Des. Codes Cryptogr. (2016) 78:425–440
DOI 10.1007/s10623-014-0010-1

Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$

Christina Delfs · Steven D. Galbraith

Received: 24 October 2013/ Revised: 8 September 2014 / Accepted: 9 September 2014 /
Published online: 21 September 2014
© Springer Science+Business Media New York 2014

Abstract Let $p > 3$ be a prime and let E, E' be supersingular elliptic curves over $\mathbb{F}_p$. We want to construct an isogeny $\phi : E \to E'$. The currently fastest algorithm for finding isogenies between supersingular elliptic curves solves this problem in the full supersingular isogeny graph over $\mathbb{F}_{p^2}$. It takes an expected $\tilde{\mathcal{O}}(p^{1/2})$ bit operations, and also $\tilde{\mathcal{O}}(p^{1/2})$ space, by performing a "meet-in-the-middle" breadth-first search in the isogeny graph. In this paper we consider the structure of the isogeny graph of supersingular elliptic curves over $\mathbb{F}_p$. We give an algorithm to construct isogenies between supersingular curves over $\mathbb{F}_p$ that works in $\tilde{\mathcal{O}}(p^{1/4})$ bit operations. We then discuss how this algorithm can be used to obtain an improved algorithm for the general supersingular isogeny problem.

Keywords Elliptic curves · Isogenies · Supersingular curves

Mathematics Subject Classification 11G20 · 11Y16 · 11G15 · 14K02 · 14G15 · 14H52

1 Introduction

The problem of computing an isogeny between two given elliptic curves has been studied by many authors and has several applications [3,6,7,10–13,19]. A natural question that has not previously been considered is to construct isogenies between two given supersingular elliptic curves over $\mathbb{F}_p$.

Communicated by G. Korchmaros.

C. Delfs
Carl von Ossietzky Universität Oldenburg, Oldenburg, Germany
e-mail: christina.delfs@uni-oldenburg.de

S. D. Galbraith (✉)
University of Auckland, Auckland, New Zealand
e-mail: s.galbraith@math.auckland.ac.nz

Let p be a prime, $q := p^n$ for some integer n and let L be a non-empty set of small primes with $p \notin L$. Let K be either $\mathbb{F}_q$ or $\bar{\mathbb{F}}_p$. The *supersingular isogeny graph* $X(K, L)$ is a directed graph where the vertices are K-isomorphism classes of supersingular elliptic curves over K and the edges are equivalence classes of ℓ-isogenies defined over K between such curves for $\ell \in L$. (Two isogenies are equivalent if they have the same kernel.) If we only consider $L = \{\ell\}$, we write $X(K, \ell)$. Usually the vertices are represented by j-invariants.

For various reasons we always assume $p > 3$ in this paper. Note that $X(\bar{\mathbb{F}}_p, L)$ has only one vertex when $p < 11$ and so all the problems we consider are trivial for small p.

If we regard the full supersingular isogeny graph $X(\bar{\mathbb{F}}_p, \ell)$, it suffices to consider elliptic curves defined over $\mathbb{F}_{p^2}$, since the j-invariant of a supersingular elliptic curve always lies in $\mathbb{F}_{p^2}$. In general the isogenies will still be defined over $\bar{\mathbb{F}}_p$ though.

Let S_{p^2} be the set of all supersingular j-invariants in $\mathbb{F}_{p^2}$. It is well-known (e.g. [18, Theorem V.4.1(c)]) that for a prime $p > 3$ we have

$$\#S_{p^2} = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12}, \\ 1 & \text{if } p \equiv 5, 7 \pmod{12}, \\ 2 & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

In contrast to the ordinary case, the graph $X(\bar{\mathbb{F}}_p, \ell)$ has an irregular structure but is always fully connected for every prime ℓ (see [14] or [13, Corollary 78]). Thus we can use a chain of isogenies of small prime degree (i.e. $\ell = 2$) to construct an isogeny between two given supersingular elliptic curves over $\mathbb{F}_{p^2}$. Those isogenies are fast to compute. These graphs are known to be expanders (see [3] for references), so they have small diameter and there is a short path between any two vertices. A natural problem is to find a path between any two vertices in the graph.

A general "meet-in-the-middle" idea for finding paths in graphs (also called "bi-directional search"), was proposed by Pohl [15]. (Indeed, this finds shortest paths.) This idea was used by Galbraith [6] to construct isogenies between elliptic curves, and it is applicable for both ordinary and supersingular curves. The problem is that the algorithm requires large storage, and is not easy to parallelise. In the ordinary case, a low-storage and parallelisable algorithm was proposed by Galbraith et al. [7] and improved by Galbraith and Stolbunov [8]. (These algorithms are no longer guaranteed to find the shortest path.) While some of these ideas can be adapted to get a low-storage parallel algorithm for the supersingular isogeny problem, there are several reasons why the supersingular case is more awkward than the ordinary case: we might wish to use just $L = \{2\}$ and then it is hard to prevent short cycles and walks are "not random enough"; unlike [7] there is no process to "shorten" or "smooth" a long walk. Hence, it has remained an open problem to get a good isogeny algorithm for the supersingular graph $X(\bar{\mathbb{F}}_p, 2)$.

The subgraph of $X(\bar{\mathbb{F}}_p, 2)$ we get through deleting the vertices where the j-invariants are in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ is considerably smaller. For a prime $p > 3$ let S_p be the set of all supersingular j-invariants in $\mathbb{F}_p$. Then

$$\#S_p = \begin{cases} \frac{1}{2}h(-4p) & \text{if } p \equiv 1 \pmod 4 \\ h(-p) & \text{if } p \equiv 7 \pmod 8 \\ 2h(-p) & \text{if } p \equiv 3 \pmod 8 \end{cases} \tag{1}$$

where $h(d)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. This may be proved using a counting argument (see [5, Theorem 14.18]).

Since the class number of an imaginary quadratic field K with discriminant d_K can be bounded as $h_K \leq \frac{1}{\pi}\sqrt{|d_K|}\ln|d_K|$ (see [4, Exercise 5.27]), the size of this set is $\tilde{\mathcal{O}}(\sqrt{p})$, so we expect shorter paths when working in this smaller graph and thus faster algorithms for constructing isogenies. The problem is that in general those graphs are not connected, and hence it is not always possible to obtain an isogeny with degree a power of ℓ between arbitrary supersingular elliptic curves over $\mathbb{F}_p$ without going via elliptic curves over $\mathbb{F}_{p^2}$.

So there are two questions arising about this subgraph:

- How many prime isogeny degrees $\ell \in L$ do we have to allow until the subgraph of supersingular elliptic curves over $\mathbb{F}_p$ is connected?
- Is there an algorithm for computing an isogeny between supersingular elliptic curves over $\mathbb{F}_p$ which is faster than the known algorithms for the full graph $X(\bar{\mathbb{F}}_p, L)$?

We will answer both questions in the course of this work. Section 2 explains the structure of the graph $X(\mathbb{F}_p, L)$. The main observation is that the supersingular case restricted to $\mathbb{F}_p$ closely resembles the ordinary case, and so the known advantages of that situation can be exploited for supersingular curves too. Section 3 presents an algorithm, arising from these considerations, that computes isogenies between supersingular elliptic curves over $\mathbb{F}_p$. Section 4 explains how our methods also lead to a good solution to the general isogeny problem (i.e., in the full graph $X(\bar{\mathbb{F}}_p, L)$). A few toy example graphs over $\bar{\mathbb{F}}_p$ and $\mathbb{F}_p$ are given in the Appendix to illustrate the results of Sect. 2.

2 The structure of supersingular isogeny graphs

We first make some remarks about the relation between $X(\mathbb{F}_p, L)$ and $X(\bar{\mathbb{F}}_p, L)$. Importantly, with our definitions, the former is not a subgraph of the latter.

An ordinary elliptic curve over $\mathbb{F}_p$ is never isogenous to its non-trivial quadratic twist since they have a different number of $\mathbb{F}_p$-rational points, so we never have to care about twists when considering isogenies between ordinary elliptic curves over $\mathbb{F}_p$. If the curves are supersingular though, this is not the case.

Let $p > 3$. A supersingular elliptic curve over $\mathbb{F}_p$ has $p + 1$ points and so all quadratic twists have the same number of points. Thus the twists are isogenous but lie in different $\mathbb{F}_p$-isomorphism classes. Therefore it is not very precise to represent the vertices in the supersingular isogeny graph over $\mathbb{F}_p$ with j-invariants, since then the different isomorphism classes collapse to only one vertex and the picture of in- and outgoing isogenies is distorted. So if we want to differentiate between twists, we have to store more information than just the j-invariants of the elliptic curves, for instance the quantities $c_4(E)$, $c_6(E)$ in addition to $j(E)$. We will see that we have twice the number of vertices in $X(\mathbb{F}_p, L)$ as in $X(\bar{\mathbb{F}}_p, L) \cap \mathbb{F}_p$.

In this situation it is no longer possible to compute the neighbours of a given vertex using only the modular polynomial, since this only produces the j-invariant of the image curve and does not keep track of twists. Instead we use the formulae of Vélu [21] to compute the image curve under an isogeny whose kernel is a Galois-invariant subgroup G of E with order ℓ. These subgroups can be constructed from factors of the ℓ^{th} division polynomial or using a basis of $E[\ell]$. This method was used to construct the graphs in the Appendix.

If we construct the supersingular ℓ-isogeny graph over $\mathbb{F}_p$ regarding these considerations, a much more regular structure appears as demonstrated in the Appendix for some examples with small p and ℓ. On closer examination the graphs $X(\mathbb{F}_p, \ell)$ resemble the "volcano"-structure of the ordinary case, only that here we have mostly "craters", that is, isogeny-circles. We want to describe now why this structure appears.

As in the ordinary case, the properties of isogenies between supersingular elliptic curves over $\mathbb{F}_p$ are closely related to the structure of their endomorphism rings. We define $\mathrm{End}_{\mathbb{F}_q} E$ to be the ring of endomorphisms of E that are defined over $\mathbb{F}_q$. In general we know that the endomorphism ring of an elliptic curve over $\mathbb{F}_q$ is an order in a division algebra $\mathcal{A} := \mathrm{End}_{\mathbb{F}_q} E \otimes_{\mathbb{Z}} \mathbb{Q}$. Depending on the number of $\mathbb{F}_q$-rational points there are some more precise results about this as can be seen in the next theorem (see [22] or [16]).

Theorem 2.1 *Let $p > 3$, $q = p^n$ and E be a supersingular elliptic curve over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$ where and $|t| \leq 2\sqrt{q}$. Then one of the following cases must be true:*

(1) n is even and $t = \pm 2\sqrt{q}$,
(2) n is even, $p \not\equiv 1 \pmod 3$ and $t = \pm\sqrt{q}$,
(3) n is even and $p \not\equiv 1 \pmod 4$ and $t = 0$,
(4) n is odd and $t = 0$,

In this situation the corresponding division algebra $\mathcal{A}$ is also determined by the cases. Let π_q be the q-th power Frobenius endomorphism.

In the first case $\mathcal{A}$ is a quaternion algebra over $\mathbb{Q}$, π_q is a rational integer and $\mathrm{End}_{\mathbb{F}_q} E$ is a maximal order in $\mathcal{A}$.

In the other three cases $\mathcal{A} = \mathbb{Q}(\pi_q)$ is an imaginary quadratic field over $\mathbb{Q}$ and $\mathrm{End}_{\mathbb{F}_q} E$ is an order in $\mathcal{A}$ with conductor prime to p.

Now, if we take a supersingular elliptic curve E over $\mathbb{F}_p$ with $p > 3$, we end up in Case 4 of Theorem 2.1. Thus we know according to the theorem that $\mathrm{End}_{\mathbb{F}_p} E$ is an order in $K := \mathbb{Q}(\pi_p)$ and its conductor is prime to p. Since $\pi_p^2 + p = 0$ holds, we get $K = \mathbb{Q}(\sqrt{-p})$. Furthermore

$$\mathbb{Z}\left[\pi_p\right] = \mathbb{Z}\left[\sqrt{-p}\right] = \mathbb{Z}\left[\frac{d+\sqrt{d}}{2}\right] \subseteq \mathrm{End}_{\mathbb{F}_p} E \subseteq \mathbb{Z}\left[\frac{d_K+\sqrt{d_K}}{2}\right] = \mathcal{O}_K$$

has to hold where $d = -4p$, $\mathcal{O}_K$ is the maximal order and d_K the fundamental discriminant of K. Due to the properties of the fundamental discriminant, we have $d = c^2 \cdot d_K$ where $c \in \mathbb{N}$ is maximal such that $d_K \equiv 0, 1 \pmod 4$ and is called the *conductor of* $\mathbb{Z}[\pi_p]$ *in* $\mathcal{O}_K$. From these observations we can conclude:

- If $p \equiv 1 \pmod 4$, we always get $d_K = d = -4p$, $\mathbb{Z}[\pi_p] = \mathcal{O}_K$ and hence $\mathrm{End}_{\mathbb{F}_p} E = \mathbb{Z}\left[\sqrt{-p}\right]$ for a supersingular elliptic curve E over $\mathbb{F}_p$.
- If $p \equiv 3 \pmod 4$, we get $d_K = -p$. Thus $\mathbb{Z}[\pi_p] = \mathbb{Z}\left[\sqrt{-p}\right]$ has conductor $c = 2$ in $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\mathrm{End}_{\mathbb{F}_p} E$ must be one of those two orders.

In terms of isogeny-volcanoes we can say that we have at most two levels. We will use the following terminology.

Definition Let E be a supersingular elliptic curve over $\mathbb{F}_p$. We say E *is on the surface* (resp. E *is on the floor*) if $\mathrm{End}_{\mathbb{F}_p} E = \mathcal{O}_K$ (resp. $\mathrm{End}_{\mathbb{F}_p} E = \mathbb{Z}[\sqrt{-p}]$). Note that for $p \equiv 1 \pmod 4$ surface and floor coincide.

Let ϕ be an ℓ-isogeny between supersingular elliptic curves E and E' over $\mathbb{F}_p$. If $\mathrm{End}_{\mathbb{F}_p} E \cong \mathrm{End}_{\mathbb{F}_p} E'$, then ϕ is called *horizontal*. If E is on the floor and E' is on the surface (resp. E on the surface and E' on the floor), ϕ is called *ℓ-isogeny up* (resp. *down*).

In the supersingular case there are fewer possibilities for ℓ-isogenies up and down than for ordinary volcanoes (though, even in the ordinary case tall volcanoes are quite rare). This is due to the fact that for an isogeny $\phi : E \to E'$ with $[\mathrm{End}\, E : \mathrm{End}\, E'] = \ell$ we have $\ell \mid \deg \phi$ (see [13, Propositions 21 and 22]). Since in our case $[\mathrm{End}\, E : \mathrm{End}\, E'] \in \{1, 2\}$ (resp. $[\mathrm{End}\, E' : \mathrm{End}\, E] \in \{1, 2\}$) we get the following statement.

Lemma 2.2 *Let ϕ be a non-horizontal isogeny between supersingular elliptic curves over $\mathbb{F}_p$. Then the degree of ϕ is divisible by* 2.

Therefore we have no isogenies of odd prime degree going up or down in this graph.

To determine how many isogenies there are we need some theory about the ideal class group. We recall the relevant background below.

First we can make an observation about the number of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ with a given j-invariant, based on the following proposition which follows directly from [2, Theorem 2.2].

Proposition 2.3 *Let $p > 3$ be a prime and $j \in \mathbb{F}_p$. Define $C_{p,j}$ as the set of $\mathbb{F}_p$-isomorphism classes of elliptic curves defined over $\mathbb{F}_p$ with j-invariant j. Then we get*

$$\#C_{p,j} = \begin{cases} 6 & j = 0 \text{ and } p \equiv 1 \pmod 3 \\ 4 & j = 1728 \text{ and } p \equiv 1 \pmod 4 \\ 2 & \text{otherwise.} \end{cases}$$

Since we know that for an elliptic curve E over $\mathbb{F}_p$ with

$$j(E) = 0 : E \text{ is supersingular} \iff p \equiv 2 \pmod 3$$
$$j(E) = 1728 : E \text{ is supersingular} \iff p \equiv 3 \pmod 4$$

holds, we can deduce from Proposition 2.3 that given a supersingular j-invariant j there are always exactly two $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with this j-invariant.

Proposition 2.4 *Let $p > 3$ and let E be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$. Then*

$$E \text{ is defined over } \mathbb{F}_p \iff \mathbb{Z}[\sqrt{-p}] \subseteq \operatorname{End} E.$$

Proof The implication ($\Rightarrow$) is immediate since π_p lies in End E. To prove the implication ($\Leftarrow$), let $\psi \in \operatorname{End} E$ satisfy $\psi^2 = [-p]$. Then ψ is an isogeny of degree p and $\widehat{\psi} \circ \psi = [p]$. Since E is supersingular it follows that ψ has kernel $\{\mathcal{O}_E\}$ and so is inseparable. Therefore, by Corollary II.2.12 of [18] , ϕ composes as

$$E \xrightarrow{\pi} E^{(p)} \xrightarrow{\lambda} E$$

where π is the p-power Frobenius map and $E^{(p)}$ is the image curve of Frobenius. Now $\deg(\lambda) = 1$ and so λ is an isomorphism. Hence, $j(E) = j(E^{(p)}) = j(E)^p$ and thus $j(E) \in \mathbb{F}_p$ holds. □

Now we want to give a connection between supersingular elliptic curves over $\mathbb{F}_p$ and certain elliptic curves in characteristic 0. In the ordinary case, the Deuring reduction theorem gives a one-to-one correspondence preserving the endomorphism ring. In the supersingular case, since $\operatorname{End}_{\bar{\mathbb{F}}_p} E$ is too large, it is less clear how to construct such a correspondence. But, for the case where E is defined over $\mathbb{F}_p$ with $p > 3$, then we have seen that $\operatorname{End}_{\mathbb{F}_p} E$ is an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Thus we can hope to get an analogous one-to-one correspondence. We now show this is the case.

Proposition 2.5 *There is a one-to-one correspondence*

$$\left\{ \begin{array}{c} \textit{supersingular elliptic} \\ \textit{curves over } \mathbb{F}_p \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{elliptic curves } E \textit{ over } \mathbb{C} \\ \textit{with } \operatorname{End} E \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\} \end{array} \right\}.$$

Proof Let $\mathcal{E}\ell\ell_p(\mathbb{C})$ be the set of isomorphism classes of elliptic curves in characteristic 0 with endomorphism ring $\mathcal{O} \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}$. Every element in $\mathcal{E}\ell\ell_p(\mathbb{C})$ corresponds to an ideal class in $\mathcal{C}\ell(\mathcal{O})$, so due to the observations above we get

$$\begin{aligned}
\#\mathcal{E}\ell\ell_p(\mathbb{C}) &= \sum_{\text{possible } \mathcal{O}} \#\mathcal{C}\ell(\mathcal{O}) \\
&= \begin{cases} h(-4p) & \text{if } p \equiv 1 \pmod 4 \\ h(-4p) + h(-p) & \text{if } p \equiv 3 \pmod 4 \end{cases} \\
&= \begin{cases} h(-4p) & \text{if } p \equiv 1 \pmod 4 \\ 2h(-p) & \text{if } p \equiv 7 \pmod 8 \\ 4h(-p) & \text{if } p \equiv 3 \pmod 8 \end{cases} \\
&= 2\#S_p.
\end{aligned}$$

We also define $\mathcal{E}\ell\ell(\mathbb{F}_p)$ as the set of supersingular elliptic curves over $\mathbb{F}_p$ up to $\mathbb{F}_p$-isomorphism. We want to show that there is a bijective map

$$\begin{aligned}
\mathcal{E}\ell\ell_p(\mathbb{C}) &\to \mathcal{E}\ell\ell(\mathbb{F}_p) \\
[E] &\mapsto \left[\bar{E}\right]
\end{aligned}$$

where $\bar{E}$ is the reduction of E at some fixed place $\mathfrak{P}_0$ over p.

- **Surjectivity:**
  Take a supersingular elliptic curve $\bar{E}$ over $\mathbb{F}_p$. Since Frobenius satisfies the polynomial $\pi_p^2 + p = 0$ it follows that $\mathrm{End}_{\mathbb{F}_p} \bar{E}$ contains the ring $\mathbb{Z}[\sqrt{-p}]$ or $\mathcal{O}_K$. Write this ring as $\mathbb{Z}[\bar{\psi}]$, so that $\bar{\psi}$ is either π_p or $(1 + \pi_p)/2$. Deuring's Lifting Theorem states that one can lift the pair $(\bar{E}, \bar{\psi})$ to a pair (E, ψ) where E is an elliptic curve over some number field H and $\psi \in \mathrm{End}(E)$ satisfies the same characteristic polynomial as $\bar{\psi}$. Indeed, H is the Hilbert class field of K or the ring class field of $\mathbb{Z}[\sqrt{-p}]$. Further, there is a place $\mathfrak{P}$ of H over p such that the reduction of E modulo $\mathfrak{P}$ is isomorphic to $\bar{E}$.
  We want to show that reduction modulo a fixed place $\mathfrak{P}_0$ of H is surjective. By Proposition 1.2 of [20] there exists $\sigma \in \mathrm{Gal}(H/K)$ such that $\mathfrak{P}^\sigma = \mathfrak{P}_0$ and so E^σ reduces modulo $\mathfrak{P}_0$ to the original curve $\bar{E}$. Hence, reduction modulo $\mathfrak{P}_0$ is surjective.
- **Injectivity:**
  We see from Eq. 1 and Proposition 2.3 that $\#\mathcal{E}\ell\ell(\mathbb{F}_p) = 2\#S_p = \#\mathcal{E}\ell\ell_p(\mathbb{C})$. Injectivity thus follows from surjectivity.

□

We re-inforce the fact that the correspondence of Proposition 2.5 is given by the Deuring lifting theorem: Given a supersingular elliptic curve $\bar{E}$ over $\mathbb{F}_p$ one performs Deuring lifting of the pair (E, ψ) where $\psi = \pi_p$ or $\psi = (1 + \pi_p)/2$.

It is important to see that isogenies behave well under this reduction. From Proposition 4.4 of [17] we know that reduction of isogenies is injective and preserves degrees. Furthermore we can show the following.

Proposition 2.6 *Let $\bar{E}_1, \bar{E}_2$ be supersingular elliptic curves over $\mathbb{F}_p$ and let (E_1, ψ_1) and (E_2, ψ_2) be the Deuring lifts of $(\bar{E}_1, \pi_p)$ and $(\bar{E}_2, \pi_p)$ to characteristic 0. Suppose there is an isogeny $\phi : E_1 \to E_2$. Then the reduced isogeny $\bar{\phi} : \bar{E}_1 \to \bar{E}_2$ is defined over $\mathbb{F}_p$.*

Proof Recall from [18, Exercise I.1.12c] that the isogeny $\bar{\phi}$ is defined over $\mathbb{F}_p$ if $\bar{\phi}^\sigma = \bar{\phi}$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ (meaning that $\bar{\phi}^\sigma(Q) = \bar{\phi}(Q)$ for all $Q \in \bar{E}_1(\bar{\mathbb{F}}_p)$). We may assume that $\bar{\phi}$ is defined over $\mathbb{F}_{p^r}$ for some r, so it suffices to consider only automorphisms $\sigma \in \mathrm{Gal}(\mathbb{F}_{p^r}/\mathbb{F}_p)$, and this Galois group is generated by the p-th power Frobenius σ_p with $\sigma_p(x) = x^p$ for all $x \in \mathbb{F}_{p^r}$. So we have to check $\bar{\phi}^{\sigma_p}(Q) = \bar{\phi}(Q)$ for all Q.

We may choose embeddings $\mathrm{End}(E_j) \to \mathbb{C}$ so that ψ_j is identified with $i\sqrt{p}$. Now every isogeny $\phi : E_1 \to E_2$ will satisfy $\phi \circ i\sqrt{p} = i\sqrt{p} \circ \phi$, since in characteristic 0 isogenies correspond to multiplication with a complex number.

After reduction the isogeny $\bar{\phi}$ commutes with π_p, and so $\pi_p \circ \bar{\phi} = \bar{\phi} \circ \pi_p$. Now,

$$\bar{\phi}^{\sigma_p}(P^{\sigma_p}) = (\bar{\phi}(P))^{\sigma_p} = \pi_p \circ \bar{\phi}(P) = \bar{\phi} \circ \pi_p(P) = \bar{\phi}(P^{\sigma_p})$$

for any $P \in \bar{E}_1$. The result follows. □

To describe the structure of $X(\mathbb{F}_p, \ell)$, we begin with a supersingular elliptic curve $\bar{E}$ over $\mathbb{F}_p$. As we have seen it has $\mathcal{O} := \mathrm{End}_{\mathbb{F}_p} \bar{E} \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\}$ in $K := \mathbb{Q}(\sqrt{-p})$, which is an order of discriminant $d_E \in \{-4p, -p\}$. Via the Deuring Lifting Theorem this elliptic curve can be lifted to an elliptic curve E over some number field with $\mathrm{End}\, E = \mathcal{O}$.

A standard fact (see [13] or Theorem 4 of [6]) is the following. Let $K = \mathbb{Q}(\sqrt{-p})$ have discriminant d_K and let E be an elliptic curve over $\mathbb{C}$ with $\mathrm{End}(E) = \mathcal{O}$ being an order in K. Let $c = [\mathcal{O}_K : \mathcal{O}]$ be the conductor of $\mathcal{O}$, so that the discriminant of $\mathcal{O}$ is $c^2 d_K$. Let ℓ be a prime. Then there are the possibilities

(1) $\ell \mid c$: one isogeny up and ℓ isogenies down,
(2) (a) ℓ **splits in** K: two horizontal isogenies and $\ell - 1$ isogenies down,
    (b) ℓ **is ramified in** K: one horizontal isogeny and ℓ isogenies down,
    (c) ℓ **is inert in** K: $\ell + 1$ isogenies down.

The structure of isogenies up and down is called a volcano. For our case, the only possibilities are $c = 1$ and, if $p \equiv 3 \pmod 4$, $c = 2$. Hence, the only prime of interest is $\ell = 2$, and when $p \equiv 3 \pmod 4$ and $\mathrm{End}(E) = \mathbb{Z}[\sqrt{-p}]$ then we have one 2-isogeny up and two 2-isogenies down.

Using these results we can construct an infinite "volcano" of elliptic curves whose endomorphism rings are orders in $\mathbb{Q}(\sqrt{-p})$. One can then consider the reduction modulo p of this volcano. All the reduced curves are supersingular. What happens is that most of the curves do not reduce to elliptic curves defined over $\mathbb{F}_p$, hence only a finite part of the volcano survives in the graph $X(\mathbb{F}_p, \ell)$. Proposition 2.4 explains why some isogenies down do not appear in the supersingular isogeny graph over $\mathbb{F}_p$. Some of the isogenies down are to orders like $\mathbb{Z}[\ell\sqrt{-p}]$ which do not contain $\sqrt{-p}$ anymore. So those reduced curves are not defined over $\mathbb{F}_p$ and do not show up as vertices in the graph $X(\mathbb{F}_p, \ell)$.

As shown in Proposition 2.6, the isogenies reduce to $\mathbb{F}_p$-rational outgoing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. It remains to be shown that every such isogeny can be reached in that way.

Let E be a supersingular elliptic curve over $\mathbb{F}_p$, so the $\mathbb{F}_p$-rational ℓ-isogenies correspond to Galois-invariant cyclic subgroups of $E[\ell]$. When we consider some prime $\ell \neq p$, $E[\ell]$ is a 2-dimensional vector space over $\mathbb{F}_\ell$ and π_p acts linearly on $E[\ell]$. Fixing a basis $\{P, Q\}$ for $E[\ell]$, the action of π_p is represented by a 2×2 matrix. We also know that $\pi_p^2 + p = 0$, so the matrix satisfies that characteristic polynomial modulo ℓ.

There are three cases for the quadratic polynomial modulo ℓ:

- it factors as $(\pi_p - a)^2$,
- it factors as $(\pi_p - a)(\pi_p - b)$ with $a \not\equiv b \pmod{\ell}$,
- it is irreducible.

Suppose there is a cyclic subgroup $G = \langle P \rangle$ of $E[\ell]$ with $\pi_p(G) = G$. Then it follows that $\pi_p(P) = [a]P$ in G for some integer a. We have that the linear map π_p has eigenspace $\langle P \rangle$ with eigenvalue a and so the characteristic polynomial has a root $(\pi_p - a)$. Hence, changing basis to use the point P and some other point Q it then follows by standard linear algebra that π_p is represented either by the matrix $\begin{pmatrix} a & 0 \\ b & a \end{pmatrix}$ or $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

We then deduce that the number of Galois-invariant cyclic subgroups of $E[\ell]$ is in the first case 1 or $\ell + 1$ depending on whether the matrix's lower left entry is $b \neq 0$ or $b = 0$. In the second case we have two of them and in the third there are none.

The polynomial $x^2 + p \pmod{\ell}$ can only have a repeated root for $\ell = 2$. When b in the matrix equals 0 resp. 1 modulo 2, we get three or one Galois-invariant subgroups of $E[2]$. We want to show that those possibilities occur in the right cases, so when $\mathrm{End}_{\mathbb{F}_p} E = \mathbb{Z}[\frac{-p+\pi_p}{2}]$ we have three outgoing 2-isogenies and when $\mathrm{End}_{\mathbb{F}_p} E = \mathbb{Z}[\pi_p]$ there is one of them.

We have $b \equiv 0 \pmod{2}$ if and only if $\pi_p(P) = P$ and $\pi_p(Q) = Q$, so $E[2] = \ker([2])$ is included in $\ker(1 + \pi_p)$. Since the multiplication-by-2-map is separable, there exists an unique isogeny $\phi \in \mathrm{End}\, E$ such that $1 + \pi_p = 2\phi$ due to [18, Corollary III.4.11]. ϕ is $\mathbb{F}_p$-rational since it is a quotient of $\mathbb{F}_p$-rational maps and therefore $\phi \in \mathrm{End}_{\mathbb{F}_p} E$. So the above is equivalent to $\mathbb{Z}[\pi_p] \subsetneq \mathrm{End}_{\mathbb{F}_p} E$ as we wanted to show.

For any other ℓ we get no $\mathbb{F}_p$-rational isogenies when the polynomial is irreducible, or two cyclic Galois-invariant subgroups when it is split. Finally, we are only interested in ℓ such that $\left(\frac{-p}{\ell}\right) = 1$, since otherwise there are no prime ideals of norm ℓ in $\mathbb{Z}[\sqrt{-p}]$ and so there are no edges in that graph. In that case we can see that the polynomial always splits with two distinct roots.

If we compare these results with the structure of the graph in characteristic 0, we have exactly the same number of outgoing ℓ-isogenies from the elliptic curves in both graphs which correspond to each other under reduction. Since the isogenies in characteristic 0 reduce to $\mathbb{F}_p$-rational isogenies, there is a correspondence

$$\left\{ \begin{array}{c} \mathbb{F}_p\text{-rational } \ell\text{-isogenies} \\ \text{between supersingular} \\ \text{elliptic curves over } \mathbb{F}_p \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \ell\text{-isogenies between} \\ \text{elliptic curves } E \text{ over } \mathbb{C} \\ \text{with } \mathrm{End}\, E \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\} \end{array} \right\}.$$

Thus we can transfer the picture from characteristic 0 exactly to our graphs $X(\mathbb{F}_p, \ell)$ and with these considerations we have described their structure completely. It can be summed up in the following way:

Theorem 2.7 *Let $p > 3$ be a prime.*

(1) $p \equiv 1 \pmod{4}$: There are $h(-4p)$ $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, all having the same endomorphism ring $\mathbb{Z}[\sqrt{-p}]$. From every one there is one outgoing $\mathbb{F}_p$-rational horizontal 2-isogeny as well as two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.

(2) $p \equiv 3 \pmod{4}$: There are two levels in the supersingular isogeny graph. From each vertex there are two horizontal ℓ-isogenies for every prime $\ell > 2$ with $\left(\frac{-p}{\ell}\right) = 1$.

(a) *If* $p \equiv 7 \pmod 8$, *on each level* $h(-p)$ *vertices are situated. Surface and floor are connected 1:1 with* 2*-isogenies and on the surface we also have two horizontal* 2*-isogenies from each vertex.*
(b) *If* $p \equiv 3 \pmod 8$, *we have* $h(-p)$ *vertices on the surface and* $3h(-p)$ *on the floor. Surface and floor are connected 1:3 with* 2*-isogenies, and there are no horizontal* 2*-isogenies.*

This provides a structure analogous to the one for the ordinary isogeny volcano, only that in our case we have no more than two levels and for $\ell > 2$ only exactly two outgoing isogenies from each elliptic curve (if any). If $p \equiv 1 \pmod 4$, there is only one 2-isogeny starting from every vertex, whereas for $p \equiv 3 \pmod 4$ we get two more when the elliptic curve is on the surface. Examples of all three cases are given in the Appendix. This result can be used to adapt the algorithms from the ordinary case that rely on the volcano structure. We will investigate one of them briefly in the next section.

3 The supersingular isogeny problem

We have seen in the last section that there is a connection between supersingular elliptic curves over $\mathbb{F}_p$ with $\mathbb{F}_p$-rational endomorphism ring $\mathcal{O}$ and the ideal class group $\mathcal{C}\ell(\mathcal{O})$. We have used this information to discover an elegant structure for the isogeny graph of supersingular elliptic curves over $\mathbb{F}_p$. Now we want to use this information to solve the isogeny problem.

Hence, let E_0 and E_1 be supersingular elliptic curves over $\mathbb{F}_p$, where $p > 3$. As we have shown, every such elliptic curve corresponds to an ideal class in $\mathcal{C}\ell(\mathcal{O})$. Furthermore any rational ℓ-isogeny from such an elliptic curve relates to an ideal of norm ℓ in $\mathcal{C}\ell(\mathcal{O})$. More precisely, if E is represented by the ideal $\mathfrak{a}$ and the isogeny ϕ by the ideal $\mathfrak{b}$ with $\mathrm{Norm}(\mathfrak{b}) = \ell$, then the image curve E' corresponds to the ideal $\mathfrak{b}^{-1} \cdot \mathfrak{a}$.

Due to a result of Bach [1], using GRH, the ideals of norm less than or equal to $6\log(|d|)^2$ (where d is the discriminant of $\mathcal{O}$) generate the ideal class group $\mathcal{C}\ell(\mathcal{O})$. Therefore we know that the supersingular isogeny graph is connected when we use all isogenies of prime degree up to $6\log(|d|)^2$. Usually we do not need all of those degrees and take a moderately small bound $B \ll 6\log|d|^2$. One can determine in subexponential time whether a set of ideals generates the ideal class group [9]. We set

$$L := \left\{\text{primes } \ell < B \mid \left(\tfrac{-p}{\ell}\right) = 1\right\}.$$

The condition $\left(\frac{-p}{\ell}\right) = 1$ comes from the fact that only in these cases do there exist $\mathbb{F}_p$-rational ℓ-isogenies between supersingular elliptic curves over $\mathbb{F}_p$, as shown in Theorem 2.7.

Since we know about the volcano-like structure now, it is possible to adapt the usual ordinary-case-algorithm [7] to this setting. First we identify the endomorphism ring of the initial curves using Theorem 2.7 as in Kohel's algorithm. If necessary we then take 2-isogenies so that both curves lie on the surface. From now on we assume we have two supersingular elliptic curves over $\mathbb{F}_p$ with the same $\mathbb{F}_p$-rational endomorphism ring $\mathcal{O}_K$. From both vertices we perform a breadth-first search (or a random walk in a lower storage version) in the graph $X(\mathbb{F}_p, L)$ whose edges are isogenies of degree $\ell \leq B$. Since the graph is connected for a big enough bound $B \leq 6\log(|d|)^2$, the algorithm invariably finds a path between the two vertices representing the elliptic curves. It is not hard to compute the whole isogeny as composition of small degree isogenies after that.

A very basic version of a random-walk/birthday-paradox bi-directional-search algorithm for computing a path in the subgraph of $X(\bar{\mathbb{F}}_p, L)$ is given as Algorithm 1. One could also

consider a high-storage breadth-first-search algorithm, but we used Algorithm 1 for our experiments as it is closer to a Pollard-style random walk approach. By the birthday paradox, the heuristic running time of the algorithm is $\tilde{O}(p^{1/4})$ binary operations.

ALGORITHM 1

INPUT: Supersingular elliptic curves E_0, E_1 over $\mathbb{F}_p$, some bound $B \leq 6\log(|d|)^2$
1: $S \leftarrow [\,]$
2: Take vertical 2-isogenies (if required) so that E_0 and E_1 are on the surface.
3: $L \leftarrow \left\{\text{primes } \ell < B \mid \left(\frac{-p}{\ell}\right) = 1\right\}$
4: $S_0 \leftarrow [j(E_0)]$, $S_1 \leftarrow [j(E_1)]$
5: $disjoint \leftarrow$ `true`
6: $i \leftarrow 0$
7: **while** $disjoint$ **do**
8: $\quad \ell \overset{R}{\leftarrow} L$
9: $\quad \Psi \leftarrow$ `ModularPolynomial`(ℓ)
10: $\quad j \overset{R}{\leftarrow$ `Roots`$(\Psi(X, S_i[\#S_i]))$
11: $\quad$ `Append`(S_i, j)
12: $\quad$ **if** $j \in S_{1-i}$ **then**
13: $\quad\quad disjoint \leftarrow$ `false`
14: $\quad\quad S \leftarrow$ `Cat`$(S_0[1, \ldots,$ `Index`$(S_0, j)], S_1[$`Index`$(S_1, j), \ldots, 1])$
15: $\quad$ **end if**
16: $\quad i \leftarrow 1 - i$
17: **end while**
OUTPUT: A path S in $X(\mathbb{F}_p, L)$ from $j(E_1)$ to $j(E_2)$

Remarks

1. Recall that the supersingular isogeny graph $X(\mathbb{F}_p, L)$ has the property that each curve and its non-trivial quadratic twist give two distinct vertices. Hence, the graph is in some sense twice as large as we would like. Hence, in practice it is more convenient to forget about the non-isomorphic twists and just work with the j-invariants. This halves the number of vertices and furthermore we can use precomputed modular polynomials instead of computing the division polynomial of each elliptic curve in the chain. The resulting isogeny from E_0 can map to a quadratic twist of E_1, in which case we simply compose with a suitable isomorphism.
2. When $p \equiv 7 \pmod 8$ one can use the prime 2 in L, though one must be careful to identify which one of the three outgoing 2-isogenies is actually going down to the floor.
3. There are many possible points of improvement like preferring small primes ℓ and using them more often [8], but to keep it simple they are omitted in this pseudo code.
4. A better algorithm would use Pollard-style random walks (i.e., walks that are deterministic and memoryless, so that when two walks collide they follow the same path from that point onwards) and distinguished points. The details of such algorithms are given in [7,8].

We implemented Algorithm 1 in MAGMA, as well as the standard high-storage bi-directional-search algorithm (breadth first search) using the full graph $X(\bar{\mathbb{F}}_p, 2)$ for comparison. Table 1 shows the results of those computations. For each bit length we took ten random primes p and for each prime selected 50 random pairs of j-invariants in $\mathbb{F}_p$. The average lengths of a path in $X(\bar{\mathbb{F}}_p, 2)$ resp. $X(\mathbb{F}_p, L)$ for $L = \left\{\text{primes } \ell < 20 \mid \left(\frac{-p}{\ell}\right) = 1\right\}$ between the same pairs and the corresponding average CPU time in seconds are displayed. The improvement from our new ideas is clear.

Table 1 Comparison of the average path length and running time for the bi-directional search algorithms in the full graph $X(\bar{\mathbb{F}}_p, 2)$ and the graph $X(\mathbb{F}_p, L)$ for random pairs of j-invariants in $\mathbb{F}_p$

	Path length		CPU time (seconds)	
p	$X(\bar{\mathbb{F}}_p, 2)$	$X(\mathbb{F}_p, L)$	$X(\bar{\mathbb{F}}_p, 2)$	$X(\mathbb{F}_p, L)$
16-Bit	178	12	0.084	0.018
20-Bit	801	31	0.380	0.029
24-Bit	3234	51	2.021	0.083
28-Bit	13040	129	18.516	0.303
32-Bit	53118	235	325.852	0.720

4 The general isogeny problem

We now consider the general isogeny problem: Given two supersingular elliptic curves E_0 and E_1 over $\bar{\mathbb{F}}_p$, to construct an isogeny between them. We desire an algorithm that is easily distributed, that requires low storage, and that has total running time of $\tilde{O}(p^{1/2})$ bit operations.

Such an algorithm can be developed using Pollard-style pseudorandom walks in the full graph, but the experience of the second author is that it is rather troublesome to implement, and the implied constants in the $\tilde{O}$ are poor. Instead, we now have a much simpler approach: The first stage is to run random walks in the graph from E_0 and E_1 until we hit a supersingular curve defined over $\mathbb{F}_p$. This stage should require $\tilde{O}(p^{1/2})$ steps. The second stage is to apply the new isogeny algorithm for supersingular elliptic curves over $\mathbb{F}_p$, which only requires $\tilde{O}(p^{1/4})$ steps. The crucial point is that the first stage can be done with simple non-backtracking random walks – rather than the much more difficult to implement stateless Pollard-style walks.

In more detail, given P processors one runs $P/2$ processors starting from each of E_0 and E_1 performing truly random non-backtracking walks (meaning that one remembers the current j-invariant j_c and the previous j-invariant j_p, and at each step one chooses uniformly at random one of the roots $\Phi_\ell(j_c, Y)/(Y - j_p)$). One could even instruct each of the processors to take a distinct path for the first $k = O(\log_2(P/2))$ steps (essentially computing distinct hash values on k-bit strings using the hash function of [3]). Since the graph is an expander, we expect the walks to quickly be sampling uniformly from the graph, and so we expect to select a vertex in the subset of $j \in \mathbb{F}_p$ with probability approximately $p^{1/2}/p = 1/p^{1/2}$. Alternatively, since the diameter is small, there will be a short path to the subset of $j \in \mathbb{F}_p$ of length at most $\frac{1}{2}\log(p)$ so one could distribute a depth-first search through all short paths from E_0. In any case, we expect the first stage to be easily distributed, require little storage, and require total effort $\tilde{O}(p^{1/2})$ bit operations (or total elapsed time $\tilde{O}(p^{1/2}/P)$ if we have P processors of equal power). The second stage has no effect on the asymptotic running time.

It is clear that this algorithm is much simpler to implement, and will have superior performance, to the approach using Pollard-style random walks in the full graph. However, there is one disadvantage: The large storage or Pollard-style algorithms can work in the graph $X(\bar{\mathbb{F}}_p, 2)$ and will find a sequence of 2-isogenies from E_0 to E_1. On the other hand, our algorithm in Sect. 3 for the subproblem where $j \in \mathbb{F}_p$ typically requires more primes, so the resulting isogeny is not a sequence of 2-isogenies. It is an open problem to transform an isogeny into a sequence of 2-isogenies in the supersingular case (in the ordinary case this

problem is the subgroup membership problem and discrete logarithm problem in the ideal class group).

Acknowledgments We thank David Kohel and Drew Sutherland for helpful conversations and Marco Streng for the idea of the proof of Proposition 2.6. Working on this paper started during a visit of the first author at the University of Auckland which was partially funded by a DAAD scholarship for PhD students.

Appendix: Example graphs

We present a few small examples of the irregular structure of the full supersingular isogeny graph $X(\bar{\mathbb{F}}_p, \ell)$. After that we display, for the same examples, the graphs $X(\mathbb{F}_p, \ell)$ which have a much more regular structure. For the examples we use the primes $p = 83, 101$ and 103, one for each of the different cases that occur. To demonstrate the two occurring structures we build the graphs for isogeny degrees $\ell = 2$ and the smallest prime $\ell > 2$ in each case for that isogenies exist.

Note that for $j(E) = 0$ resp. $j(E) \equiv 1728 \pmod p$ there are three resp. two non-equivalent isogenies mapping from E to another curve E'. but their dual isogenies are all equivalent. This is due to the fact that $\#\operatorname{Aut}(E) = 6$ resp. $\#\operatorname{Aut}(E) = 4$ in these cases. If $\phi : E \to E'$ is an isogeny and $\rho \in \operatorname{Aut}(E)$, then $\phi \circ \rho$ may not be equivalent (i.e., have the same kernel) as ψ, whereas the dual of $\phi \circ \rho$ is $\hat{\rho} \circ \hat{\phi}$, so this is equivalent to the dual of ϕ. We denote these multiple isogenies in the graph using a single arrow together with an integer to indicate the multiplicity.

An example for $p \equiv 1 \pmod 4$

If we take $p = 101$, we expect $\lfloor \frac{101}{12} \rfloor + 1 = 9$ supersingular j-invariants in $\mathbb{F}_{p^2}$. In the next figure we show how they are connected using 2-isogenies. The nodes labeled α and $\bar{\alpha}$ represent j-invariants in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ where $\bar{\alpha}$ is the conjugate of α. The graph can be easily computed with help of modular polynomials (Fig. 1).

In $X(\mathbb{F}_p, \ell)$ we will have $h(-4p) = 14$ nodes which are supersingular elliptic curves over $\mathbb{F}_p$ with endomorphism ring $\mathbb{Z}[\sqrt{-101}]$. There will be only one outgoing 2-isogeny from each curve, so naturally the graph can not be connected. It can be seen in Fig. 2.

It is notable that in this graph there are fewer connecting isogenies than in the full graph before. For example, in the first graph we have two isogenies going from the node 64 to the node 3 and two ones back, which are all missing in the new graph. This is due to the fact that those isogenies are not defined over $\mathbb{F}_p$, so they are not computed as edges in $X(\mathbb{F}_p, 2)$. Likewise the two loops from 59 to itself are isogenies over $\mathbb{F}_{p^2}$ that are dual to each other, whereas the loop at 21 is a $\mathbb{F}_p$-rational isogeny that is its own dual.

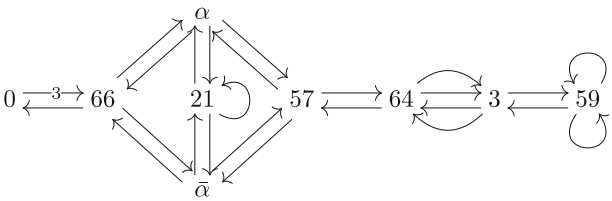

Fig. 1 Supersingular isogeny graph $X(\bar{\mathbb{F}}_{101}, 2)$

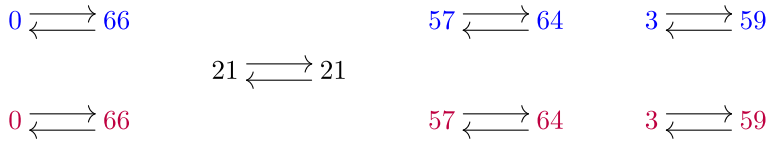

Fig. 2 $\mathbb{F}_p$-rational supersingular isogeny graph $X(\mathbb{F}_{101}, 2)$

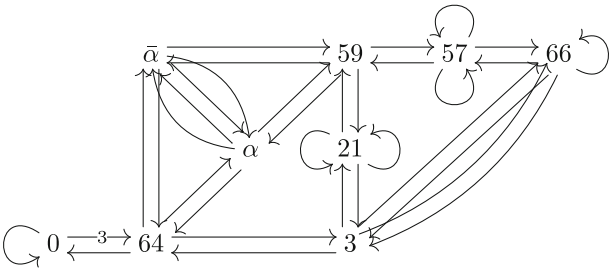

Fig. 3 Supersingular isogeny graph $X(\bar{\mathbb{F}}_{101}, 3)$

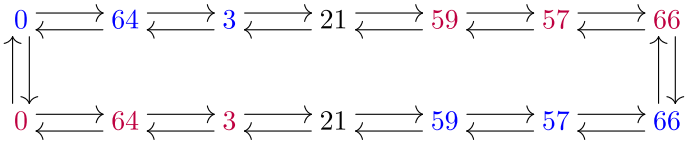

Fig. 4 Rational supersingular isogeny graph $X(\mathbb{F}_{101}, 3)$

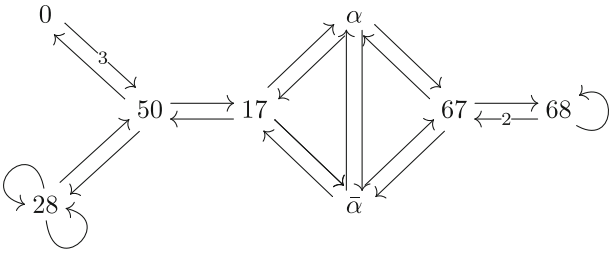

Fig. 5 Supersingular isogeny graph $X(\bar{\mathbb{F}}_{83}, 2)$

For higher isogeny degrees the number of outgoing isogenies from each vertex grows, so the graph becomes more complicated to draw. For this example we can take $\ell = 3$ since $\left(\frac{-p}{3}\right) = 1$ (Fig. 3).

Despite the complicated picture of the full graph, the graph over $\mathbb{F}_p$ becomes just a big circle. In particular, it is already fully connected. This is because the ideal class group of $\mathbb{Q}(\sqrt{-101})$ is generated by a prime ideal of norm 3 (Fig. 4).

Again you can see how the isogenies from the full graph that are defined over $\mathbb{F}_{p^2}$ vanish in the rational graph, and the single loops become isogenies from an elliptic curve to its quadratic twist. This latter fact can be shown in general.

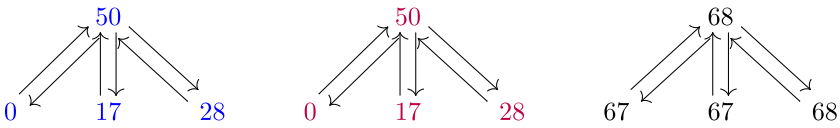

Fig. 6 Rational supersingular isogeny graph $X(\mathbb{F}_{83}, 2)$

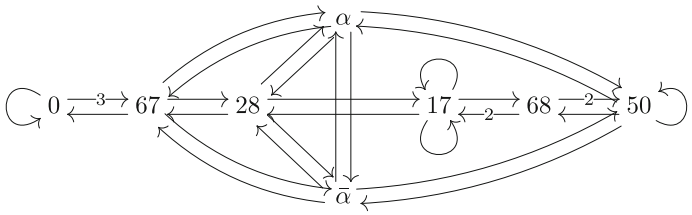

Fig. 7 Supersingular isogeny graph $X(\bar{\mathbb{F}}_{83}, 3)$

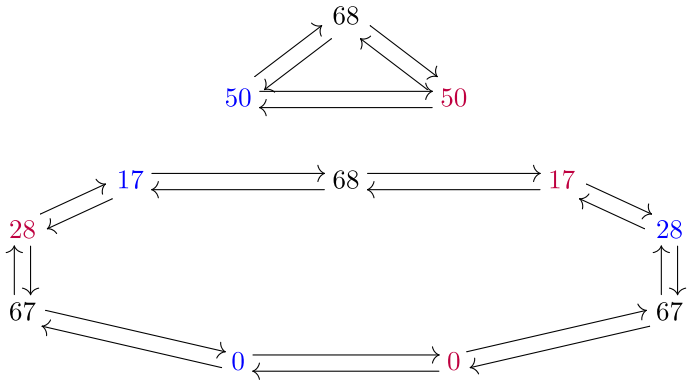

Fig. 8 Rational supersingular isogeny graph $X(\mathbb{F}_{83}, 3)$

An example for $p \equiv 3 \pmod 8$

For this case we take $p = 83$, so the full graph will have $\lfloor \frac{83}{12} \rfloor + 2 = 8$ vertices. Again we have two j-invariants $\alpha, \bar{\alpha} \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. The full 2-isogeny graph is given in Fig. 5.

In the graph over $\mathbb{F}_p$ we get $h(-p) = 3$ supersingular elliptic curves on the surface and $h(-4p) = 9$ ones on the floor. In the next figure we can see how 2-isogenies connect floor and surface as explained in case (2)(b) of Theorem 2.7 (Fig. 6).

If we repeat the procedure for $\ell = 3$, the full graph looks like Fig. 7.

And in the graph over $\mathbb{F}_p$ we get two isogeny circles, one on the floor and one on the surface (Fig. 8).

An example for $p \equiv 7 \pmod 8$

Our example here is $p = 103$ where we have $h(-p) = 5$ supersingular elliptic curves on the surface and also $h(-4p) = 5$ ones on the floor. In this case we have four nodes in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$ (Fig. 9).

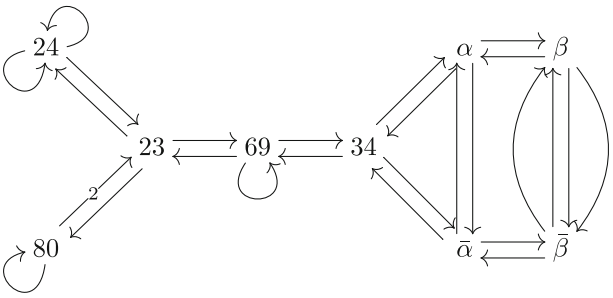

Fig. 9 Supersingular isogeny graph $X(\bar{\mathbb{F}}_{103}, 2)$

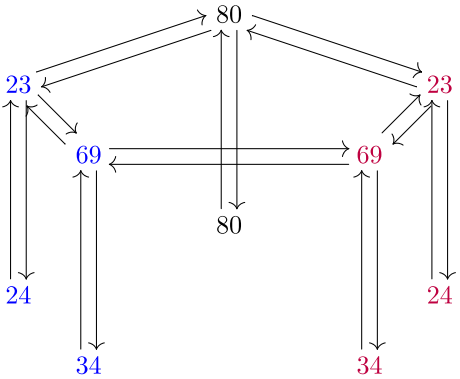

Fig. 10 Rational supersingular isogeny graph $X(\mathbb{F}_{103}, 2)$

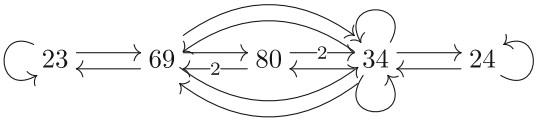

Fig. 11 Subgraph of supersingular isogeny graph $X(\bar{\mathbb{F}}_{103}, 7)$

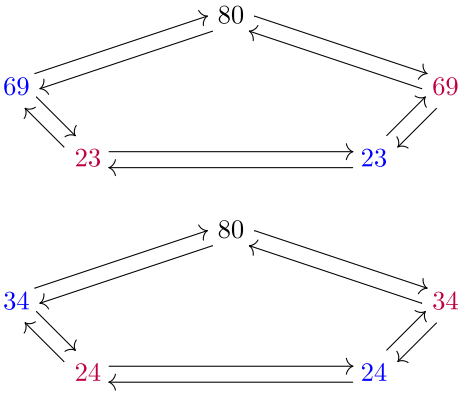

Fig. 12 Rational supersingular isogeny graph $X(\mathbb{F}_{103}, 7)$

The 2-isogeny graph over $\mathbb{F}_p$ in this case is already connected. Again a volcano structure can be observed where every supersingular elliptic curve on the floor has exactly one isogeny up starting at it (Fig. 10).

The smallest prime $\ell > 2$ with $\left(\frac{-103}{\ell}\right) = 1$ is $\ell = 7$. In the full graph every vertex has eight outgoing isogenies so it is not nice to draw. The subgraph of $X(\bar{\mathbb{F}}_{103}, 7)$ only consisting of j-invariants in $\mathbb{F}_{103}$ is presented in Fig. 11, so it can be compared to $X(\mathbb{F}_{103}, 7)$.

Again we get two isogeny cycles such that floor and surface each are fully connected when we draw the graph $X(\mathbb{F}_{103}, 7)$. This is because the ideal class group is cyclic and generated by a prime ideal of norm 7 (Fig. 12).

References

1. Bach E.: Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms. MIT Press, Cambridge (1984).
2. Bröker R.: Constructing Elliptic Curves of Prescribed Order. PhD thesis, Universiteit Leiden (2006).
3. Charles D.X., Lauter K.E., Goren E.Z.: Cryptographic hash functions from expander graphs. J. Cryptol. **22**(1), 93–113 (2009).
4. Cohen H.: A Course in Computational Algebraic Number Theory. Springer, Berlin (1996).
5. Cox D.A.: Primes of the Form $x^2 + ny^2$. Wiley, Hoboken (1989).
6. Galbraith S.D.: Constructing isogenies between elliptic curves over finite fields. LMS J. Comput. Math. **2**, 118–138 (1999).
7. Galbraith S.D., Hess F., Smart N.: Extending the GHS Weil descent attack. In: Advances in Cryptology—EUROCRYPT 2002, pp. 29–44. Springer, Berlin (2002).
8. Galbraith S.D, Stolbunov A.: Improved algorithm for the isogeny problem for ordinary elliptic curves. Appl. Algebr. Eng. Commun. Comput. **24**(2), 107–131 (2013).
9. Hafner J.L., McCurley K.S.: A rigorous subexponential algorithm for computation of class groups. J. Am. Math. Soc. **2**, 837–850 (1989).
10. Jao D., De Feo L.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Post-Quantum Cryptography, volume 7071 of Lecture Notes in Computer Science, pp. 19–34. Springer, Berlin (2011).
11. Jao D., Miller S.D., Venkatesan R.: Do all elliptic curves of the same order have the same difficulty of discrete log? In: Advances in Cryptology—ASIACRYPT 2005, pp. 21–40. Springer, Berlin (2005).
12. Jao D., Miller S.D., Venkatesan R.: Expander graphs based on GRH with an application to elliptic curve cryptography. J. Number Theory **129**(6), 1491–1504 (2009).
13. Kohel D.: Endomorphism rings of elliptic curves over finite fields. PhD thesis, University of California at Berkeley (1996).
14. Mestre J.-F.: La méthode des graphes. Exemples et applications. In: Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata), pp. 217–242 (1986).
15. Pohl I.: Bi-directional and heuristic search in path problems. Technical Report 104, Stanford Linear Accelerator Center, Stanford, California (1969).
16. Rück H.-G.: A note on elliptic curves over finite fields. Math. Comput. **49**(179), 301–304 (1987).
17. Silverman J.H.: Advanced Topics in the Arithmetic of Elliptic Curves. Springer, New York (1994).
18. Silverman J.H.: The Arithmetic of Elliptic Curves, 2nd edn. Springer, Dordrecht (2009).
19. Stolbunov A.: Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. Adv. Math. Commun. **4**(2), 215–235 (2010).
20. Tate J.T.: Global class field theory. In: Cassels J.W.S., Frölich A. (eds.) Algebraic Number Theory, pp. 162–203. Academic Press, Washington, DC (1967).
21. Vélu J.: Isogénies entre courbes elliptiques. C. R. Acad. Sci. Paris, Ser. A **273**, 238–241 (1971).
22. Waterhouse W.C.: Abelian varieties over finite fields. Ann. Sci. Ecole Norm. Sup. **2**(4), 521–560 (1969).