Annali di Matematica Pura ed Applicata (1923 -)
https://doi.org/10.1007/s10231-024-01528-x

On random sampling of supersingular elliptic curves

Marzio Mula[1] · Nadir Murru[2] · Federico Pintore[2]

Received: 8 March 2024 / Accepted: 13 November 2024

Abstract
We consider the problem of sampling random supersingular elliptic curves over finite fields of cryptographic size (SRS problem). The currently best-known method combines the reduction of a suitable complex multiplication (CM) elliptic curve and a random walk over some supersingular isogeny graph. Unfortunately, this method is not suitable when the endomorphism ring of the generated curve needs to be hidden, like in some cryptographic applications. This motivates a stricter version of the SRS problem, requiring that the sampling algorithm gives no information about the endomorphism ring of the output curve (cSRS problem). In this work we formally define the SRS and cSRS problems, which are both of theoretical interest. We discuss the relevance of the two problems for cryptographic applications, and we provide a self-contained survey of the known approaches to solve them. Those for the cSRS problem have exponential complexity in the characteristic of the base finite field (since they require computing and finding roots of polynomials of large degree), leaving the problem open. In the second part of the paper, we propose and analyse some alternative techniques—based either on the Hasse invariant or division polynomials—and we explain the reasons why they do not readily lead to efficient cSRS algorithms, but they may open promising research directions.

Keywords Isogeny-based cryptography · Isogeny graphs · Supersingular elliptic curves

Mathematics Subject Classification 14H52 · 11Y16 · 11T71

1 Introduction

The problem of efficiently sampling random supersingular elliptic curves over $\mathbb{F}_{p^2}$, or *SRS problem*, is not as easy as drawing marbles from a bag. When the prime p is large, the best known algorithm is only able to 'directly' extract a negligible fraction of all the existing supersingular elliptic curves, by leveraging some classical number-theoretic results (see [1, p. 4]) or by Bröker's algorithm [10]. The other curves can be sampled 'indirectly' as

✉ Marzio Mula
marzio.mula@unibw.de

Nadir Murru
nadir.murru@unitn.it

Federico Pintore
federico.pintore@unitn.it

[1] Research Institute CODE, University of the Bundeswehr, Munich, Germany

[2] Department of Mathematics, University of Trento, Trento, Italy

Published online: 02 December 2024

the endpoints of random walks in suitable isogeny graphs. In other words, they cannot be reached without first passing through one of those few supersingular elliptic curves which can be sampled directly. This is satisfactory when the only purpose is to efficiently sample uniformly random supersingular elliptic curves. However, some cryptographic applications require more: the output curve should be sampled in such a way that its endomorphism ring remains unknown. This further requirement can be met with the best-known algorithm for the SRS problem only by means of an oblivious computation, which in turn requires a trusted authority or a multiparty protocol [3, 44]. Apart from this cryptographic approach, though, a mathematical solution to the problem of sampling supersingular elliptic curves with unknown endomorphism ring, or *cSRS problem*, is yet to be found.

Although the cSRS problem is often mentioned in the literature [59, p. 71]; [18, p. 3], to the best of our knowledge no formal definition has been given.

Therefore, the first goal of this article is to formalize the SRS and cSRS problems, with the definition of the former being instrumental for that of the latter (Sect. 3).

Our second goal is to give a comprehensive and self-contained introduction to the known results on both the SRS and cSRS problems, which we consider to be still lacking in the literature. To this end, we provide a detailed description of the best-known algorithm for the SRS problem and survey some of the known approaches for the cSRS problem (Sect. 4).

In particular, we first give a thorough theoretical explanation of Bröker's algorithm [10], which is based on the the deep connection, already observed by Deuring in [24], between CM elliptic curves over number fields and elliptic curves over finite fields. To be more precise, it samples a supersingular elliptic curve modulo a large prime p by reducing modulo p some suitably-chosen CM curve. Then, we discuss why the algorithm which combines Bröker's algorithm with random walks in suitable supersingular isogeny graphs solves the SRS problem but does not solve the cSRS one. In fact, such an algorithm gives information on the endomorphism ring of the output curve. Later on, we consider some standard characterizations of supersingular elliptic curves, which lead to two highly inefficient methods for sampling supersingular elliptic curves with unknown endomorphism ring, i.e. exhaustive search over randomly sampled elliptic curves, and root-finding on a polynomial of large degree (the Hasse invariant).

In the second part of this work, we propose some alternative approaches to

the SRS and cSRS problems, exploring ways to sample supersingular elliptic curves which do not make use of CM curves. In particular, in Theorem 4.18 a classical result about the Hasse invariant is extended to elliptic curves in Jacobi form. Then,

in Sect. 5, we compute the Hasse invariant of different models of elliptic curves, in order to assess whether some models lead to sparser Hasse invariants. 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 Sect. 6.2, we prove the following generalization (Proposition 6.7) of a result in [29], from which we deduce another explicit characterization of supersingular elliptic curves in terms of their p-th division polynomial.

Proposition *Let E be an elliptic curve over $\mathbb{F}_{p^2}$, where p is a prime number. Then E is supersingular if and only if the division 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 $\mathbb{F}_p[x]$.

In Sect. 6.3, under an assumption on the shape of the prime p, we formulate a further characterization (Proposition 6.9) of supersingular elliptic curves based on $\mathbb{F}_p$-rational points of small torsion.

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

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

and denote by r' the minimum integer in $\{1, \ldots, r\}$ satisfying the above inequality. An elliptic curve E, over $\mathbb{F}_p$ and in Weierstrass form, is supersingular if and only if the division polynomial ψ_{ℓ_i} relative to E has a root $(x_i, y_i) \in E(\mathbb{F}_p)$ for each $i \in \{1, \ldots, r'\}$.

This characterisation of supersingular elliptic curves provides the following idea to sample supersingular elliptic curves. Given a prime $p = \prod_{i=1}^{r} \ell_i^{e_i} - 1$ such that (1) is satisfied for some (minimal) $r' \leq r$, then any solution of the system of equations

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

yields the coefficients A, B 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) on E for $i \in \{1, \ldots, r'\}$.

Unfortunately, none of the proposed alternative approaches leads to a solution of the cSRS problem, but we hope they may open fruitful research directions.

1.1 Related work

The SRS and cSRS problems are also tackled in an independent work (which was made public almost simultaneously with the finalisation of our work) by Booher et al. [9].

In [9, §2] the Hasse invariant $H_p(\lambda)$ is considered for elliptic curves in Legendre form, with additional remarks on how some root over $\mathbb{F}_p$ could be found, by means of an iterative method which also requires an efficient evaluation of the derivative $H_p'(\lambda)$ over $\mathbb{F}_p$. Moreover, some variants of the method which we derive from Proposition 6.9 are illustrated in [9, §4].

The following new approaches are also presented in [9]:

- Computing the roots of gcd $(\Phi_n(x, x^p), \Phi_m(x, x^p))$, where n, m are positive integers coprime with p and Φ_n, Φ_m denote the modular polynomials of levels n and m, respectively [9, §3]. This amounts to finding j-invariants of elliptic curves having two non-scalar endomorphisms of degrees np and mp, respectively. The roots found have good chances of being supersingular and can be computed in time linear with respect to m, n and $\log p$. However, since the output curve has a non-scalar endomorphism of degree nm, either m or n should have the same size as p (otherwise the endomorphism ring can be retrieved [41], as we will explain more thoroughly in the proof of Proposition 4.14).
- Finding supersingular elliptic curves as components of algebraic varieties of higher dimension or higher genus [9, §5]. One method consists in performing a random walk

on the isogeny graph of abelian surfaces, starting from a product of supersingular elliptic curves, until another product of (supersingular) elliptic curves is reached. Another method starts from Kummer surfaces of superspecial abelian surfaces, and looks for their components (if any).

- Using a quantum computer to perform a random chain of ℓ-isogeny paths 'in superposition', for some small primes ℓ [9, §5]. This method hides most of the information that a classic ℓ-isogeny path would otherwise reveal, but requires a quantum computer to be implemented.

Despite their theoretical interest, none of the methods presented in [9] result in an efficient algorithm for the cSRS problem.

We stress that, even though [9] and our work bear some similarities, these two works are complementary as they propose some similar but not identical approaches. Furthermore, our work aims also at giving a self-contained survey on the topic, while providing the first formalisations of the cSRS problem.

2 Preliminaries

2.1 Elliptic curves

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

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

having a base point at infinity O and such that the *discriminant*, $\Delta(E) = -16(4A^3 + 27B^2)$, is not 0. Every elliptic curve E can be endowed with the structure of an abelian group $(E, +)$ whose zero element is O [53, § III.2].

Since elliptic curves are defined up to isomorphism, there exist various representations other than the Weierstrass model considered above. In Table 1, we summarize the form of the affine equation and the corresponding formula for the j-invariant (whose definition is recalled in the following Sect. 2.2) for some of these alternative models. We also provide the values of the coefficients A and B of an isomorphic elliptic curve in Weierstrass form.

2.2 Isogenies and isomorphisms

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 [53, § III.4] for the basic properties of isogenies and the definition of degree.

An isogeny of degree 1 is an isomorphism. Every isomorphism class of elliptic curves over $\overline{K}$ can be uniquely identified by an element $j \in K$, called the j*-invariant*. The value of j can be easily retrieved from the coefficients of any elliptic curve $E\colon\, y^2 = x^3 + Ax + B$ in the isomorphism class as

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

Table 1 Other models of elliptic curves

Model	Affine equation	j-invariant	Equivalent Weierstrass form
Legendre [53, 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 [20, § 2.4]	$B'y^2 = x^3 + A'x^2 + x$	$\frac{256(A'^2-3)^3}{A'^2-4}$	$\begin{cases} A = B'^2\left(1-\frac{A'^2}{3}\right) \\ B = \frac{B'^3A'}{3}\left(\frac{2A'^2}{9}-1\right) \end{cases}$
Jacobi [7, § 3]	$y^2 = \epsilon x^4 - 2\delta x^2 + 1$	$64\frac{(\delta^2+3\epsilon)^3}{\epsilon(\delta^2-\epsilon)^2}$	$\begin{cases} A = -4\epsilon - \frac{4}{3}\delta^2 \\ B = -\frac{16}{27}\delta(\delta^2-9\epsilon) \end{cases}$

We recall from [53, Prop. III.1.4.b-c] the fundamental properties of j-invariants.

Proposition 2.1 *(a) Two elliptic curves over K are isomorphic over $\overline{K}$ if and only if they have the same j-invariant.*
(b) Let $j_0 \in \overline{K}$. There exists an elliptic curve over $K(j_0)$ whose j-invariant is j_0.

Given an elliptic curve E, for each positive integer m, let $[m]$ denote the ‘multiplication-by-m’ map which is an isogeny from E to itself such that:

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

for each $P \in E$. 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 $E[m] = \ker[m]$.

Let $\operatorname{End}(E)$ be the set of endomorphisms of an elliptic curve E (that is, isogenies $E \to E$). Since $\operatorname{End}(E)$ is a torsion-free ring, 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 *scalar*. Whenever the map $[\ \ ]$ is *not* surjective, that is, there exists some non-scalar 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 to generate supersingular elliptic curves over finite fields, as we are going to see in Sect. 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 $\varphi \circ \hat{\varphi} = \hat{\varphi} \circ \varphi = [m]$.

Proof See [53, Thm. III.6.1.a]. □

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

2.3 Endomorphism rings

In this section we summarize some fundamental facts about the structure of $\mathrm{End}(E)$ for an elliptic curve E. We first recall that an algebra B over a field K (with 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 as a K-vector space and

$$i^2 = a, \qquad j^2 = b, \qquad ji = -ij \tag{3}$$

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.

Theorem 2.3 (Structure of $\mathrm{End}(E)$) *Let E be an elliptic curve over K. Then* $\mathrm{End}(E)$ *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 [53, 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

$$\varphi^2 - [a] \circ \varphi + [d] = [0]. \tag{4}$$

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 over a finite field $\mathbb{F}_q$ of characteristic p, the endomorphism

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

is called the *q-th power Frobenius endomorphism* of E, and its trace is the *trace of E* over $\mathbb{F}_q$. Moreover, its degree equals q [53, Prop. II.2.11], so that the following 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 exploited in Sects. 4, 5 and 6 to generate supersingular curves. In the following, we will use p for a prime number larger than 3 and q for a generic power p^n with $n \in \mathbb{N}$.

Theorem 2.5 (Definitions of supersingular elliptic curve) *Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_q$. The following are equivalent:*

(a1) $E[p^r] = \{O\}$ *for some* $r \geq 1$.
(a2) $E[p^r] = \{O\}$ *for each* $r \geq 1$.

(b) *The endomorphism* $[p]: E \to E$ *is purely inseparable*[1] *and* $j(E) \in \mathbb{F}_{p^2}$.
(c) $\mathrm{End}(E)$ *is an order in a quaternion algebra over* $\mathbb{Q}$.
(d) $\#E(\mathbb{F}_q) \equiv 1 \mod p$.

If an elliptic curve satisfies one of the above conditions, it is called supersingular. *In particular, the set of* supersingular j-invariants, *i.e.*

$$\{\, j(E) \mid E \textit{ is supersingular over } K\,\},$$

lies in $\mathbb{F}_{p^2}$.

Proof See [53, Thm. V.3.1];[61, Prop. 4.31]. □

We highlight that every supersingular elliptic curve is a CM curve (this actually holds true for every elliptic curve defined over a finite field). Non-supersingular elliptic curves are called *ordinary*.

Corollary 2.6 *Every supersingular elliptic curve over a field of characteristic p is isomorphic to a supersingular elliptic curve 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. □

2.5 Supersingular ℓ-Isogeny Graphs

Supersingular ℓ-isogeny graphs are a major object of study in isogeny-based cryptography. Their vertices represent (isomorphism classes of) supersingular elliptic curves, while their edges are isogenies of degree ℓ for some prime $\ell \neq p$. For $\ell \sim \log p$, one can 'walk' on the supersingular ℓ-isogeny graph in such a way that

- each step can be performed quickly (via Vélu's formulae, see [35, § 25.1.1];[58]);
- starting from a given supersingular elliptic curve, every other supersingular elliptic curve can be reached within a 'small' number of steps;
- the endpoints of 'long enough' 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 graph. Finally, referring to a famous result due to Pizer [47], we show that random walks on suitably-chosen supersingular ℓ-isogeny graphs end on 'random' vertices.

2.5.1 Random walks

Let G be a graph with set of vertices $V = \{v_1, \ldots, v_n\}$ and set of edges $\mathcal{E}$. 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;

[1] We refer to [53, p. 21] for a precise definition of purely inseparable isogenies.

- for each pair of vertices $v_i, v_j \in V$,

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

  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. If G is k-regular, then its transition matrix T is closely related to the adjacency matrix A, namely:

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

Since the adjacency matrix encloses all information about the structure of G, it is natural to ask which assumptions on G ensure that a sufficiently-long random walk on the graph approaches the uniform distribution, no matter how the starting vertex is chosen. To address this question, we call a *probability function* a non-negative map $p\colon V \to \mathbb{R}$ such that $\sum_{i=1}^{n} p(v_i) = 1$. We represent p as a vector $(p_1, \ldots, p_n)$ where $p_i = p(v_i)$.

Remark 2.7 Let n be the number of vertices of G, and suppose that we are able to sample a starting node X_0 in G according to a certain probability function $p = (p_1, p_2, \ldots, p_n)$. Then, a random walk from X_0 of length t and transition matrix T on G allows us to sample vertices with probability distribution $T^t p$.

Theorem 2.8 *Suppose that the graph $G = (V, \mathcal{E})$ is connected, non-bipartite and k-regular with n vertices. Let A be its adjacency matrix and $T = (1/k)A$ the Markov transition matrix. Then, for every probability function p on G we have*

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

where u is the uniform distribution $u = (1/n, \ldots, 1/n)$.

Proof See [57, Thm. 6.1]. □

A classical way to enforce a fast convergence to the uniform distribution is to consider only *non-backtracking* random walks, i.e. random walks $(X_t)_{t\geq 0}$ such that $X_t \neq X_{t+2}$ for each $t \geq 0$. The rate of convergence in this particular case is quantified in [2] by considering the mixing rate. Given a k-regular graph $G = (V, \mathcal{E})$ with n vertices, the *mixing rate* of a non-backtracking random walk on G is defined as

$$\rho = \limsup_{t\to\infty} \max_{i,j} \left(\left|\mathbb{P}[X_t = v_i \mid X_0 = v_j] - 1/n\right|\right)^{\frac{1}{t}},$$

The convergence of a non-backtracking random walk to the uniform distribution is closely related to the absolute values of the eigenvalues of the adjacency matrix.

Theorem 2.9 *Suppose that the graph $G = (V, \mathcal{E})$ is connected, non-bipartite and k-regular ($k \geq 3$) with n vertices. Define $\psi : [0, \infty) \to \mathbb{R}$ by:*

$$\psi(x) = \begin{cases} x + \sqrt{x^2 - 1} & \mathit{if}\, x \geq 1, \\ 1 & \mathit{if}\, 0 \leq x \leq 1. \end{cases}$$

Then its mixing rate ρ satisfies

$$\rho = \frac{\psi\left(\frac{\max(|\lambda_2|,|\lambda_n|)}{2\sqrt{k-1}}\right)}{\sqrt{k-1}},$$

where $\lambda_1 = k > \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of the adjacency matrix of G.

Proof See [2, Thm 1.1]. □

Building on the above theorem, [2] proves that the mixing rate of a non-backtracking random walk may be up to twice as fast as the mixing rate ρ' of a generic random walk. In particular, the maximum value of the ratio ρ/ρ' is achieved when the k-regular graph G is *Ramanujan*, i.e.

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

2.5.2 Rapid mixing on isogeny graphs

Let ℓ and p be two distinct primes, $p \geq 5$ and $q = p^n$ for some non-zero $n \in \mathbb{N}$. By Tate's theorem [56, § 3], two elliptic curves over $\mathbb{F}_q$ are $\mathbb{F}_q$-isogenous 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 [1, §3]:

- its vertices are the $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$ with trace a. For each vertex we set a representative and we denote by $\mathcal{V}_\ell(\mathbb{F}_q, a)$ a complete set of representatives;
- given $E, E' \in \mathcal{V}_\ell(\mathbb{F}_q, a)$, the edges between the corresponding vertices are the isogenies $E \to E'$ over $\mathbb{F}_q$ of degree ℓ, modulo post-composition with an $\mathbb{F}_q$-automorphism.

An easy consequence of Tate's theorem is that two curves in the same ℓ-isogeny graph are either both supersingular or both ordinary, depending on whether their trace over $\mathbb{F}_q$ is a multiple of p. From now on we will focus on supersingular ℓ-isogeny graphs (more information about the ordinary case can be found in [39, 55]).

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 [1].

Proposition 2.10 *Let $a \in \{2p, -2p\}$. Then, each supersingular j-invariant $j_0 \in \mathbb{F}_{p^2}$ is represented by exactly one vertex in $\mathcal{G}_\ell(\mathbb{F}_{p^2}, a)$.*

Proof See [1, pp. 5-6]. □

An alternative supersingular ℓ-isogeny graph, denoted by $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, can be defined as follows:

- its vertices are the $\overline{\mathbb{F}_p}$-isomorphism classes of elliptic curves over $\overline{\mathbb{F}_p}$. For each vertex we set a representative (defined over $\mathbb{F}_{p^2}$) and we denote by $\mathcal{V}_\ell(\overline{\mathbb{F}_p})$ a complete set of representatives;
- given $E, E' \in \mathcal{V}_\ell(\overline{\mathbb{F}_p})$, the edges between the corresponding vertices are the isogenies $E \to E'$ over $\overline{\mathbb{F}_p}$ of degree ℓ, modulo post-composition with an $\overline{\mathbb{F}_p}$-automorphism.

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

Theorem 2.11 *$\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ and $\mathcal{G}_\ell(\mathbb{F}_{p^2}, \pm 2p)$ are isomorphic.*

Proof See [1, Thm. 6]. □

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

Proposition 2.12 *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 $\ker \alpha$ has order ℓ [53, Thm. III.4.10]; in particular,

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

By [53, 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 of E, the quotient curve $E' = E/G$ (i.e. the image of the isogeny with kernel G) is unique up to post-composition with an isomorphism [53, Prop. III.4.12]. □

Actually, with the possible exception of the vertices 0 and 1728 and their neighbours [1, Thm. 7], we can consider $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ as an undirected $(\ell + 1)$-regular graph. In [47], a stronger result is proven.

Theorem 2.13 *$\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ is Ramanujan.*

Further results about the Ramanujan property of isogeny graphs have recently appeared. For instance, in [14, Cor. 1.8], the authors prove that this property holds for a larger family of isogeny graphs with level structure.

A fundamental feature of Ramanujan graphs, which is particularly relevant for cryptographic applications, is their *rapid mixing property*. This property can be also seen as a particular case of a more general statement proven in [48, Thm. 3.10]. Here we focus on non-backtracking random walks on $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, as their mixing rate improves that of generic random walks (see Theorem 2.9). Notably, the length of non-backtracking random walks can be explicitly related to their rate of convergence to the uniform distribution.

Theorem 2.14 *Let $\varphi : E \to E'$ be a non-backtracking random walk of length h on $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. Then, for all $\epsilon \in]0, 2]$, the distribution of E' has statistical distance $\tilde{O}(p^{-\epsilon/2})$ to the uniform distribution in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$, provided that $h \geq (1 + \epsilon)\log_\ell p$.*

Proof See [22, Prop. 29]. □

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 present the main hard mathematical problems on which the security of isogeny-based cryptography is based in Sect. 3.1.

Then, in Sect. 3.2, we provide some examples of cryptosystems whose security is affected by the (partial) knowledge of the endomorphism ring of the *starting* supersingular elliptic curve. Finally, in Sect. 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

The following mathematical problems are considered computationally hard [34, § 2.2].

Problem 1 *(ℓ-ISOGENYPATH) Let p and ℓ be distinct primes. Given two uniformly-random 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 prime p and a uniformly-random 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.*

There exist supersingular elliptic curves whose endomorphism rings can be easily computed; namely, those having non-scalar endomorphisms of small degree. We will discuss this in Sect. 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 under heuristic assumptions or Generalized Riemann Hypothesis. More precisely:*

- *if two elliptic curves E, E' are given together with their endomorphism rings* $\mathrm{End}(E)$ *and* $\mathrm{End}(E')$*, then an ℓ-isogeny $E \to E'$ can be computed in polynomial time;*
- *if an elliptic curve E is given together with an ℓ-isogeny $E \to E'$ and the endomorphism ring* $\mathrm{End}(E')$*, then* $\mathrm{End}(E)$ *can be computed in polynomial time.*

Proof This was proven first under heuristic assumptions in [31, § 5.5], and later in [62] under the Generalized Riemann Hypothesis. □

3.2 Cryptographic applications

Hard mathematical problems can often be exploited to construct secure cryptographic protocols, and ℓ-ISOGENYPATH and ENDRING are no exceptions. Here we provide some examples, which will naturally lead us to the formulation of the SRS and cSRS problems in Sect. 3.3. In particular, concerning the cSRS problem, we will discuss how a *naive* choice of the supersingular elliptic curves involved in some of these protocols can heavily undermine their security.

The digital signatures SQIsignHD and SQIsign2D-West Many of the isogeny-based digital signatures that have been recently proposed (see, for example, [4, 5, 22, 26, 36]) are built on a Σ-protocol (between a Prover and a Verifier) by using the Fiat-Shamir transform. The base Σ-protocol is required to satisfy some security properties for the resulting digital signature to be resistant against forgery attacks. More precisely, the Σ-protocol should be special sound and honest-verifier zero knowledge (HVZK). The latter property guarantees that no information

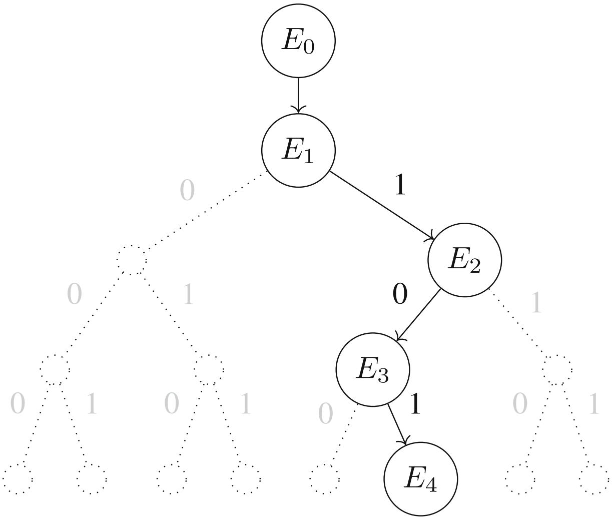

Fig. 1 The path followed by the CGL function within the graph $\mathcal{G}_2(\overline{\mathbb{F}_p})$ for the bitstring 101

is leaked about the secret material during the interaction between prover and verifier. This usually translates in the need, for the first message of the interaction (the commitment), to be uniformly distributed over a public set. For example, in SQIsignHD [22] and SQIsign2D-West [5], the distribution of the commitment should be close to uniform among supersingular elliptic curves over a given finite field $\mathbb{F}_{p^2}$. The special-sound property of the base Σ-protocol is backed by the hardness of EndRing.

CGL hash function The *CGL function* [15] is a hash function based on the ℓ-isogeny graph $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ for some small prime $\ell \neq p$. Such function is outlined in Algorithm 1 for the case $\ell = 2$. Figure 1 depicts the path in $\mathcal{G}_2(\overline{\mathbb{F}_p})$ determined by the computation of the image of the bitstring 101.

Algorithm 1: CGL hash function

```
Input: A supersingular elliptic curve $E_0$ over $\mathbb{F}_{p^2}$; a bitstring $m$ of $n$ bits, i.e. $m = b_1 b_2 \cdots b_n$.
Output: $\mathsf{CGL}(m)$.
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 the map $E_i \to E_i/\langle P \rangle$ with kernel $\langle P \rangle$ is the dual of $\varphi_{i-1}$;
    Label the remaining 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 $\mathsf{CGL}(m) = j\left(E_{n+1}\right)$;
```

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 (see [15, § 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 collisions becomes easy as well.

VDF based on ℓ-isogeny graphs A function is called a *verifiable delay function (VDF)* [8] if it requires a specified number of sequential steps to be evaluated (independent of the hardware architecture used for the computation) and it is possible to efficiently verify that a value is the correct output of the function. In particular, evaluating a VDF over any input should not be significantly easier if parallel computation is employed.

In [25, §3,§5], De Feo et al. construct a VDF that consists in evaluating at some point $Q \in E'(\mathbb{F}_p)$ a given ℓ^T-degree isogeny $\hat{\varphi}\colon E' \to E$ between two supersingular elliptic curves defined over $\mathbb{F}_p$. Such evaluation requires, in general, polynomial time in T.

However [25, §6.2], if $\mathrm{End}(E)$ is known, an auxiliary isogeny $\psi\colon E \to E'$ of small degree can be precomputed and exploited to speed up the computation of $\hat{\varphi}(Q)$, breaking the sequentiality of the VDF. Therefore, as in the previous example, E should be chosen in such a way that no information about its endomorphisms can be retrieved easily.

Delay encryption The same computational challenge described above—i.e. evaluating at some point $Q \in E'(\mathbb{F}_p)$ a given ℓ^T-degree isogeny $\hat{\varphi}\colon E' \to E$ between two supersingular elliptic curves defined over $\mathbb{F}_p$—is also exploited in [6] to instantiate a new cryptographic primitive called *delay encryption*, used to produce encrypted messages that can be decrypted (by anyone) only after a given amount of time T. In this case, too, the choice of E is problematic for the same reasons described in the previous paragraph, so that anyone knowing $\mathrm{End}(E)$ would be able to decrypt messages earlier than expected.

Public-key cryptosystems Until July 2022, the key encapsulation mechanism SIKE, based on the public-key cryptosystem SIDH [27], was one of the flagships of isogeny-based cryptography. Its fall was due to three attacks [13, 43, 49], the latter of which proved that randomizing the starting curve is not enough to avoid the attack. However, new protocols are still rising from the ashes of SIKE: two examples that require random supersingular elliptic curves among their parameters are IS-CUBE [45] and M-SIDH [33, §7].

Other applications We have already observed that the knowledge of $\mathrm{End}(E)$ can be exploited to speed up the computation of isogenies starting from E. When this fact does not represent a security issue, it provides on the contrary a good motivation for using E instead of some other supersingular elliptic curve with unknown endomorphism ring. This is the case for SQISign [26] and SQISignHD [22], and also CSIDH [12], the VDF in [21] and many other isogeny-based protocols. However, we cannot exclude that the discovery/refinement of attacks might eventually force the use of supersingular elliptic curves with unknown endomorphism rings for some of these protocols, too.

3.3 SRS and cSRS problems

In this section we formalize the problem of (almost) uniformly sampling supersingular elliptic curves over $\mathbb{F}_{p^2}$, in two different flavours:

- the first, weaker, version solely focuses on the mathematical problem;
- the second, stronger, version adds some further requirements which take into account the cryptographic applications.

A *supersingular random sampler* is a randomized algorithm A, on input a prime p and a random seed s, that produces a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ in such a way that the output distribution of A – as s varies—is computationally indistinguishable from the uniform distribution over the set of all supersingular elliptic curves over $\mathbb{F}_{p^2}$.

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 of Theorem 2.14. Namely, on input p and a random seed s, A simply performs the CGL hash of s starting from $E \leftarrow \mathsf{A}'(p)$.

The first problem we define is named Supersingular Random Sampler (SRS in short) problem:

Supersingular Random Sampling (SRS) problem
Construct a supersingular random sampler whose time complexity is polynomial in $\log p$.

Remark 3.3 The SRS problem finds a cryptographic application, for example, in SQIsignHD and SQIsign2D-West. In fact, a solution for the problem enforces the Honest-Verifier Zero-Knowledge property of the base Σ-protocol in both cases.

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, relative to A itself.

Problem 3 *(*EndRing$_{\mathsf{A}}$*) Given* $E \leftarrow \mathsf{A}(p, s)$ *and the random seed s, compute* $\mathrm{End}(E)$.

Given a supersingular random sampler A, we say that A is a *supersingular random crypto sampler* if EndRing$_{\mathsf{A}}$ is computationally hard. This definition motivates the following stronger version the SRS problem.

Crypto Supersingular Random Sampling (cSRS) problem
Construct a supersingular random crypto sampler whose time complexity is polynomial in $\log p$.

Remark 3.4 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 random seed 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 random seed of A is equivalent to computing $\mathrm{End}(E)$. Therefore, if computing $\mathrm{End}(E)$ is easy, then A cannot be a supersingular random crypto sampler.

3.3.1 SRS and cSRS problems over $\mathbb{F}_p$

Our formalisation of the SRS and cSRS problems deals with supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, while the majority of applications considered in Sect. 3.2 make use of supersingular elliptic curves defined over the subfield $\mathbb{F}_p$. Nothing ensures that an efficient supersingular random (crypto-)sampler can find supersingular elliptic curves over $\mathbb{F}_p$ as efficiently as over $\mathbb{F}_{p^2}$, since the probability that a random supersingular elliptic curve over $\mathbb{F}_{p^2}$ is defined over $\mathbb{F}_p$ is about $1/\sqrt{p}$ [28, §4]. However, all the methods considered in this paper can be easily adapted to sample supersingular elliptic curves defined over $\mathbb{F}_p$ (in fact, most of them can be made more efficient in this way). For this reason we will often switch between $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$.

It is also worth mentioning that some extra information about $\operatorname{End}(E)$ is automatically known when E is defined over p. To be more precise, the imaginary quadratic order $\mathbb{Z}[\sqrt{-p}]$ embeds in $\operatorname{End}(E)$ via the map $\sqrt{-p} \mapsto \pi$, where π is the Frobenius endomorphism. Nevertheless, retrieving the full endomorphism ring of E from this information is considered a hard problem. In fact, the security of CSIDH relies (also) on it [63, Cor. 5].

4 Known approaches

We now survey some known supersingular random samplers which solve the SRS problem, showing that none of them leads to a supersingular random crypto sampler.

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

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

Our goal for this section is to provide a comprehensive and illuminating explanation of the combination of these blocks.

In Sect. 4.3.2 we will discuss why the resulting algorithm is not a supersingular random crypto sampler. Finally, in Sect. 4.4 we present some cSRS algorithms. They are mainly of theoretical interest, though, since their computational cost is exponential in $\log p$, and therefore they are not a solution of the cSRS problem.

4.1 Bröker's algorithm

For any given prime $p \geq 5$, at least one supersingular j-invariant over $\mathbb{F}_{p^2}$ can be efficiently found thanks to Bröker's algorithm [10], whose core is the reduction of a suitable CM elliptic curve. We recall that an elliptic curve E over a number field K *has a good reduction* modulo $\mathfrak{P}$ if the $\mathfrak{P}$-adic valuation of $\Delta(E)$ does not equal 0 (see [53, § 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 $\mathfrak{P}$.

Theorem 4.1 (Deuring) *Fix a prime $p \geq 5$. Let E be an elliptic curve over a number field K, with* $\operatorname{End}(E)$ *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 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 in k).*

Moreover, let $\mathscr{E}$ be an elliptic curve over a field of characteristic p with a non-scalar 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 [24, 40, Thm. 13.12 and 13.14]. □

The first part of Deuring's theorem provides a criterion for determining whether the reduction modulo a suitable 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 CM curve.

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—over some number field—such that p does not split in $\mathrm{End}(E)$. Equivalently, if we denote by k the imaginary quadratic field which $\mathrm{End}(E)$ is an order of, and by D the discriminant of k, p does not split in k if and only if

$$\left(\frac{D}{p}\right) \neq 1, \tag{5}$$

where the left-hand expression denotes the Legendre symbol [17, Prop. 5.16, Cor. 5.17].

Once a quadratic field k satisfying (5) is fixed, the goal is to determine the CM j-invariants whose endomorphism rings lie in k. To this end, a deeper insight into 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 be two $\mathbb{R}$-linearly independent vectors in the complex plane $\mathbb{C}$ (viewed 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 [17, § 10];[53, § C.11];[61, § 9.1–9.3, 10.1] (see also [35, § 16.1] for a general overview on lattices in $\mathbb{R}^n$).

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

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

converges [61, 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 Λ is defined as

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}. \tag{6}$$

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

Proof See [17, 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

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

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

Proof See [61, § 9.2 and 9.3]. □

The following proposition clarifies the connection between a complex lattice 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*

$$\mathrm{End}(E_\Lambda) \cong \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}. \tag{7}$$

Proof See [61, Thm 10.1]. □

Therefore, for a complex lattice Λ such that $\mathbb{Z} \subsetneq \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}$, the corresponding elliptic curve E_Λ has complex multiplication. In 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 [17, § 10.C]. □

Remark 4.6 On the other hand, a complex sublattice of an imaginary order $\mathcal{O}$ is not, in general, a fractional ideal, nor even a subring, of $\mathcal{O}$. For example, consider $k = \mathbb{Q}(\sqrt{-1})$ 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 (7), 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 [17, § 7.A]. When it is (i.e. Λ is *not* a fractional ideal of 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 fractional 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. □

The above result provides a class of complex elliptic curves whose endomorphism ring is exactly $\mathcal{O}$, that is 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 ideal of $\mathcal{O}$.*

Proof See [17, Thm. 10.14]. □

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 ideal of $\mathcal{O}$, say 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 (7) 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 ideal of $\mathcal{O}\simeq$, which we denote by 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.
$\mathcal{O} = \mathcal{O}\simeq$. □

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 and that the image is a set of j-invariants of CM curves with endomorphism ring $\mathcal{O}$. Finally, surjectivity follows from Corollary 4.9. □

Hilbert class polynomials Corollary 4.10 alone does not provide an explicit strategy to compute CM j-invariants. In fact, even though a suitable complex lattice Λ can be easily determined, the infinite sums $g_2(\Lambda)$ and $g_3(\Lambda)$ involved in (6) 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 the ideal class group $\mathscr{C}(\mathcal{O})$. Then the polynomial*

$$P_{\mathcal{O}} = \prod_{i=1}^{h}\bigl(X - j(E_{\Lambda_i})\bigr) \tag{8}$$

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 [17, Thm. 13.2]. □

The polynomial $P_{\mathcal{O}}$ defined in (8) is called *Hilbert class polynomial* (or *ring class polynomial*, whenever $\mathcal{O}$ is not maximal) of the imaginary 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 [16, § 7.6.2]:

(1) Compute a set of representatives $\Lambda_1, \Lambda_2, \dots, \Lambda_h$ for $\mathscr{C}(\mathcal{O})$. Equivalently, following [16, § 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

$$j(\tau) = 1728 \frac{\left(1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k}\right)^3}{\left(1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k}\right)^3 - \left(1 - 504 \sum_{k=1}^{\infty} \frac{k^5 q^k}{1-q^k}\right)^2}, \tag{9}$$

where $q = e^{2\pi i \tau}$ [61, Prop. 9.12].

(3) If the approximations $\tilde{j}_1, \ldots, \tilde{j}_h$ 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 (9) 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 (9), the second one requires a deeper analysis of the coefficients of $P_{\mathcal{O}}$ [32, § 4].

4.1.2 The algorithm

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

(1) Choose an imaginary quadratic field k whose discriminant D satisfies equation (5);
(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 summarized 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 $\log p$, and the j-invariant found lies in $\mathbb{F}_p$. This is achieved by executing the following steps:

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

In particular, the fact that q is the smallest possible ensures that $\mathcal{O}$ is uniquely determined by p, and for this reason we will denote it by $\mathcal{O}_p$ in the following. 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 [10, 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 of the elements of $\mathbb{Z}/p\mathbb{Z}$ are quadratic non-residues. In [42] it is proven that, under the Generalized Riemann Hypothesis, q has size $O\big((\log p)^2\big)$.
- $P_{\mathcal{O}}$ can be computed in $\tilde{O}(\mathrm{disc}(\mathcal{O})) = \tilde{O}(q) = \tilde{O}\big((\log p)^2\big)$ time, as we have already pointed out in Sect. 4.1.1.
- a root of $P_{\mathcal{O}}$ in $\mathbb{F}_p$ can be found, as described for example in [60, § 14.5], in probabilistic time

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

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 $j = \alpha$.
```

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 [52], where $h(\mathcal{O})$ denotes the class number of the order $\mathcal{O}$).

4.2 Extending Bröker's algorithm

The output distribution of Bröker's algorithm is far from being uniform. In fact, for any p, the output belongs to a pre-determined subset of all possible supersingular j-invariants over $\mathbb{F}_{p^2}$, i.e. the roots of $P_{\mathcal{O}}$ in $\mathbb{F}_p$, of which there are $\tilde{O}(\sqrt{q})$. In order to construct an SRS algorithm, we would need to expand this set of possible outputs: it can be done, mathematically, by applying the general strategy summarized at the beginning of Sect. 4.1.2, but it comes—as we will now see following [41]—with the price of a major computational tradeoff.

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*

$$\{\textit{Imaginary quadratic orders}\} \leftrightarrow \mathbb{Z}_{<0}$$

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

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

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

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

we have

$$\mathcal{D} = \left\{f^2 d \mid f, d \in \mathbb{Z},\ d < 0,\ d \textit{ square-free and either } d \equiv 1 \bmod 4 \textit{or } f \textit{ is even}\right\}. \quad (10)$$

Proof We recall from [17, § 5.B] that every imaginary quadratic field can be written as $\mathbb{Q}(\sqrt{D})$ with D negative square-free integer, 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 [17, Lemma 7.2].

Finally, the discriminant of an order of conductor f in $\mathbb{Q}(\sqrt{D})$ is $f^2 d_{\mathbb{Q}(\sqrt{D})}$ (see [17, 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 Sect. 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, which we label 'Extended Bröker's algorithm', exactly follows this strategy, setting a lower bound $-4M$ for disc $\mathcal{O}$.

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 (10);
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 imaginary 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 the Generalized Riemann Hypothesis, it is enough to set $M = \tilde{O}\left((\log p)^2\right)$ [42].

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

- $|n|$ is at most $4M$.
- $P_{\mathcal{O}}$ can be computed in $\tilde{O}(\mathrm{disc}(\mathcal{O})) = \tilde{O}(M)$ time.
- a root of $P_{\mathcal{O}}$ in $\mathbb{F}_{p^2}$ can be found in probabilistic time

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

In the light of Theorem 4.1 and since any supersingular elliptic curve is a CM curve, 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 big (a more precise estimate can be found in [41, Prop. A.5]).

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 $\tilde{O}(M^{1/2})$. If we denote by $h(n)$ the class number of the quadratic order of discriminant n, then

$$N = \sum_{\substack{n \in \mathcal{D} \\ -4M \leq n}} h(n) \leq 4M \cdot \tilde{O}(M^{1/2}) = \tilde{O}(M^{3/2}), \tag{11}$$

where $\mathcal{D}$ is defined as in (10). □

For N to be (close to) the total number of supersingular j-invariants over $\mathbb{F}_{p^2}$, which is about $p/12$ (see Corollary 5.4 and [61, Cor. 4.40]), the previous proposition rules that the value of M must be $\tilde{O}(p^{2/3})$. In that case, the output distribution of Algorithm 3 is close to uniform over the set of all supersingular j-invariants over $\mathbb{F}_{p^2}$, but the running time of the algorithm is exponential—namely, it is $\tilde{O}(p^{1/3})$.

4.2.3 Endomorphisms of small degree

For values of M that make Algorithm 3 efficient, the output supersingular elliptic curves are not suitable for cryptographic applications, as we formally prove in the following proposition. Informally, the reason is related to the location of these curves within $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$. Specifically, each output curve is associated with some (small) discriminant $d = d_{\mathbb{Q}(\sqrt{D})}$, where $\mathbb{Q}(\sqrt{D})$ is the field in which the smallest non-scalar endomorphism of the curve embeds. It is shown in [41, Thm. 1.3] that curves associated with the same d are very close to each other in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$—forming a sort of cluster—while curves associated with distinct discriminants are relatively far apart, though connected by efficiently computable isogenies. Therefore, if M is chosen such that Algorithm 3 is efficient, output curves distribute uniformly over a subset of all possible clusters.

Proposition 4.14 *If E is an output of Algorithm 3 (on input M polynomial in* $\log p$*), then* $\mathrm{End}(E)$ *can be computed efficiently.*

Proof The statement is remarked in [41, p. 1], but here we provide a more explicit explanation. Following [41], we say that a curve is M-*small* if it has a non-scalar endomorphism of degree at most M. Let $\mathcal{O}$ be the quadratic order selected at the end of the while loop in Algorithm 3, and E be an elliptic curve over $\mathbb{F}_{p^2}$ whose j-invariant is the output of the algorithm.

A copy of $\mathcal{O}$ is embedded in $\mathrm{End}(E)$. To prove this, we recall from Sect. 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 injective ring homomorphism [54, Prop. 4.4]. Therefore, $\mathcal{O}$ is embedded in $\mathrm{End}(E)$.

In particular, E is M-small [41, Prop. 2.4], i.e. $\mathrm{End}(E)$ contains a non-scalar endomorphism of degree $|\mathrm{disc}\, \mathcal{O}| \leq M$, 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 $\log p$.

In fact, the whole structure of $\mathrm{End}(E)$ can be computed as follows:

1) Depending on p, consider a 'special' order as in [30, Prop. 1]. By [30, 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 the Generalized Riemann Hypothesis, E_0 is $O(\log^2 p)$-small.

2) [41, § 7] shows that isogenies of power-smooth degree between M-small curves can be computed in polynomial time in $\log p$. 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. □

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 $\log p$ (so that the running time is polynomial, too).

The only known algorithm for (almost) uniformly sampling over the set of all supersingular j-invariants over $\mathbb{F}_{p^2}$ [59, p. 71] is constructed according to the strategy described in Remark 3.2. In particular, it performs a random walk in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ (for some small prime $\ell \neq p$) starting from an output of Algorithm 3. This algorithm, though, does not solve the cSRS problem, as we are going to show in Sect. 4.3.2.

Remark 4.15 For some special cases, Bröker's algorithm is not strictly necessary in order to determine a random-walk starting point. In fact, it is well known that an elliptic curve E—over a quadratic finite field $\mathbb{F}_{p^2}$—of j-invariant 0 or 1728 is supersingular if and only if $p \equiv 2 \pmod 3$ or $p \equiv 3 \pmod 4$, respectively (see Sect. 5.1).

4.3.1 Almost uniform output

Theorem 2.14 shows that, 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 $\log_\ell p$ steps in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ with almost uniform distribution. Thus, the combination of the (extended) Bröker's algorithm and non-backtracking random walks solves the SRS problem. This strategy is employed, for example, in SQIsignHD [22], where a random walk in $\mathcal{G}_\ell(\overline{\mathbb{F}_p})$ of prescribed length is executed in order to ensure the uniformity of the commitment curve [22, Prop. 29].

In addition, an analogous of this approach is practically used for SQIsign2D-West [5]. There, the prover generates a random secret isogeny $\varphi_{\mathsf{com}} : E_0 \to E_{\mathsf{com}}$, where E_0 is a supersingular elliptic curve—over a given quadratic finite field $\mathbb{F}_{p^2}$—of known endomorphism ring $\mathrm{End}(E_0)$ and such that it has smooth torsion defined over a small extension of $\mathbb{F}_{p^2}$. The prime p is chosen so that $\log_2 p \approx 2\lambda$, where λ is the security parameter. The random isogeny is obtained by means of an algorithm, called $\mathsf{RandomFixedNormIdeal}$, which samples left ideals of $\mathrm{End}(E_0)$ of fixed norm N with a uniform distribution [5, Alg. 4]. The norm N is of the form ℓ^h for some prime number ℓ and $h > 0$. Here we note that ℓ is not a constant, but $\ell \in O(\sqrt{p})$. The sampled ideal is then turned into an isogeny (see [5, Alg. 3]) whose image is at statistical distance $\tilde{O}(2^{-\lambda})$ from a uniformly random supersingular elliptic curve if $N \geq 2^{4\lambda}$ [5, Lemma 20].

4.3.2 Non-minimal output

Unfortunately, combining the (extended) Bröker's algorithm with random walks does not solve the cSRS problem. This is a corollary of Proposition 4.14.

Corollary 4.16 *Let* A *be the algorithm that performs random walks starting from an output of Algorithm 3 (on input M polynomial in* $\log p$*). Then* $\textsc{EndRing}_{\mathsf{A}}$ *can be solved in polynomial time in* $\log p$*. In particular,* A *is not a supersingular random crypto sampler.*

Proof The argument is the same as in Remark 3.4: 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 this section we will also explain why the computational cost of these two methods is exponential in $\log p$.

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 [50, § 3] and checks if it equals 1 modulo p (in the light of Theorem 2.5.d). Therefore, it is natural to ask if an 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 review 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 negligible:

Theorem 4.17 *There are $O(\sqrt{p}\log p)$ supersingular j-invariants over $\mathbb{F}_p$.*

Proof See [28, 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 a solution for the cSRS problem.

4.4.2 Hasse invariant

Let $\mathbb{F}_q$ be a finite field of odd characteristic p. Hasse [37] defines a polynomial $A_q \in \mathbb{F}_q[g_2, g_3]$, such that $A_q(\tilde{g}_2, \tilde{g}_3) = 0$ if and only if the elliptic curve over $\mathbb{F}_q$ of equation

$$y^2 = 4x^3 - \tilde{g}_2 x - \tilde{g}_3$$

is supersingular. Below, we generalize Hasse's characterisation of supersingular elliptic curves to other models of elliptic curves.

Consider an elliptic curve E over $\mathbb{F}_q$ given by an equation

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

where $f(x)$ is a 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* of E.

The case in which $f(x)$ has degree 3 is considered in [53, Thm. V.4.1.a]. For use in Sect. 5, we prove here an extension of that case to the polynomials f in Table 1.

Theorem 4.18 *Consider a finite field $\mathbb{F}_q$ of odd 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. [7, § 3] shows that the points of E are in one-to-one correspondence with non-zero triplets $(X : Y : Z)_{[1,2,1]}$ which satisfy

$$Y^2 = \epsilon X^4 - 2\delta X^2 Z^2 + Z^4, \tag{12}$$

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

$$(X : Y : Z) = (X' : Y' : Z') \qquad \iff \qquad \exists\, k \in \overline{\mathbb{F}_p}^* \text{ such that } \begin{cases} X' = kX, \\ Y' = k^2 Y, \\ Z' = kZ. \end{cases} \tag{13}$$

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 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

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

The 'points at infinity' of E, on the other hand, are triplets $(X : Y : 0)$ satisfying (12). 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,

$$\#E(\mathbb{F}_q) = 1 + \chi(\epsilon) + q + \sum_{x \in \mathbb{F}_q} \chi\big(f(x)\big). \tag{14}$$

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, (14) becomes

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

We stress that, *a priori*, this is an equality in $\mathbb{F}_q$. However, if we represent equivalence classes modulo p by integers in $\{-(p-1)/2, \ldots, (p-1)/2\}$, then $\epsilon^{\frac{q-1}{2}}, (f(x))^{\frac{q-1}{2}} \in \{-1, 0, 1\}$ and the above equation holds in $\mathbb{Z}$.

Furthermore, one can prove the following equality [61, Lem. 4.35] for every $i \in \mathbb{N}$:

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

As a consequence, since $f(x)$ has degree 4, the only non-zero terms in $\sum_{x \in \mathbb{F}_q} f(x)^{(q-1)/2}$ are (up to the 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 $x^{2(q-1)}$ 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 [53, Theorem V.2.3.1] we know that

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

where a is the trace of the q-th power Frobenius endomorphism. By Theorem 2.5.d we can therefore conclude

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

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 [61, Lemma 4.36]). □

The explicit formula for the Hasse invariant of a generic elliptic curve in Legendre form is a classical result. Seen as a polynomial in the variable λ, the Hasse invariant can be exploited to find supersingular elliptic curves by determining its roots.

Proposition 4.19 *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 [24, p. 201];[61, Thm. 4.34];[53, Thm. V.4.1.b]. □

As a polynomial in the variable λ, A_p has the following coefficients (considered modulo p)[2]

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

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

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

In particular, since no coefficient is zero, A_p is far from being sparse and therefore very impractical to store. In terms of computational complexity, computing the zeroes of A_p appears to be worse than an exhaustive search of supersingular j-invariants over $\mathbb{F}_{p^2}$ (described in Sect. 4.4.1). We will say more on this subject in Sect. 5.

5 Hasse invariant of other models of elliptic curves

It is natural to wonder whether the Hasse invariant for a generic elliptic curve in a model other than the Legendre one can lead to a sparser polynomial for which computing roots is *efficient*.

In this section, the Hasse invariant A_p (defined in Sect. 4.4.2) is explicitly computed for a generic elliptic curve in Weierstrass, Montgomery and Jacobi form. Namely, for each model we construct A_p as a (bivariate or univariate) 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 Sect. 4.4.2, i.e.

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

where $p \geq 5$ is a prime.

5.1 Weierstrass model

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 for a generic curve in this family can be regarded as a polynomial in $\mathbb{F}_q[A, B]$.

Proposition 5.1 *The Hasse invariant of an elliptic curve $E\colon y^2 = x^3 + Ax + B$, over $\mathbb{F}_q$ and in Weierstrass form, is*

$$A_p = \sum_{i=\left\lceil \frac{p-1}{4} \right\rceil}^{\left\lfloor \frac{p-1}{3} \right\rfloor} \binom{m}{i}\binom{m-i}{2m-3i} A^{2m-3i} B^{2i-m}. \tag{15}$$

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

Proof Write

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

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

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

□

The same result can be found also in [11, Lem. 8].

In order to find supersingular elliptic curves over $\mathbb{F}_{p^2}$, we wonder which values of $A, B \in \mathbb{F}_{p^2}$ are roots of A_p. The cases $A=0$ or $B=0$ yield elliptic curves with j-invariant 0 or 1728, for which the following result holds [53, Thm. V.4.1.c];[61, Prop. 3.37, Cor. 4.40]:

$$\begin{aligned}E \text{ with } j\text{-invariant 0 is supersingular} &\iff p\equiv 2 \mod 3,\\ E \text{ with } j\text{-invariant 1728 is supersingular} &\iff p\equiv 3 \mod 4.\end{aligned}$$

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:

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

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

$$\sum_{i=\left\lceil \frac{p-1}{4}\right\rceil}^{\left\lfloor \frac{p-1}{3}\right\rfloor}\binom{m}{i}\binom{m-i}{2m-3i}g^{i(2\ell-3k)}. \tag{16}$$

Notice that (16) 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*

$$2L - 3K \equiv C \mod p^n - 1 \tag{17}$$

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

Proof Observe that

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

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

  are distinct solutions of (17);
- if $k \not\equiv C \mod 2$, there is no $\ell \in \mathbb{Z}/(p^n-1)\mathbb{Z}$ such that (k, ℓ) satisfies equation (17).

Therefore, equation (17) has

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

solutions. □

The zeroes of (16), seen as a polynomial over $\mathbb{F}_p$ in the variable $g^{2\ell-3k}$, correspond to the supersingular j-invariants over $\mathbb{F}_{p^2}$ 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 g^C is a root of*

$$G(X) = \sum_{i=\left\lceil \frac{p-1}{4} \right\rceil}^{\left\lfloor \frac{p-1}{3} \right\rfloor} \binom{m}{i}\binom{m-i}{2m-3i} X^i \in \mathbb{F}_p[X]. \tag{18}$$

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 elliptic curves over $\mathbb{F}_{p^2}$ and isomorphic to E' are exactly the curves of the form $y^2 = x^3 + Ax + B$ where

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

with

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

Proof Let E be a curve over $\mathbb{F}_{p^2}$ and isomorphic to E' (over $\overline{\mathbb{F}_p}$). Therefore the coefficients of E must satisfy

$$A = u^2 A', \qquad B = u^3 B' \tag{19}$$

for some $u \in \mathbb{F}_{p^2}^*$ [53, p. 45]. Notice that there are exactly $p^2 - 1$ such curves. In terms of a given generator g of $\mathbb{F}_{p^2}^*$, we have

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

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 in $\mathbb{F}_{p^2}^*$, we have $p^2 - 1$ distinct solutions for the equation in L and K

$$2L - 3K \equiv C \mod (p^2 - 1). \tag{20}$$

Lemma 5.2 ensures that there is no other solution. □

Corollary 5.4 *Let $G(X)$ be the polynomial defined in (18). The non-zero roots of $G(X)$ are in bijection with the supersingular j-invariants in $\mathbb{F}_{p^2} \setminus \{0, 1728\}$.*

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 elliptic 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

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

Therefore the correspondence

$$\begin{array}{ccc} \{\text{non-zero roots of } G(X)\} & \leftrightarrow & \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2} \setminus \{0, 1728\}\} \\ g^C & \mapsto & \dfrac{1728 \cdot 4}{4 + 27g^C} \\ \dfrac{64 \cdot 4}{j} - \dfrac{4}{27} & \mapsfrom & j \end{array} \tag{21}$$

is one-to-one. □

Let

$$c_i = \binom{m}{i}\binom{m - i}{2m - 3i}$$

be the coefficients of $G(X)$ (equation (18)), for $i \in \left\{\left\lceil \frac{p-1}{4} \right\rceil, \dots, \left\lfloor \frac{p-1}{3} \right\rfloor\right\}$. We have:

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

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

$$c_{i+1} = -12 \cdot \frac{(3i+1)(3i+2)}{(4i+3)(4i+5)} \cdot c_i. \tag{22}$$

With the eventual exception of $c_{\lfloor \frac{p-1}{3} \rfloor}$, p does not appear within the factors of any c_i, and hence every coefficient of $G(X)$ is different from 0. This implies that obtaining $G(X)$ requires exponential storage in $\log p$.

5.2 Montgomery model

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 of a generic curve in this family can be regarded as a polynomial in $\mathbb{F}_q[A, B]$.

We note that the zeroes of A_p do not depend on B, which is in accordance

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 $E\colon y^2 = x^3 + Ax^2 + x$, over $\mathbb{F}_q$ and in Montgomery form, is*

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

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

$$\begin{aligned}(x^3 + Ax^2 + x)^m &= x^m (x^2 + Ax + 1)^m \\ &= x^m \cdot \sum_{i=0}^{m} \binom{m}{i} x^{2i} (Ax+1)^{m-i} \\ &= x^m \cdot \sum_{i=0}^{m} \binom{m}{i} x^{2i} \left(\sum_{j=0}^{m-i} \binom{m-i}{j} A^j x^j \right).\end{aligned}$$

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 $c_0 = 1$ is 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 is a zero of A_p, also $-A$ is. This is, again, in accordance with the fact that j-invariants (and then 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 definition of the j-invariant for 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 [61, 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 a. Then one of its twists has trace $-a$.*

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

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

and consider the curve

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

From [53, p. 45] we know that

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

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 a' be the trace of E'. By [53, Rem. V.2.6] and [38, Prop. 13.1.10] we have

$$\#E(\mathbb{F}_{p^2}) = 1 + p^2 - a, \quad \#E'(\mathbb{F}_{p^2}) = 1 + p^2 - a', \quad \#E(\mathbb{F}_{p^2}) + \#E'(\mathbb{F}_{p^2}) = 2p^2 + 2.$$

The conclusion 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*, and denote by E' its quadratic twist. Then either $E[4] \subseteq E(\mathbb{F}_{p^2})$ or $E'[4] \subseteq E'(\mathbb{F}_{p^2})$.*

Proof It is well-known [53, 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 $p^2 + 1 - a$, where

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

Furthermore, $a \in \{0, \pm p\}$ if and only if $j(E) \in \{0, 1728\}$ [1, 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 [51, Lemma 4.8.ii] we know the structure of the $\mathbb{F}_{p^2}$-rational groups of the two curves:

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

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 [53, 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 [53, 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 isomorphic 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 $s \in \mathbb{F}_q^*$,

and the coefficients of E are

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

Proof See [46, Prop. 4.1, 7.5]. □

Proposition 5.10 *The Hasse invariant A_p for a generic elliptic curve over $\mathbb{F}_q$ in Montgomery form splits completely over $\mathbb{F}_{p^2}$. Equivalently, the coefficient A of any 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 an elliptic curve in Montgomery form $E\colon\ By^2 = x^3 + Ax^2 + x$ 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 an elliptic curve representative of supersingular j-invariant $j' \in \mathbb{F}_{p^2} \setminus \{0, 1728\}$. 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. In particular, it has the 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

$$B' = -\alpha_i^3 - A'\alpha_i \tag{23}$$

for every $i \in \{1, 2, 3\}$. Such relation can be used to factor the fourth division polynomial ψ_4 (see Sect. 6.1) as follows:

$$\begin{aligned}\psi_4/2y &= 2x^6 + 10A'x^4 + 40B'x^3 - 10(A')^2x^2 - 8A'B'x - 2(A')^3 - 16(B')^2 \\ &= 2x^6 - 40x^3\alpha_i^3 - 16\alpha_i^6 + 10A'x^4 - 40A'x^3\alpha_i + \\ &\quad + 8A'x\alpha_i^3 - 32A'\alpha_i^4 - 10(A')^2x^2 + 8(A')^2x\alpha_i - 16(A')^2\alpha_i^2 - 2(A')^3 \\ &= -2(-x^2 + 2x\alpha_i + 2\alpha_i^2 + A')(x^4 + 2x^3\alpha_i + 6x^2\alpha_i^2 - 4x\alpha_i^3 + \\ &\quad + 4\alpha_i^4 + 6A'x^2 - 6A'x\alpha_i + 6A'\alpha_i^2 + (A')^2).\end{aligned} \tag{24}$$

Since ψ_4 vanishes exactly on the x-coordinates of the 4-torsion points (see Proposition 6.5), for each i there exist two distinct values x_i and x_i' in $\mathbb{F}_{p^2}$ such that the first factor of (24) is zero, i.e.

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

or, equivalently, satisfy

$$A' + 3\alpha_i^2 = (x - \alpha_i)^2. \tag{25}$$

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 isomorphic to elliptic curves, over $\mathbb{F}_{p^2}$ and in Montgomery form, 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 (25) 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 (23) implies $\alpha_i \neq -\alpha_j$.

To summarize, starting from a suitable supersingular elliptic curve in Weierstrass form with j-invariant $j' \in \mathbb{F}_{p^2} \setminus \{0, 1728\}$, 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 could not be any other solution, the coefficient of x^2 of an elliptic curve in Montgomery form with j-invariant j' must belong to the set $\{\pm A_i \mid i = 1, 2, 3\}$, which is contained 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 of a generic curve in the family can be regarded as a polynomial in $\mathbb{F}_q[\epsilon, \delta]$.

Proposition 5.11 *The Hasse invariant of an elliptic curve $E\colon\ y^2 = \epsilon x^4 - 2\delta x^2 + 1$, over $\mathbb{F}_q$ and 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 a generic elliptic curve in different models, in the form of a polynomial. 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 (extended) Bröker's algorithm and random walks, as described in Sect. 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 formulas 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 torsion points.

6.1 Division polynomials

Following [53, ex. 3.7];[61, § 3.2], we introduce division polynomials, which constitute the main tool for the two characterisations. Let

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

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

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

$$\psi_{2n} = \frac{\psi_{n-1}^2\psi_n\psi_{n+2} - \psi_{n-2}\psi_n\psi_{n+1}^2}{\psi_2} \qquad \text{for } n \geq 3. \tag{27}$$

For ease of notation, for $m \geq 1$ we also define

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

for $m \geq 1$.

We now review some well-known results about division polynomials, which can be proven by induction (see [61, 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 $K[x, \psi_2^2]$; 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

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

Proposition 6.3 *Consider ϕ_m and ψ_m^2 as elements in $K[x]$. 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:*

$$[m]P = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right) \tag{28}$$

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 and ω_m the evaluations $\phi_m(x_0, y_0)$, $\psi_m(x_0, y_0)$ and $\omega_m(x_0, y_0)$, respectively.

Proof See [61, 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*

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

Proof See [19, Prop. 9.10]. □

6.2 *p*-torsion points

Theorem 2.5 ensures that an elliptic curve E over a field of characteristic p is supersingular if and only if $E[p^r] = \{O\}$ for some $r \geq 1$. As in Sect. 4.4.2 and Sect. 5, in this section we construct a polynomial whose zeroes are exactly the pairs of coefficients A and B defining supersingular elliptic curves in Weierstrass form. In this case, though, the *coefficients* of the considered polynomial lie in a much larger 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.(a1) 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 $\psi_{p^r}(x)$ is constant for some $r \geq 1$.*

A refinement of the above result, which we state below in a more general fashion, is given in [29, Lem. 4].

Proposition 6.7 *Let $E\colon y^2 = x^3 + Ax + B$ be a elliptic curve over $\mathbb{F}_{p^2}$. Then E is supersingular if and only if 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 $\mathbb{F}_p[x]$.

Proof Suppose that E is supersingular (the other implication is a trivial consequence of Proposition 6.6). Doliskani's proof covers the case $\operatorname{tr}(E) = \pm 2p$, but it can be easily extended to the other cases, as follows. The characteristic polynomial of the Frobenius endomorphism φ_{p^2} of a supersingular elliptic 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 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

$$[p^3](x, y) = \left(x^{p^6}, y^{p^6}\right) \tag{29}$$

for every $(x, y) \in E$, while from equation (28) and Proposition 6.3 we obtain

$$[p^3](x, y) = \left(\frac{\phi_{p^3}}{\psi_{p^3}^2}, \frac{\omega_{p^3}}{\psi_{p^3}^3}\right) = \left(\frac{x^{p^6} + \text{terms of lower degree}}{p^6 x^{p^6-1} + \text{terms of lower degree}}, \frac{\omega_{p^3}}{\psi_{p^3}^3}\right). \tag{30}$$

Comparing the first coordinates on the right-hand sides of (29) and (30) 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:

- consider ψ_p for a generic elliptic curve over a field of characteristic p, i.e. $\psi_p \in \mathbb{F}_p[A, B, x]$;
- find pairs (A, B) such that $\psi_p^2 - 1$ is zero. Such pairs are coefficients of supersingular elliptic curves.

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 $J = (A + B + 1, A^{p-1} - 1)$. The second assumption is without loss of generality since every $\mathbb{F}_{p^2}$-isomorphism class of supersingular elliptic 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 elliptic curve of equation $y^2 = x^3 - x$ has j-invariant 1728 and passes through $(1, 0)$. Assume $j \neq 1728$ and let $E\colon y^2 = x^3 + A'x + B'$ be an elliptic curve, over $\mathbb{F}_p$ and in Weierstrass form, of j-invariant j (it is by Proposition 2.1.b that we can assume E is defined over $\mathbb{F}_p$). Combining Theorem 2.5.d and Hasse's inequality

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

(see [61, Thm. 4.2]), we know that any supersingular curve over $\mathbb{F}_p$ has exactly $p+1$ rational points; in particular,

$\#E(\mathbb{F}_p)$ is even. Therefore, as O is one of the rational points, and every 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 E.

Since $j \neq 1728$, x_0 must be non-zero. Let $u \in \mathbb{F}_{p^2}^*$ be a square root of ${x_0}^{-1}$. Then [53, p. 45] the curve defined by the coefficients

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

is isomorphic over $\mathbb{F}_{p^2}$ to E and passes through $(1, 0)$ because we have

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

□

As Wouter Castryck pointed out to us, since each coefficient of $\psi_p^2 - 1$ (viewed as a polynomial in x) must be zero for a pair (A, B) to yield a supersingular elliptic curve, every such coefficient is in fact a multiple of the Hasse invariant computed in Sect. 5.1. Even more was proven in [23]: the coefficient of $x^{p(p-1)/2}$ in ψ_p is *equal* to the Hasse invariant. Therefore, there is no hope that working with $\psi_p^2 - 1$ can be more efficient than considering the Hasse invariant from Sect. 5.

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*

$$\prod_{i=1}^{r} \ell_i > 2\sqrt{p}, \tag{31}$$

and denote by r' the minimum integer in $\{1, \ldots, r\}$ satisfying (31). An elliptic curve $E : y^2 = x^3 + Ax + B$, over $\mathbb{F}_p$ and in Weierstrass form, is supersingular if and only if the division polynomial $\psi_{\ell_i}(x, y)$ relative to E has a root $(x_i, y_i) \in E(\mathbb{F}_p)$ for each $i \in \{1, \ldots, r'\}$.

Proof Suppose that E is supersingular.

As observed in the proof of Proposition 6.8,

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) of E. Such point is a zero for ψ_{ℓ_i} by Proposition 6.5.

For the converse, the bound (31) is needed. Suppose that there exists an $\mathbb{F}_p$-rational ℓ_i-torsion point of E, and then ℓ_i divides $\#E(\mathbb{F}_p)$, for each $i \in \{1, \ldots, r'\}$.

Equivalently, by the Chinese Remainder Theorem,

$$\#E(\mathbb{F}_p) \equiv 0 \mod \prod_{i=1}^{r} \ell_i. \tag{32}$$

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

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}. \tag{33}$$

Since $\prod_{i=1}^{r'} \ell_i > 2\sqrt{p}$, it is easy to check that the only way for (32) and (33) to both hold is for $\#E(\mathbb{F}_p) = p + 1$. Therefore, E is supersingular by Theorem 2.5.d. □

Remark 6.10 Some of the primes used in cryptographic applications do satisfy the hypotheses of Proposition 6.9. For example, the prime p in CSIDH-512 [12, § 8.1] is $p = 4 \cdot 587 \cdot \ell_1 \cdots \ell_{73} - 1$ where $\ell_1, \dots, \ell_{73}$ are the first 73 odd primes.

The characterisation of supersingular elliptic curves given by Proposition 6.9 provides a method to sample supersingular elliptic curves. In particular, given a prime $p = \prod_{i=1}^{r} \ell_i^{e_i} - 1$ such that (31) is satisfied for some (minimal) $r' \leq r$, then any solution of the system of equations

$$\begin{cases} \psi_{\ell_i}(A, B, x_i, y_i) = 0 & \text{for each } i \in \{1, \dots r'\} \\ y_i^2 - x_i^3 - Ax_i - B = 0 & \text{for each } i \in \{1, \dots r'\} \\ x_i^p - x_i = 0 & \text{for each } i \in \{1, \dots r'\} \\ y_i^p - y_i = 0 & \text{for each } i \in \{1, \dots r'\} \\ A^p - A = 0 \\ B^p - B = 0 \end{cases} \tag{34}$$

yields the coefficients A, B 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 $i \in \{1, \dots, r'\}$.

6.3.1 Efficiency analysis

The polynomials involved in system (34) have either low degree or sparse coefficients. A naive use of Groebner bases or other polynomial-system solvers, though, is far from enough to turn this method into an efficient algorithm to solve the cSRS problem, due to the exponential size of the set of solutions of system (34). We leave any improvement of this technique for future work.

7 Conclusions

We have provided a formalisation for the SRS and cSRS problems, relative to randomly sampling supersingular elliptic curves. We have surveyed a solution to the first and known (non-resolving) approaches to the latter, for which we have also presented some new approaches. 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 of the discussed approaches, will be a useful starting point for future research on the subject.

Acknowledgements The authors are grateful to Wouter Castryck, Sören Kleine and the anonymous referees for their corrections and remarks which helped improve the paper. The second author was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU. The second and third authors acknowledge support from Ripple's University Blockchain Research Initiative. The first and third authors acknowledge support from the INDAM group GNSAGA.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1. Adj, G., Ahmadi, O., Menezes, A.: On isogeny graphs of supersingular elliptic curves over finite fields. Finite Fields Their Appl. **55**, 268–283 (2019)
2. Alon, N., Benjamini, I., Lubetzky, E., Sodin, S.: Non-backtracking random walks mix faster. In: Communications in Contemporary Mathematics 09.04, pp. 585–603 (2007). https://doi.org/10.1142/S0219199707002551
3. Basso, A., et al.: Supersingular curves you can trust. In: Advances in Cryptology—EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23–27, 2023, Proceedings, Part II, pp. 405–437. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-30617-4_14
4. Basso, A., et al.: Exploring SIDH-based signature parameters. In: Christina Pöpper, L.B. (eds.) International Conference on Applied Cryptography and Network Security (ACNS) 2024. Lecture Notes in Computer Science, pp. 432–456. Springer Nature Switzerland, Cham (2024)
5. Basso, A., et al.: SQIsign2D-west the fast, the small, and the safer. Cryptology ePrint Archive, Report 2024/760. https://eprint.iacr.org/2024/760 (2024)
6. Burdges, J., De Feo, L.: Delay encryption. In: Canteaut, A., Standaert, F.-X. (eds.) Advances in Cryptology—EUROCRYPT 2021, pp. 302–326. Springer International Publishing, Cham (2021)
7. Billet, O., Joye, M.: 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, pp. 34–42 (2003)
8. Boneh, D., Bonneau, J., Bünz, B., Fisch, B.: Verifiable delay functions. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology—CRYPTO 2018, pp. 757–788. Springer International Publishing, Cham (2018)
9. Booher, J., et al.: Failing to hash into supersingular isogeny graphs. Cryptology ePrint Archive, Paper 2022/518. https://eprint.iacr.org/2022/518 (2022)
10. Bröker, R.: Constructing supersingular elliptic curves. J. Comb. Number Theory **1**(3), 269–273 (2009)
11. Castryck, W., Folsom, A., Hubrechts, H., Sutherland, A.: The probability that the number of points on the Jacobian of a genus 2 curve is prime. In: Proceedings of the London Mathematical Society, vol. 104. https://doi.org/10.1112/plms/pdr063 (2011)
12. Castryck, W., et al.: CSIDH: an efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology—ASIACRYPT 2018, pp. 395–427. Springer International Publishing, Cham (2018)
13. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology—EUROCRYPT 2023, pp. 423–447. Springer Nature Switzerland, Cham (2023)
14. Codogni, G., Lido, G.: Spectral theory of isogeny graphs. arxiv: 2308.13913 (2023)
15. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. J. Cryptol. **22**, 93–113 (2009)
16. Cohen, H.: A course in computational algebraic number theory. Graduate Texts in Mathematics. vol. 138. Springer-Verlag, Berlin (1993)
17. Cox, D.A.: Primes of the Form $x^2 + ny^2$. John Wiley & Sons, Ltd (2013)
18. Castryck, W., Panny, L., Vercauteren, F.: Rational isogenies from irrational endomorphisms. In: Canteaut, A., Ishai, Y. (eds) 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, Lecture Notes in Computer Science. vol. 12106, pp. 523–548. Springer (2020)
19. Charlap, L.S., Robbins, D.P.: An elementary introduction to elliptic curves. https://cs.nyu.edu/courses/spring05/G22.3220-001/ec-intro1.pdf (1988)
20. Costello, C., Smith, B.: Montgomery curves and their arithmetic: The case of large characteristic fields. J. Cryptogr. Eng. **8**, 227–240 (2017)

21. Chavez-Saab, J., Rodríguez-Henríquez, F., Tibouchi, M.: Verifiable isogeny walks: towards an isogeny-based postquantum VDF. In: AlTawy, R., Hülsing, A. (eds.) Selected Areas in Cryptography, pp. 441–460. Springer International Publishing, Cham (2022)
22. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQISignHD: new dimensions in cryptography. In: Hazay, C., Stam, M. (eds) Advances in Cryptology—EUROCRYPT 2024, pp. 3–32. Springer Nature Switzerland (2024)
23. Debry, C.: Beyond two criteria for supersingularity: coefficients of division polynomials. In: Journal de Théorie des Nombres de Bordeaux 26.3, pp. 595–605. http://www.jstor.org/stable/43973204 (visited on 03/06/2024) (2014)
24. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **14**(1), 197–272 (1941)
25. De Feo, L., Masson, S., Petit, C., Sanso, A.: Verifiable delay functions from supersingular isogenies and pairings. In: Advances in Cryptology—ASIACRYPT 2019, 25th International Conference on the Theory and Application of Cryptology and Information Security. pp. 248–277 (2019)
26. De Feo, L., et al.: SQISign: compact post-quantum signatures from quaternions and isogenies. In: Advances in Cryptology–ASIACRYPT 2020, Part I, pp. 64–93. Springer International Publishing (2020)
27. De Feo, L., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Math. Cryptol. **8**(3), 209–247 (2014)
28. Delfs, C., Galbraith, S.D.: Computing isogenies between supersingular elliptic curves over F_p. Des. Codes Cryptogr. **78**, 425–440 (2016)
29. Doliskani, J.: On division polynomial PIT and supersingularity. Appl. Algebra Eng. Commun. Comput. **29**(5), 393–407 (2018)
30. Eisenträger, K., et al.: Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In: Nielsen, J.B., Rijmen, V. (eds) Advances in Cryptology—EUROCRYPT 2018, pp. 329–368. Springer International Publishing (2018)
31. Eisenträger, K., et al.: Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs. In: Fourteenth Algorithmic Number Theory Symposium, pp. 215–232 (2020)
32. Enge, A.: The complexity of class polynomial computation via floating point approximations. Math. Comput. **78**, 1089–1107 (2006)
33. Fouotsa, T., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: countering SIDH attacks by masking information. In: Hazay, C. and M. Stam (eds) Advances in Cryptology—EUROCRYPT 2023. Lecture Notes in Computer Science. 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2023; Conference date: 23-04-2023 Through 27-04-2023, pp. 282–309. Springer. https://doi.org/10.1007/978-3-031-30589-4_10 (2023)
34. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Cheon, J.H., Takagi, T. (eds) Advances in Cryptology—ASIACRYPT 2016, pp. 63–91. Springer Berlin Heidelberg (2016)
35. Galbraith, S.D.: Mathematics of public key cryptography. Version 2.0. https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf (2018)
36. Ghantous, W., Pintore, F., Veroni, M.: Efficiency of SIDH-based signatures (yes, SIDH). J. Math. Cryptol. **18**(1), 20230023 (2024)
37. Hasse, H.: Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p. Journal für die reine und angewandte Mathematik **172**, 77–85 (1935)
38. Husemöller, D.: Elliptic Curves, 2nd edn. Graduate Texts in Mathematics, vol. 111. Springer, New York (1987)
39. Kohel, D.: Endomorphism Rings of Elliptic Curves Over Finite Fields. Ph.D. thesis. http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf (1996)
40. Lang, S.: Elliptic Functions. Graduate texts in mathematics. Springer (1987)
41. Love, J., Boneh, D.: Supersingular curves with small non-integer endomorphisms. In: Fourteenth Algorithmic Number Theory Symposium, pp. 7–22 (2020)
42. Lagarias, J., Odlyzko, A.: Effective versions of the chebotarev density theorem. In: Frhlich, A. (ed.) Algebraic Number Fields, L-Functions and Galois Properties, pp. 409–464. Academic Press (1977)
43. Maino, L., et al.: A direct key recovery attack on SIDH. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology—EUROCRYPT 2023, pp. 448–471. Springer Nature Switzerland, Cham (2023)
44. Mokrani, Y., Jao, D.: Generating supersingular elliptic curves over $\mathbb{F}_p$ with unknown endomorphism ring. Cryptology ePrint Archive, Paper 2023/984. https://eprint.iacr.org/2023/984 (2023)
45. Moriya, T.: IS-CUBE: an isogeny-based compact KEM using a boxed SIDH diagram. Cryptology ePrint Archive, Paper 2023/1506. https://eprint.iacr.org/2023/1506 (2023)

46. Okeya, K., Kurumatani, H., Sakurai, K.: Elliptic curves with the montgomery-form and their cryptographic applications. In: Imai, H., Zheng, Y. (eds) Public Key Cryptography, pp. 238–257. Springer Berlin Heidelberg (2000)
47. Pizer, A.K.: Ramanujan graphs. In: Computational perspectives on number theory (Chicago, IL, 1995), pp. 159–178. American Mathematical Society (1998)
48. Page, A., Wesolowski, B.: The supersingular endomorphism ring and one endomorphism problems are equivalent. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 388–417. Springer International Publishing, Cham (2024)
49. Robert, D.: Breaking SIDH in polynomial time. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology—EUROCRYPT 2023, pp. 472–503. Springer Nature Switzerland, Cham (2023)
50. Schoof, R.: Elliptic curves over finite fields and the computation of square roots mod p. Math. Comput. **44**(170), 483–494 (1985)
51. Schoof, R.: Nonsingular plane cubic curves over finite fields. J. Combin. Theory Ser. A **46**(2), 183–211 (1987)
52. Siegel, C.L.: Über die Classenzahl quadratischer Zahlkörper. Acta Arithmetica **1**, 83–86 (1935)
53. Silverman, J.H.: The arithmetic of elliptic curves. Graduate Texts in Mathematics. vol. 151. Springer (2009)
54. Silverman, J.: Advanced topics in the arithmetic of elliptic curves. Springer-Verlag, (1994)
55. Sutherland, A.: Isogeny volcanoes. The Open Book Series **1**(1), 507–530 (2013)
56. Tate, J.: Endomorphisms of abelian varieties over finite fields. Inventiones mathematicae **2**, 134–144 (1966)
57. Terras, A.: Fourier Analysis on Finite Groups and Applications. London Mathematical Society Student Texts, Cambridge University Press (1999)
58. Vélu, J.: Isogénies entre courbes elliptiques. Comptes Rendus de l'Académie des Sciences de Paris **273**, 238–241 (1971)
59. Vitse, V.: Simple oblivious transfer protocols compatible with supersingular isogenies. In: Buchmann, J., Nitaj, A., Rachidi, T. (eds.) Progress in Cryptology—AFRICACRYPT 2019, pp. 56–78. Springer International Publishing, Cham (2019)
60. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra, 3rd edn. Cambridge University Press (2013)
61. Washington, L.C.: Elliptic Curves: Number Theory and Cryptography, 2nd edn. Chapman & Hall/CRC (2008)
62. Wesolowski, B.: 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, 2021, pp. 1100–1111. IEEE (2022)
63. Wesolowski, B.: Orientations and the supersingular endomorphism ring problem. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology—EUROCRYPT 2022, pp. 345–371. Springer International Publishing, Cham (2022)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.