersingularity”. In: *Computing Research Repository (CoRR)* abs/1801.02664 (2018). arXiv: `1801.02664`. URL: `http://arxiv.org/abs/1801.02664`.

[Eis+18] K. Eisenträger et al. “Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions”. In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by J. B. Nielsen and V. Rijmen. Springer International Publishing, 2018, pp. 329–368.

[Eng06] A. Enge. “The complexity of class polynomial computation via floating point approximations”. In: *Mathematics of Computation* 78 (2006), pp. 1089–1107.

[Gal+16] S. D. Galbraith, C. Petit, B. Shani, and Y. B. Ti. “On the Security of Supersingular Isogeny Cryptosystems”. In: *Advances in Cryptology – ASIACRYPT 2016*. Ed. by J. H. Cheon and T. Takagi. `https://eprint.iacr.org/2016/859`. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 63–91.

[Gal18] S. D. Galbraith. *Mathematics of Public Key Cryptography. Version 2.0*. 2018. URL: `https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf`.

[GG13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. 3rd ed. Cambridge University Press, 2013.

[Gha+21] W. Ghantous, S. Katsumata, F. Pintore, and M. Veroni. *Collisions in Supersingular Isogeny Graphs and the SIDH-based Identification Protocol*. Cryptology ePrint Archive, Report 2021/1051. `https://ia.cr/2021/1051`. 2021.

[Has35] H. Hasse. “Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p.” In: *Journal für die reine und angewandte Mathematik* 172 (1935), pp. 77–85. URL: `http://eudml.org/doc/149903`.

[Hus87] D. Husemöller. *Elliptic Curves*. 2nd ed. Vol. 111. Graduate Texts in Mathematics. Springer New York, 1987.

[JMV09] D. Jao, S. Miller, and R. Venkatesan. “Expander graphs based on GRH with an application to elliptic curve cryptography”. In: *Journal of Number Theory* 129 (June 2009), pp. 1491–1504.

[Koh96] D. Kohel. “Endomorphism rings of elliptic curves over finite fields”. Ph.D thesis. 1996. URL: `http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf`.

[Lan87] S. Lang. *Elliptic Functions*. Graduate texts in mathematics. Springer, 1987.

[LB20] J. Love and D. Boneh. “Supersingular Curves With Small Non-integer Endomorphisms”. In: *Fourteenth Algorithmic Number Theory Symposium*. 2020, pp. 7–22.

[LO77] J. Lagarias and A. Odlyzko. “Effective Versions of the Chebotarev Density Theorem”. In: *Algebraic Number Fields, L-Functions and Galois Properties (A. Fr6hlich, ed.)* Ed. by A. Press. 1977, pp. 409–464.

[Lov96] L. Lovász. “Random Walks on Graphs: A Survey”. In: *Combinatorics, Paul Erdős is Eighty*. Ed. by D. Miklós, V. T. Sós, and T. Szőnyi. Vol. 2. Budapest: János Bolyai Mathematical Society, 1996, pp. 353–398.

[OKS00] K. Okeya, H. Kurumatani, and K. Sakurai. “Elliptic Curves with the Montgomery-Form and Their Cryptographic Applications”. In: *Public Key Cryptography*. Ed. by H. Imai and Y. Zheng. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 238–257.

[Pet17] C. Petit. “Faster Algorithms for Isogeny Problems Using Torsion Point Images”. In: *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*. Ed. by T. Takagi and T. Peyrin. Vol. 10625. Lecture Notes in Computer Science. Springer, 2017, pp. 330–353.

[Piz98] A. K. Pizer. “Ramanujan graphs”. In: *Computational perspectives on number theory (Chicago, IL, 1995)*. Amer. Math. Soc., 1998, 159–178.

[PL17] C. Petit and K. Lauter. *Hard and Easy Problems for Supersingular Isogeny Graphs*. IACR Cryptol. ePrint Arch. `https://eprint.iacr.org/2017/962`. 2017.

[Sch85] R. Schoof. “Elliptic Curves Over Finite Fields and the Computation of Square Roots $\bmod p$”. In: *Mathematics of Computation* 44.170 (1985), pp. 483–494. URL: `http://www.jstor.org/stable/2007968`.

[Sch87] R. Schoof. “Nonsingular plane cubic curves over finite fields”. In: *Journal of Combinatorial Theory, Series A* 46.2 (1987), pp. 183 –211.

[Sie35] C. L. Siegel. “Über die Classenzahl quadratischer Zahlkörper”. In: *Acta Arithmetica* 1 (1935), pp. 83–86.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Vol. 151. Graduate Texts in Mathematics. Springer, 2009.

[Sil94] J. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Springer-Verlag, 1994.

[Sut13] A. Sutherland. “Isogeny volcanoes”. In: *The Open Book Series* 1.1 (2013), 507—530.

[Tat66] J. Tate. “Endomorphisms of abelian varieties over finite fields”. In: *Inventiones mathematicae* 2 (1966), pp. 134–144.

[Ter99] A. Terras. *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[Vél71] J. Vélu. “Isogénies entre courbes elliptiques”. In: *Comptes Rendus de l’Académie des Sciences de Paris* 273 (1971), pp. 238–241.

[Vit19] V. Vitse. “Simple Oblivious Transfer Protocols Compatible with Supersingular Isogenies”. In: *Progress in Cryptology – AFRICACRYPT 2019*. Ed. by J. Buchmann, A. Nitaj, and T. Rachidi. Cham: Springer International Publishing, 2019, pp. 56–78.

[Was08] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2nd ed. Chapman & Hall/CRC, 2008.

[Wes21] B. Wesolowski. “The supersingular isogeny path and endomorphism ring problems are equivalent”. In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 1100–1111.