A quantum algorithm for computing isogenies between supersingular elliptic curves

Jean-François Biasse[1,2], David Jao[1], and Anirudh Sankar[1]

[1] Department of Combinatorics and Optimization
[2] Institute for Quantum Computing
University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada
{jbiasse,djao,asankara}@uwaterloo.ca

Abstract. In this paper, we describe a quantum algorithm for computing an isogeny between any two supersingular elliptic curves defined over a given finite field. The complexity of our method is in $\tilde{O}(p^{1/4})$ where p is the characteristic of the base field. Our method is an asymptotic improvement over the previous fastest known method which had complexity $\tilde{O}(p^{1/2})$ (on both classical and quantum computers). We also discuss the cryptographic relevance of our algorithm.

Keywords: Elliptic curve cryptography, quantum safe cryptography, isogenies, supersingular curves

1 Introduction

The computation of an isogeny between two elliptic curves in an important problem in public key cryptography. It occurs in particular in Schoof's algorithm for calculating the number of points of an elliptic curve [23], and in the analysis of the security of cryptosystems relying on the hardness of the discrete logarithm in the group of points of an elliptic curve [16, 17]. In addition, cryptosystems relying on the hardness of computing an isogeny between elliptic curves have been proposed in the context of quantum-safe cryptography [7, 22, 26, 5, 15]. For the time being, they perform significantly worse than other quantum-safe cryptosystems such as those based on the hardness of lattice problems. However, the schemes are worth studying since they provide an alternative to the few quantum-resistant cryptosystems available today.

In the context of classical computing, the problem of finding an isogeny between two elliptic curves defined over a finite field $\mathbb{F}_q$ of characteristic p has exponential complexity in p. For ordinary curves, the complexity is $\tilde{O}(q^{1/4})$ (here $\tilde{O}$ denotes the complexity with the logarithmic factors omitted) using the algorithm of Galbraith and Stolbunov [12]. In the supersingular case, the method of Delfs and Galbraith [9] is the fastest known technique, having complexity $\tilde{O}(p^{1/2})$.

With quantum computers, the algorithm of Childs, Jao and Soukharev [6] allows the computation of an isogeny between two ordinary elliptic curves defined

over a finite field $\mathbb{F}_q$ and having the same endomorphism ring in subexponential time $L_q(1/2, \sqrt{3}/2)$. This result is valid under the Generalized Riemann Hypothesis, and relies on computations in the class group of the common endomorphism ring of the curves. The fact that this class group in an abelian group is crucial since it allows one to reduce this task to a hidden abelian shift problem. In the supersingular case, the class group of the endomorphism ring is no longer abelian, thus preventing a direct adaptation of this method. The fastest known method for finding an isogeny between two isogenous supersingular elliptic curve is a (quantum) search amongst all isogenous curves, running in $\tilde{O}(p^{1/2})$. The algorithm of Childs, Jao and Soukharev [6] leads directly to attacks against cryptosystems relying on the difficulty of finding an isogeny between ordinary curves [7, 22, 26], but those relying on the hardness of computing isogenies between supersingular curves [5, 15] remain unaffected to this date.

Contribution. Our main contribution is the description of a quantum algorithm for computing an isogeny between two given supersingular curves defined over a finite field of characteristic p that runs in time $\tilde{O}(p^{1/4})$. Moreover, our algorithm runs in subexponential time $L_p(1/2, \sqrt{3}/2)$ when both curves are defined over $\mathbb{F}_p$. Our method is a direct adaptation of the algorithm of Delfs and Galbraith [9] within the context of quantum computing, using the techniques of Childs, Jao, and Soukharev [6] to achieve subexponential time in the $\mathbb{F}_p$ case. We address the cryptographic relevance of our method in Section 6.

2 Mathematical background

An elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p \neq 2, 3$ is an algebraic variety given by an equation of the form

$$E: \ y^2 = x^3 + ax + b,$$

where $\Delta := 4a^3 + 27b^2 \neq 0$. A more general form gives an affine model in the case $p = 2, 3$ but it is not useful in the scope of this paper since we derive an asymptotic result. The set of points of an elliptic curve can be equipped with an additive group law. Details about the arithmetic of elliptic curves can be found in many references, such as [25, Chap. 3].

Let E_1, E_2 be two elliptic curves defined over $\mathbb{F}_q$. An isogeny $\phi\colon E_1 \to E_2$ is a non-constant rational map defined over $\mathbb{F}_q$ which is also a group homomorphism from E_1 to E_2. Two curves are isogenous over $\mathbb{F}_q$ if and only if they have the same number of points over $\mathbb{F}_q$ (see [28]). Two curves over $\mathbb{F}_q$ are said to be isomorphic over $\overline{\mathbb{F}}_q$ if there is an $\overline{\mathbb{F}}_q$-isomorphism between their group of points. Two such curves have the same j-invariant given by $j := 1728\frac{4a^3}{4a^3+27b^2}$. In this paper, we treat isogenies as mapping between (representatives of) $\overline{\mathbb{F}}_q$-isomorphism classes of elliptic curves. In other words, given two j-invariants $j_1, j_2 \in \mathbb{F}_q$, we wish to construct an isogeny between (any) two elliptic curves E_1, E_2 over $\mathbb{F}_q$ having j-invariant j_1 (respectively j_2). Such an isogeny exists if and only if $\Phi_\ell(j_1, j_2) = 0$ for some ℓ, where $\Phi_\ell(X, Y)$ is the ℓ-th modular polynomial.

Let E be an elliptic curve defined over $\mathbb{F}_q$. An isogeny between E and itself defined over $\mathbb{F}_{q^n}$ for some $n > 0$ is called an endomorphism of E. The set of endomorphisms of E is a ring that we denote by $\mathrm{End}(E)$. For each integer m, the multiplication by m map on E is an endomorphism. Therefore, we always have $\mathbb{Z} \subseteq \mathrm{End}(E)$. Moreover, to each isogeny $\phi\colon E_1 \to E_2$ corresponds an isogeny $\widehat{\phi}\colon E_2 \to E_1$ called its dual isogeny. It satisfies $\phi \circ \widehat{\phi} = [m]$ where $m = \deg(\phi)$. For elliptic curves over a finite field, we know that $\mathbb{Z} \subsetneq \mathrm{End}(E)$. In this particular case, $\mathrm{End}(E)$ is either an order in an imaginary quadratic field (and has $\mathbb{Z}$-rank 2) or an order in a quaternion algebra ramified at p and ∞ (and has $\mathbb{Z}$-rank 4). In the former case, E is said to be ordinary while in the latter it is called supersingular.

An order $\mathcal{O}$ in a field K such that $[K : \mathbb{Q}] = n$ is a subring of K which is a $\mathbb{Z}$-module of rank n. The notion of ideal of $\mathcal{O}$ can be generalized to fractional ideals, which are sets of the form $\mathfrak{a} = \frac{1}{d} I$ where I is an ideal of $\mathcal{O}$ and $d \in \mathbb{Z}_{>0}$. The invertible fractional ideals form a multiplicative group $\mathcal{I}$, having a subgroup consisting of the invertible principal ideals $\mathcal{P}$. The ideal class group $\mathrm{Cl}(\mathcal{O})$ is by definition $\mathrm{Cl}(\mathcal{O}) := \mathcal{I}/\mathcal{P}$. In $\mathrm{Cl}(\mathcal{O})$, we identity two fractional ideals $\mathfrak{a}, \mathfrak{b}$ if there is $\alpha \in K$ such that $\mathfrak{b} = (\alpha)\mathfrak{a}$. The ideal class group is finite and its cardinality is called the class number $h_{\mathcal{O}}$ of $\mathcal{O}$. For a quadratic order $\mathcal{O}$, the class number satisfies $h_{\mathcal{O}} \leq |\Delta| \log |\Delta|$, where Δ is the discriminant of $\mathcal{O}$.

The endomorphism ring of an elliptic curve plays a crucial role in most algorithms for computing isogenies between curves. The class group of $\mathrm{End}(E)$ acts transitively on isomorphism classes of elliptic curves (that is, on j-invariants of curves) having the same endomorphism ring. More precisely, the class of an ideal $\mathfrak{a} \subseteq \mathcal{O}$ acts on the isomorphism class of curve E with $\mathrm{End}(E) \simeq \mathcal{O}$ via an isogeny of degree $\mathcal{N}(\mathfrak{a})$ (the algebraic norm of $\mathfrak{a}$). Likewise, each isogeny $\varphi\colon E \to E'$ where $\mathrm{End}(E) = \mathrm{End}(E') \simeq \mathcal{O}$ corresponds (up to isomorphism) to the class of an ideal in $\mathcal{O}$. From an ideal $\mathfrak{a}$ and the ℓ-torsion (where $\ell = \mathcal{N}(\mathfrak{a})$), one can recover the kernel of φ, and then using Vélu's formulae [29], one can derive the corresponding isogeny.

Given $\ell > 0$ prime, the ℓ-isogeny graph between (isomorphism classes of) elliptic curves defined over $\mathbb{F}_q$ is a graph whose vertices are the j-invariants of curves defined over $\mathbb{F}_q$ having an edge between j_1 and j_2 if and only if there exists an ℓ-isogeny ϕ between some two curves E_1, E_2 defined over $\mathbb{F}_q$ having j-invariant j_1 (respectively j_2). Note that while the curves E_1 and E_2 are required to be defined over $\mathbb{F}_q$, the isogeny ϕ is not. When $\ell \nmid q$, the ℓ-isogeny graph is connected. In this case, finding an isogeny between E_1 and E_2 amounts to finding a path between the j-invariant j_1 of E_1 and the j-invariant j_2 of E_2 in the ℓ-isogeny graph. Most algorithms for finding an isogeny between two curves perform a random walk in the ℓ-isogeny graph for some small ℓ. Our method is based on this strategy.

3 High level description of the algorithm

Our algorithm to find an isogeny between supersingular curves E, E' defined over $\mathbb{F}_q$ of characteristic p is based on the approach of Galbraith and Delfs [9], which exploits the fact that it is easier to find an isogeny between supersingular curves when they are defined over $\mathbb{F}_p$. The first step consists of finding an isogeny between E and E_1 (respectively between E' and E_2) where E_1, E_2 are defined over $\mathbb{F}_p$. On a quantum computer, we achieve a quadratic speedup for this first step using Grover's algorithm [13]. We then present a novel subexponential time quantum algorithm to find an isogeny between E_1 and E_2.

All isomorphism classes of supersingular curves over $\overline{\mathbb{F}}_q$ admit a representative defined over $\mathbb{F}_{p^2}$. As pointed out in [9], it is a well-known result that the number of supersingular j-invariants (that is, of isomorphism classes of supersingular curves defined over $\mathbb{F}_{p^2}$) is

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

where S_{p^2} is the set of supersingular j-invariants in $\mathbb{F}_{p^2}$. A certain proportion of these j-invariants in fact lie in $\mathbb{F}_p$; we denote this set by S_p. The number of such j-invariants satisfies

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

where $h(d)$ is the class number of the maximal order of $\mathbb{Q}(\sqrt{d})$ (See [8, Thm. 14.18]). As $h(d) \in \tilde{O}(\sqrt{d})$, we have $\#S_p \in \tilde{O}(\sqrt{p})$ (while $\#S_{p^2} \in O(p)$). The method used in [9] to find an isogeny path to a curve defined over $\mathbb{F}_p$ has complexity $\tilde{O}(\sqrt{p})$ (mostly governed by the proportion of such curves), while the complexity of finding an isogeny between curves defined over $\mathbb{F}_p$ is $\tilde{O}(p^{1/4})$.

Following this approach, we obtain a quantum algorithm for computing an isogeny between two given supersingular curves defined over a finite field of characteristic p that has (quantum) complexity in $\tilde{O}(p^{1/4})$. As illustrated in Figure 3, the search for a curve defined over $\mathbb{F}_p$, which is detailed in Section 4, has complexity $\tilde{O}(p^{1/4})$. Then, the computation of an isogeny between curves defined over $\mathbb{F}_p$, which we describe in Section 5, has subexponential complexity.

Theorem 1 (Main result). *Algorithm 1 is correct and runs under the Generalized Riemann Hypothesis in quantum complexity*

- $\tilde{O}(p^{1/4})$ *in the general case.*
- $L_q(1/2, \sqrt{3}/2)$ *when both curves are defined over* $\mathbb{F}_p$*,*

where $L_p(a, b) := e^{b \log(p)^a \log\log(p)^{1-a}}$.

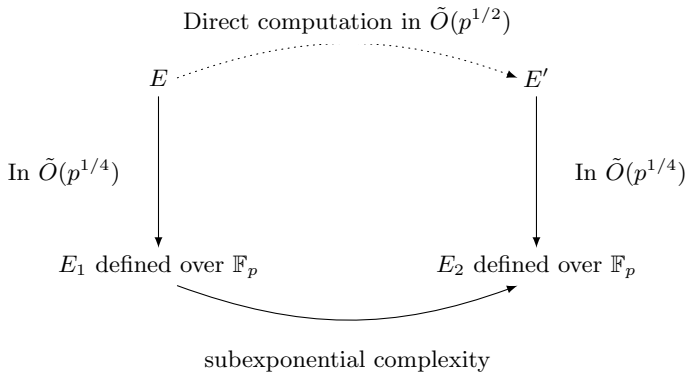


Fig. 1. $\tilde{O}(p^{1/4})$ method for supersingular curves

Algorithm 1 Isogeny computation between supersingular curves defined over a finite field

Input: Supersingular curves E, E' defined over $\mathbb{F}_q$ of characteristic p.
Output: An isogeny between E and E'

1: Find $\phi\colon E \to E_1$ where E_1 is defined over $\mathbb{F}_p$ by using Algorithm 2
2: Find $\psi\colon E' \to E_2$ where E_2 is defined over $\mathbb{F}_p$ by using Algorithm 2
3: Find $\alpha\colon E_1 \to E_2$ by using Algorithm 3
4: **return** $\widehat{\psi} \circ \alpha \circ \phi$

Proof. Steps 1 and 2 run in complexity $\tilde{O}(p^{1/4})$ as shown in Section 4 while Step 3 runs in subexponential complexity as shown in Section 5. Moreover, Steps 1 and 2 can be skipped if both curves are defined over $\mathbb{F}_p$.

4 The quantum search for a curve defined over $\mathbb{F}_p$

Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, we describe in this section how to find an isogeny path to a curve E' defined over $\mathbb{F}_p$. Our method has complexity $\tilde{O}(p^{1/4})$ and is based on a quantum search amongst a set of short isogeny paths initiating from E.

With classical algorithms, searching an unsorted database of N elements cannot be done in time faster than $O(N)$. With a quantum computer, Grover's algorithm [13] allows us to find an element x in the database such that $C(x) = 1$ (assuming all other elements y satisfy $C(y) = 0$) in complexity $O(\sqrt{N})$ with success probability greater than $1/2$. A rigorous analysis of the run time appears in Boyer et al. [2], which also contains a generalization to a multiple target search. The elements of the database are states that are encoded on n bits where $N = 2^n$, and condition $C(x)$ is assumed to be evaluated in unit time on these states.

The ℓ-isogeny graph for a prime $\ell \nmid p$ is a Ramanujan graph [10, Sec. 2]. This property allows us to evaluate the probability that an ℓ-isogeny path reaches a certain subset of the vertices. The following proposition applies this to the problem of finding a path leading to the subset S_p of the set S_{p^2} of all the vertices of the graph.

Proposition 1. *Under the Generalized Riemann Hypothesis, there is a probability at least* $\frac{\pi}{2^\gamma}\frac{1}{p^{1/2}}$ *that a random* 3*-isogeny path of length*

$$\lambda \geq \frac{\log\left(\frac{2}{\sqrt{6e^\gamma}}p^{3/4}\right)}{\log\left(\frac{2}{\sqrt{3}}\right)}$$

passes through a supersingular j*-invariant defined over* $\mathbb{F}_p$*, where* γ *is the Euler constant.*

Proof. This is a direct application of [10, Prop. 2.1] which states that for $c \geq 2\sqrt{\ell}$ and $k = \ell+1$, a random ℓ-isogeny walk (for $\ell \nmid p$) of length at least $\frac{\log\left((2|G|/|S|^{1/2}\right)}{\log(k/c)}$ starting from a given curve will hit a subset S of the vertices G with probability at least $\frac{|S|}{2|G|}$. We apply this to $G = S_{p^2}$ and $S = S_p$, knowing that $|G| \geq p/12$, and that under the Generalized Riemann Hypothesis [14], the class number of the maximal order of $\mathbb{Q}(\sqrt{-d})$ satisfies

$$h(d) \geq (1 + o(1)) \cdot \frac{\pi}{12e^\gamma}\frac{\sqrt{d}}{\log\log(d)}.$$

A direct substitution of these values allows us to obtain the desired result.

When p is large enough, the probability that all of $\log(2)\frac{e^\gamma}{\pi}p^{1/2}$ random 3-isogeny-paths of length λ defined in Proposition 1 initiating from a given curve do not hit any supersingular j-invariant defined over $\mathbb{F}_p$ is

$$\begin{aligned}\left(1 - \frac{\pi}{e^\gamma}\cdot\frac{1}{p^{1/2}}\right)^{\log(2)\frac{e^\gamma}{\pi}p^{1/2}} &= e^{\log(2)\frac{e^\gamma}{\pi}p^{1/2}\cdot\log\left(1-\frac{\pi}{e^\gamma}\cdot\frac{1}{p^{1/2}}\right)} \\ &\sim e^{\log(2)\frac{e^\gamma}{\pi}p^{1/2}\cdot\left(-\frac{\pi}{e^\gamma}\cdot\frac{1}{p^{1/2}}\right)} = \frac{1}{2}.\end{aligned}$$

Therefore, a set of $N := \log(2)\frac{e^\gamma}{\pi}p^{1/2}$ random 3-isogeny-paths of length λ contains at least one that passes through S_p with probability at least $1/2$. A quantum search with Grover's algorithm yields our target isogeny path (which exists with probability $1/2$) in complexity $O(\sqrt{N}) = O(p^{1/4})$. Let us formalize this search. At each node corresponding to the j-invariant j_0, the polynomial $\Phi_3(j_0, X)$ has four roots, one corresponding to the father of the node, and j_1, j_2, j_3 corresponding to its children. Therefore, each path can be encoded in $\{0,1,2\}^\lambda$. As $\lambda \in O(\log(p))$, the number of bits needed to encode such a path is also in

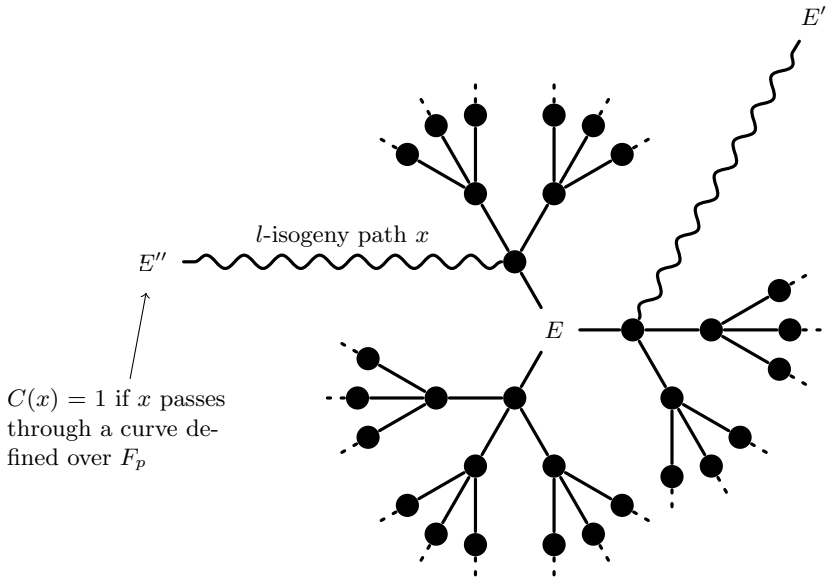


Fig. 2. Quantum walk to a curve defined over $\mathbb{F}_p$

$O(\log(p))$. Note that the actual computation of a 3-isogeny between representatives of the isomorphism classes of two given j-invariants is classical and used in Section 5. It can be done in polynomial time. At the beginning of the algorithm, we compute a random injection

$$f\colon [1, \cdots, N] \to \{\text{3-isogeny paths of length } \lambda \text{ starting from } E\}.$$

For our search, we use the function C defined on $x \in [1, \cdots, N]$ by

$$C_f(x) := \begin{cases} 1 & \text{if } f(x) \text{ passes through } S_p, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 2. *Algorithm 2 has success probability* $1/4$ *and expected run time in* $\tilde{O}(p^{1/4})$.

Proof. The complexity derives from the analysis of Grover's algorithm. The only difference is that the evaluation of C_f is done in polynomial time, thus inducing terms in $\log(p)$ in the complexity.

Remark 1. We can find an isogeny between two given supersingular curves E, E' directly by using a quantum search method. It suffices to apply the above method to the trivial subset $S = \{j(E')\}$ of size 1. The corresponding complexity is in $\tilde{O}(p^{1/2})$.

Algorithm 2 Quantum walk to a curve defined over $\mathbb{F}_p$

Input: Supersingular curve E defined over $\mathbb{F}_q$ of characteristic p.
Output: E' defined over $\mathbb{F}_p$ and $\phi\colon E \to E'$

1: $\lambda := \left\lceil \frac{\log\left(\frac{2}{\sqrt{6e^{\gamma}}} p^{3/4}\right)}{\log\left(\frac{2}{\sqrt{3}}\right)} \right\rceil$.
2: Choose $f\colon [1, \cdots, N] \to \{\text{3-isogeny paths of length } \lambda \text{ starting from } E\}$ randomly.
3: Use Grover's algorithm to find $x \in [1, \cdots, N]$ such that $C_f(x) = 1$.
4: Compute the isogeny path $\phi_1, \cdots, \phi_\lambda$ corresponding to x.
5: **return** $\phi_1 \circ \cdots \circ \phi_\lambda, \phi_1 \circ \cdots \circ \phi_\lambda(E)$.

5 Computing an isogeny between curves defined over $\mathbb{F}_p$

We now present a quantum algorithm for computing an isogeny between supersingular curves defined over $\mathbb{F}_p$ in subexponential time $L_p(1/2, \sqrt{3}/2)$. Our approach relies on the correspondence between these curves and elliptic curves with complex multiplication by a quadratic order described by Delfs and Galbraith [9], and on the quantum subexponential algorithm for ordinary curves of Childs, Jao and Soukharev [6].

General strategy. The endomorphism ring $\mathrm{End}(E)$ of a supersingular curve is an order in a quaternion algebra, but as shown in [9, Th. 2.1], the ring $\mathrm{End}_{\mathbb{F}_p}(E)$ of endomorphisms defined over $\mathbb{F}_p$ is isomorphic to an order $\mathcal{O}$ in the quadratic number field $K := \mathbb{Q}(\sqrt{-p})$. More specifically, it is equal to either $\mathbb{Z}[\sqrt{-p}]$ or the maximal order $\mathcal{O}_K$. There is a transitive action of $\mathrm{Cl}(\mathcal{O})$ on the $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$. As in the ordinary case, the class of an ideal $\mathfrak{a}$ acts via an isogeny of degree $\mathcal{N}(\mathfrak{a})$. Therefore, for each supersingular curve E defined over $\mathbb{F}_p$ with endomorphism ring isomorphic to $\mathcal{O}$, we have an injective function

$$\begin{array}{rccc} f_E\colon & \mathrm{Cl}(\mathcal{O}) & \longrightarrow & \mathbb{F}_p - \text{isomorphism classes of curves over } \mathbb{F}_p \\ & [\mathfrak{b}] & \longmapsto & \text{action of } [\mathfrak{b}] \text{ on the class of } E \end{array}.$$

Given two supersingular curves E_1 and E_2 defined over $\mathbb{F}_p$, the problem of finding the ideal class $[\mathfrak{a}]$ such that $f_{E_2}(x) = f_{E_1}([\mathfrak{a}] \cdot x)$ for all x is an instance of the *hidden abelian shift problem*. We solve it to find the ideal class $[\mathfrak{a}]$ such that the class of E_2 is the image of the action of $[\mathfrak{a}]$ on the class of E_1. Then we find the corresponding isogeny $\phi\colon E_1 \to E_2'$ where E_2' lies in the same $\mathbb{F}_p$-isomorphism class as E_2. Finally, we use the method described in [11, Appendix A.2] to calculate the $\mathbb{F}_p$-isomorphism between E_2' and E_2. The composition of both maps is an isogeny between E_1 and E_2. The procedure is summarized in Algorithm 3.

The action of $\mathrm{Cl}(\mathcal{O})$. Let K be the quadratic number field $\mathbb{Q}(\sqrt{-p})$ having maximal order $\mathcal{O}_K$. By [9, Prop. 2.5], there is a one-to-one correspondence

$$\left\{ \begin{array}{l} \text{Supersingular elliptic curves} \\ \text{defined over } \mathbb{F}_p \end{array} \right\} \leftrightarrow \left\{ \begin{array}{l} \text{Elliptic curves } E \text{ over } \mathbb{C} \text{ with} \\ \mathrm{End}(E) \in \{\mathbb{Z}[\sqrt{-p}], \mathcal{O}_K\} \end{array} \right\}.$$

Algorithm 3 Computation of an isogeny between supersingular curves over $\mathbb{F}_p$

Input: Supersingular curves E_1, E_2 defined over $\mathbb{F}_p$.
Output: An isogeny $\phi\colon E_1 \to E_2$.
1: Compute an isogeny $\phi_1\colon E_1 \to E_1'$ with $\mathrm{End}(E_1') = \mathcal{O}_K$.
2: Compute an isogeny $\phi_2\colon E_2 \to E_2'$ with $\mathrm{End}(E_2') = \mathcal{O}_K$.
3: Solve the hidden abelian shift problem to find $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)$ such that the action of $[\mathfrak{a}]$ on the isomorphism class of E_1' is the class of E_2'.
4: Deduce an isogeny $\phi_3\colon E_1' \to E_2''$ where E_2'' is $\mathbb{F}_p$-isomorphic to E_2'.
5: Find the $\mathbb{F}_p$ isomorphism $\alpha\colon E_2'' \to E_2'$.
6: **return** $\widehat{\phi_2} \circ \alpha \circ \phi_3 \circ \phi_1$.

In one direction, this correspondence is given by the Deuring lift, while in the other direction, it is given by the reduction at a place $\mathfrak{P}$ above p. Moreover, we have a bijective map

$$\begin{array}{ccc} \text{Classes of curves with } \mathrm{End}(E) = \mathcal{O} & \longrightarrow & \text{Classes of curves with } \mathrm{End}(E)_{\mathbb{F}_p} = \mathcal{O} \\ \text{Isomorphism class of } E & \longmapsto & \mathbb{F}_p\text{-isomorphism class of } \bar{E} \end{array}$$

where $\bar{E}$ is the reduction of E modulo $\mathfrak{P}$. Therefore, the $\mathbb{F}_p$-isomorphism classes of curves over $\mathbb{F}_p$ with $\mathbb{F}_p$-endomorphism ring $\mathcal{O}$ are in one-to-one correspondence with isomorphism classes of complex curves with endomorphism ring $\mathcal{O}$. The class group of $\mathcal{O}$ acts on these complex curves, therefore inducing by modular reduction an action on the curves over $\mathbb{F}_p$. Indeed, the class $[\mathfrak{a}]$ of an ideal $\mathfrak{a} \subseteq \mathcal{O}$ acts on the class of a complex curve E via an isogeny $\phi\colon E \to E'$ with $\deg(\phi) = \mathcal{N}(\mathfrak{a})$. By [9, Prop.2.6], this gives us by reduction an isogeny $\overline{\phi}\colon \bar{E} \to \bar{E}'$. From the correspondence between isomorphism classes over $\mathbb{C}$ and $\mathbb{F}_p$-isomorphism classes over $\mathbb{F}_p$, we get a group action of $\mathcal{O}$ on $\mathbb{F}_p$-isomorphism classes of supersingular curves defined over $\mathbb{F}_p$.

Computing the action of $\mathrm{Cl}(\mathcal{O})$. Our method to solve the hidden abelian shift problem is based on the algorithm described by Childs, Jao and Soukharev [6] which relies on a (classical) subexponential algorithm to compute the action of $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ on isomorphism classes of ordinary curves. In this paragraph, we show how to compute (classically) the action of $\mathrm{Cl}(\mathcal{O})$ on $\mathbb{F}_p$-isomorphism classes of supersingular curves $E : Y^2 = X^3 + aX + b = 0$ with $\mathrm{End}_{\mathbb{F}_p}(E) \simeq \mathcal{O}$. In a nutshell, it is similar to the approach of Childs, Jao and Soukharev [6], except that the role of $\mathrm{End}(E)$ is replaced by $\mathrm{End}_{\mathbb{F}_p}(E)$.

The first step consists of finding split prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$ having norm $\mathcal{N}(\mathfrak{p}_i) \leq L_p(1/2, \sqrt{3}/2)$ such that $[\mathfrak{a}] = [\mathfrak{p}_1]^{e_1} \cdots [\mathfrak{p}_k]^{e_k}$. This way, the action of $[\mathfrak{a}]$ can be calculated as the composition of the action of the $[\mathfrak{p}_i]$ for $i \leq k$. The subexponential classical strategy for performing this decomposition is standard in class group computation and discrete logarithm resolution. In this paper, we use the particular version described in [6, Alg. 1].

Once $[\mathfrak{a}]$ has been successfully rewritten, evaluating its action reduces to evaluating that of $[\mathfrak{p}]$ where $\mathfrak{p}$ is a split prime ideal with $\mathcal{N}(\mathfrak{p}) = \ell$. Let us denote by $\bar{E}$ a representative of the $\mathbb{F}_p$-isomorphism class on which we want to evaluate

the action of $[\mathfrak{p}]$ and by E its Deuring lift (which we do not actually compute). Amongst the $\ell+1$ complex roots of $\Phi_\ell(j(E), X)$ (where $\ell \nmid p$, $\ell \neq 2$), only two reduce to j-invariants defined over $\mathbb{F}_p$. One of them corresponds to the action of $[\mathfrak{p}]$ on the isomorphism class of E while the other one is the result of the action of $[\overline{\mathfrak{p}}]$ (where $\overline{\mathfrak{p}}$ is the complex conjugate of $\mathfrak{p}$). The other roots correspond to ascending or descending isogenies.

Let j be one of the roots mentioned above. As described in Bröker, Charles and Lauter [4, Section 3], there are two methods for computing the equation of a curve E' in the isomorphism class identified by j. One method is to use the Atkin-Elkies formulas given by Schoof in [23, Sec. 7] to compute $E' : Y^2 = X^3 + a'X + b'$ where

$$a' = -\frac{1}{48}\frac{{j'}^2}{j(j-1728)}\ ,\ b' = -\frac{1}{864}\frac{{j'}^3}{j^2(j-1728)}\ ,\ j' = -\frac{18}{\ell}\frac{b}{a}\frac{\Phi_{\ell,X}(j(E),j)}{\Phi_{\ell,Y}(j(E),j)}j(E),$$

with $\Phi_{\ell,X}(X,Y) = \frac{\partial \Phi_\ell}{\partial X}(X,Y)$ and $\Phi_{\ell,Y}(X,Y) = \frac{\partial \Phi_\ell}{\partial Y}(X,Y)$. Reduction modulo $\mathfrak{P}$ of the above formulas yield an equation of a supersingular curve defined over $\mathbb{F}_p$ in the $\mathbb{F}_p$-isomorphism class corresponding to the class of complex curves having j-invariant j. This method can fail in the event that one of the terms appearing in a denominator (namely, j, $j-1728$, or $\Phi_{\ell,Y}(j(E),j)$) equals zero. The second method is to use division polynomials to construct $E[\ell]$ explicitly over a field extension. One then checks each of the possible $\ell+1$ cyclic ℓ-subgroups of $E[\ell]$ until the correct kernel is found.

In the case of ordinary elliptic curves, the j-invariants $j=0$ and $j=1728$ that induce failure in the first method can often be avoided (for example, if they do not belong to the isogeny class in question), and the term $\Phi_{\ell,Y}(j(E),j)$ never vanishes as long as $\ell < 4 \cdot |\operatorname{disc}(\operatorname{End}(E))|$. In the supersingular case, we found experimentally that the $\Phi_{\ell,Y}(j(E),j)$ term does often vanish even when $\ell < 4 \cdot |\operatorname{disc}(\operatorname{End}(E))|$, necessitating the second approach, which works unconditionally.

To determine if j was the j-invariant of the isomorphism class resulting from the action of the class of $\mathfrak{p}$ or its conjugate, we first compute the kernel $C \subset \bar{E}[\ell]$ of the isogeny between $\bar{E}$ and $\bar{E}'$ by the approach described by Schoof [23, Sec. 8] and used by Bröker Charles and Lauter [4]. The ideal $\mathfrak{p}$ is of the form $\mathfrak{p} = \ell\mathcal{O} + (c + d\sqrt{-p})\mathcal{O}$, and it induces an action on the points P of $\bar{E}$ given by $\mathfrak{p}\cdot P = [\ell]P + [c]P + [d]\pi_p(P)$ where π_p is the p-th power Frobenius endomorphism. If $\mathfrak{p} \cdot P = 0$ for all $P \in C$, our choice was correct; otherwise, we redo the computation with the other root of $\Phi_\ell(j(E), X)$.

Proposition 3. *The running time of Algorithm 4 is* $L_p\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$

Proof. The proof of complexity follows from the considerations of [6, Sec. 4.1].

Solving the abelian shift problem. As we have an action of $\mathrm{Cl}(\mathcal{O})$ on the $\mathbb{F}_p$-isomorphism classes of supersingular curves defined over $\mathbb{F}_p$ that we can compute in subexponential time, we can readily apply the same method as in [6, Sec. 5] to

Algorithm 4 Action of $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$

Input: A supersingular curve E defined over $\mathbb{F}_p$, a quadratic order $\mathcal{O} \simeq \mathrm{End}_{\mathbb{F}_p}(E)$ and an ideal $\mathfrak{a} \subseteq \mathcal{O}$.

Output: A supersingular curve E' defined over $\mathbb{F}_p$ in the $\mathbb{F}_p$-isomorphism class resulting from the action of $[\mathfrak{a}]$ on the class of E.

1: Find $(\mathfrak{p}_i)_{i \leq k}$ with $\mathfrak{p}_i \nmid (2) \cdot (\#E(\mathbb{F}_p))$ and $\mathcal{N}(\mathfrak{p}_i) \leq L_p(1/2, \sqrt{3}/2)$ such that $[\mathfrak{a}] = \prod_i [\mathfrak{p}_i]$
2: **for** $i \leq k$ **do**
3: Compute $\Phi_i(X, Y)$ where $l = \mathcal{N}(\mathfrak{p}_i)$.
4: Find the two roots j_1, j_2 of $\Phi_l(j(E), X)$ defined over $\mathbb{F}_p$.
5: Compute E' of j-invariant j_1 using the method of [23, Sec. 7].
6: Compute the kernel C of the isogeny $E \to E'$ using the method of [23, Sec. 8].
7: If there exists $P \in C$ such that $[c]P + [d]\pi_p(P) \neq 0$, where c and d are integers such that $\mathfrak{p} = (\ell, c + d\pi_p)$, go back to Step 5 and use j_2 instead of j_1.
8: $E \leftarrow E'$.
9: **end for**
10: **return** E'.

solve the hidden abelian shift problem. Childs, Jao and Soukharev considered two quantum algorithms. The first one is Kuperberg's approach based on a Clebsch-Gordan sieve on coset states [19]. The other one relies on Regev's algorithm [21]. In this way we obtain the following result.

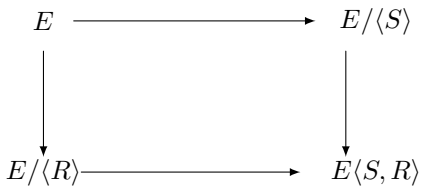
Proposition 4 (Theorem 5.4 of [6]). *On a quantum computer, the hidden abelian shift of Step 3 in Algorithm 3 can be solved in time $L_p(1/2, \sqrt{3}/2)$ under the Generalized Riemann Hypothesis.*

Climbing the volcano. Steps 1 and 2 of Algorithm 3 ensure that the curves between which we are trying to compute an isogeny have the same endomorphism ring. As mentioned in [9], a supersingular elliptic curve defined over $\mathbb{F}_p$ has $\mathbb{F}_p$-endomorphism ring satisfying $\mathrm{End}_{\mathbb{F}_p}(E) \simeq \mathcal{O}$ for $\mathcal{O} \in \{\mathbb{Z}[\sqrt{-p}, \mathcal{O}_K\}$. This means that the isogeny volcano has at most two levels, namely the crater and the ground level. In Steps 1 and 2 of Algorithm 3 we climb to the crater. This step can be done by computing a single 2-isogeny. As shown in [9, Sec. 2], if $\Phi_2(j(E), X)$ has three roots, then $\mathrm{End}_{\mathbb{F}_p}(E) = \mathcal{O}_K$ and we do nothing. Otherwise, $\Phi_2(j(E), X)$ has one root, which is the j-invariant of an isogenous curve E' on the crater (that is, with $\mathrm{End}_{\mathbb{F}_p} = \mathcal{O}_K$). In this case, we know that $\mathrm{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}] \neq \mathcal{O}_K$ and we compute $\phi \colon E \to E'$.

6 Cryptographic relevance

The main motivation for our result is its impact on existing cryptosystems relying on the hardness of finding an isogeny between two given curves. Those that use ordinary elliptic curves [7, 22, 26] are not affected by our method. The subexponential algorithm of Childs, Jao and Soukharev [6] already provides a quantum subexponential attack against these.

De Feo-Jao-Plût cryptographic schemes. In [10] (which is an extended version of [15]), De Feo, Jao and Plût presented a key exchange protocol, an encryption protocol and a zero knowledge proof of identity all relying on the difficulty of computing an isogeny between supersingular curves. More specifically, given a secret point S of a curve E over $\mathbb{F}_{p^2}$, and a public point R, they exploit the commutative diagram



The unified treatment of these three cryptographic schemes around the above commutative diagram yields situations where the degree of the secret isogenies is known and in $O(\sqrt{p})$. Therefore, there is a classical attack in $O(p^{1/4})$ and a quantum attack relying on a claw algorithm [24] with complexity $O(p^{1/6})$. Given these results, our $p^{1/4}$ quantum algorithm does not yield the fastest attack. Moreover, it is not even clear that finding an arbitrary isogeny between two given curves yields an attack at all since the cryptosystems described in [10] rely on the difficulty of finding an isogeny of given degree, while our method returns an isogeny of arbitrary degree. Note that a recent contribution of Jao and Soukharev [18] uses similar methods to describe a quantum-resistant undeniable signature scheme.

Even though our work does not directly yield a faster attack against the existing schemes of [10], it does introduce the possibility that choosing a base curve E defined over $\mathbb{F}_p$ may be insecure. The base curve E is a public parameter, chosen once and for all at the time the system is initialized, and never changed during the life of the system. If this base curve is defined over $\mathbb{F}_p$, then Step 1 of Algorithm 1 becomes trivial. While this situation is not fatal, it does seem to be cause for some concern, provided that the arbitrary degree obstacle mentioned above can be overcome; at the very least, it decreases by half the amount of work the attacker must perform. De Feo et al. [10, Section 4.1] propose two methods for choosing the base curve. One of these methods uses random walks, and would not normally produce base curves defined over $\mathbb{F}_p$. The other method uses Bröker's algorithm [3] to produce a supersingular curve which is then used directly as the base curve. This method does sometimes produce curves defined over $\mathbb{F}_p$, and in light of our results, we recommend avoiding this method out of an abundance of caution.

Generalizations of De Feo-Jao-Plût. It is possible to conceive of potential generalizations of the cryptosystems presented in [10] to a situation where the degree of the isogenies is unknown, in which case our algorithm would yield the fastest (quantum) attack. For example, let us sketch how this could be done for the zero knowledge proof of identity. Assume Peggy knows a secret kernel C_1 and

$\psi\colon E \to E/C_1$. At each round, Peggy draws a kernel C_2 coprime with C_1 and publishes $E, E/C_1, E/C_2, E_{\langle C_1, C_2\rangle}$. Then Vic flips a coin b.

- If $b = 0$, she asks to know $E \to E/C_2$ and $E/C_1 \to E/\langle C_1, C_2\rangle$.
- If $b = 1$, she asks to know $E/C_2/C_1 \to E/\langle C_1, C_2\rangle$.

The kernels can be drawn from coprime power-products of ideals of small norm in $\mathrm{End}(E)$, thus ensuring that the diagram commutes. A proof similar to that of [10, Th. 6.3] shows that it is zero knowledge. This protocol relies on the difficulty of finding an isogeny between two given curves, and the fastest quantum attack is our $p^{1/4}$ algorithm. Of course, this generalization is difficult to make practical, and many optimizations were made in [10] that justify using isogenies of known degrees. Our suggestion is merely an illustration of the fact that adaptations to the case of secret isogenies of unknown degree could be used.

The Charles-Goren-Lauter hash function. In [5], Charles, Gore and Lauter described a cryptographic hash function using supersingular elliptic curves. More specifically, its preimage resistance relies on the difficulty of finding an isogeny between two given (supersingular) elliptic curves over $\mathbb{F}_{p^2}$. In this context, our algorithm directly yields the fastest known quantum attack in $\tilde{O}(p^{1/4})$.

7 Example

For the purposes of validating our algorithm, we implemented Algorithm 4 in the MAGMA Computational Algebra System [1, 20] (Algorithm 4 being the only algorithm in this work which can be implemented on a classical computer). We present an example calculation here.

Let $p = 101$, $\ell = 83$, and $\mathfrak{a} = (\ell, 27+\pi_p)$ (corresponding to the quadratic form $83x^2 - 54xy + 10y^2$). Let E be the curve $y^2 = x^3 + 77x + 42$ over $\mathbb{F}_p$. This example was chosen to be small enough to allow direct calculation of the answer, in order to check the correctness of our work. Using the division polynomial-based method of [4, Section 3.2], we find that the 83-isogenous curve corresponding to $\mathfrak{a}$ is $E' : y^2 = x^3 + 40x + 65$, having j-invariant $j(E') = 66$. In order to redo the calculation according to the method specified in Algorithm 4, we used Sutherland's `smoothrelation` program [27] to find the relation

$$\mathfrak{p}_{83} = \bar{\mathfrak{p}}_5^{25}\bar{\mathfrak{p}}_7^{16}\bar{\mathfrak{p}}_{11}^{3}.$$

We then calculated the chain of isogenies corresponding to the right side of the equation. This calculation results in the curve $E'' : y^2 = x^3 + 44x + 24$ which has the same j-invariant as E'.

8 Conclusion

We described the fastest known quantum method for computing isogenies between supersingular curves, both for the general case and when the curves are

defined over $\mathbb{F}_p$. In the general case, the quantum complexity of our attack is $\tilde{O}(p^{1/4})$. Some cryptographic applications of our work include a faster quantum preimage attack against the Charles-Goren-Lauter hash function, and a recommendation to avoid using base curves defined over $\mathbb{F}_p$ in De Feo-Jao-Plût type schemes.

Acknowledgments

The first author thanks Luca De Feo for helpful discussions on the quantum safe protocols based on isogenies between supersingular curves described in [10]. This work was supported by an NSERC Discovery Grant.

References

1. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. the user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
2. M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortschritte Der Physik*, 46:493–505, 1998.
3. R. Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, 1(3):269–273, 2009.
4. R. Bröker, D. Xavier Charles, and K. Lauter. Evaluating large degree isogenies and applications to pairing based cryptography. In S. Galbraith and K. Paterson, editors, *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, Lecture Notes in Computer Science, pages 100–112. Springer, 2008.
5. D. Charles, K. Lauter, and E. Goren. Cryptographic hash functions from expander graphs. *Jornal of cryptology*, 22:93–113, 2009.
6. A. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1 – 29, 2013.
7. J.-M. Couveignes. Hard homgeneous spaces. http://eprint.iacr.org/2006/291.
8. D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.
9. C. Delfs and S. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. To appear in the proceedings of the 11th Algorithmic Nnumber Theory Symposium (ANTS XI).
10. L. De Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology (to appear)*, 2014. `http://eprint.iacr.org/2011/506`.
11. S. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1 1999.
12. S. Galbraith and A. Stolbunov. Improved algorithm for the isogeny problem for ordinary elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 24(2):107–131, 2013.
13. L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing*, STOC '96, pages 212–219, New York, NY, USA, 1996. ACM.
14. E. Littlewood J.˙On the class number of the corpus $p(\sqrt{k})$. *Proc. London Math.Soc*, 27:358–372, 1928.

15. D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Proceedings of the 4th International Conference on Post-Quantum Cryptography*, PQCrypto'11, pages 19–34, Berlin, Heidelberg, 2011. Springer-Verlag.
16. D. Jao, S. D. Miller, and R. Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log? In *Advances in cryptology—ASIACRYPT 2005*, volume 3788 of *Lecture Notes in Computer Science*, pages 21–40. Springer, Berlin, 2005.
17. D. Jao, S. D. Miller, and R. Venkatesan. Expander graphs based on GRH with an application to elliptic curve cryptography. *J. Number Theory*, 129(6):1491–1504, 2009.
18. D. Jao and V. Soukharev. Isogeny-based quantum-resistant undeniable signatures. In Michele Mosca, editor, *Post-Quantum Cryptography—6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1–3, 2013. Proceedings*, volume 8772 of *Lecture Notes in Computer Science*, pages 160–179. Springer, 2014.
19. G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.
20. MAGMA Computational Algebra System. `http://magma.maths.usyd.edu.au/`.
21. O. Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. arXiv:quant-ph/0406151.
22. A. Rostovtsev and A. Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006.
23. R. Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7:219–254, 1995.
24. T. Seiichiro. Claw finding algorithms using quantum walk. *Theoretical Computer Science*, 410(50):5285 – 5297, 2009. Mathematical Foundations of Computer Science (MFCS 2007).
25. J. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate texts in Mathematics*. Springer-Verlag, 1992.
26. A. Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Adv. in Math. of Comm.*, 4(2):215–235, 2010.
27. A. Sutherland. `smoothrelation`. Available at `http://math.mit.edu/~drew/smooth_relation_v1.2.tar`.
28. J. Tate. Endomoprhisms of abelian varieties over finite fields. *Inventiones Mathematica*, 2:134–144, 1966.
29. J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.