Isogenies of elliptic curves over finite fields and genus theory

Jana Sotáková

QuSoft/University of Amsterdam

June 8, 2020

Abstract

This is a written exposition [1] of our article [3] based on my talk at the Linfoot number theory seminar in Bristol on June 3rd, 2020.

Contents

1 Elliptic curves and isogenies

Recall that an elliptic curve E over a finite field $\mathbb{F}_q$ (of characteristic > 3) is an algebraic group given by an equation

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q,\, 4a^3 + 27b^2 \neq 0$$

That is, it is an algebraic variety that is also an (abelian) group, and the group law is given by geometric formulae: the chord-and-tangent law.

When we talk about points of E, we mean pairs $P = (x_P, y_P) \in (\overline{\mathbb{F}}_q)^2$ satisfying the defining equation and the point at infinity O_E. However, in this setting, we are mostly concerned with rational points $E(\mathbb{F}_q)$: points of E with both coordinates in $\mathbb{F}_q$.

An isogeny (defined over $\mathbb{F}_q$) between elliptic curves $E, E'/\mathbb{F}_q$ is a rational map $\varphi : E \to E'$

$$\varphi : \quad (x, y) \mapsto (f(x, y), g(x, y))$$

for some $f, g \in \mathbb{F}_q(x, y)$ which is also a group homomorphism. In short, it is a morphism of algebraic groups.

[1] Please contact me with any comments or remarks at ja.sotakova@gmail.com.

An important example is the multiplication by m: denoted $[m] : E \to E$ and defined as

$$P \mapsto [m]P.$$

As the group law is given algebraically, it is easily seen that $[m]$ is indeed an isogeny. It is possible to write down the exact formulae for $[m]$, depending only on the coefficients a, b.

We can compose isogenies as we can compose rational maps, but we can also add isogenies using the group law of elliptic curves. With addition and composition as multiplication, the endomorphisms of E form a ring, denoted $\mathrm{End}(E)$.

All non-zero isogenies have a finite kernel, for instance,

$$\ker([m]) = E[m] \qquad \text{subgroup of points of order } m$$

Note that even though $[m]$ is always a rational isogeny, the m-torsion points can be defined over an extension field. As abelian groups, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Conversely, from any finite subgroup $H \subset E$ we can construct an isogeny

$$\varphi : E \to E/H \qquad \ker \varphi = H$$

Then the isogeny φ can be defined over $\mathbb{F}_q$ if and only if the group H can be defined over H. Note that this does not imply that all the points of H have to be rational points. Also, the isogeny is only defined up to postcomposing with automorphism.

The degree of a separable isogeny $\varphi : E \to E'$ is the size of the kernel:

$$\deg \varphi = \# ker(\varphi)$$

There is essentially only one exception to this rule: the inseparable Frobenius endomorphism

$$\pi : (x, y) \mapsto (x^q, y^q)$$

has degree q but kernel $\ker \pi = \{O_E\}$. However, any inseparable isogeny is a composition of the Frobenius with a separable isogeny.

To sum up: isogenies are the group homomorphisms of elliptic curves and have essentially the same properties as group homomorphisms of abelian groups. Moreover, the finiteness of the kernel is forced on us by geometry and the degree map is the correct notion of size.

2 Isogeny-based cryptography

In isogeny-based cryptography, elliptic curves are the public keys and isogenies are the secret. Namely, from a chosen starting curve $E_0/\mathbb{F}_q$ (which is a public parameter), construct some secret isogeny

$$\varphi : E_0 \to E.$$

- E is your public key: everyone can contact you using the public data and your public key E,
- the isogeny φ is your secret key: you are the only one who knows φ, nobody should be able to impersonate you without knowing φ.

Main problem to break in isogeny-based cryptography: Given two elliptic curves $E_0, E/\mathbb{F}_q$, find an isogeny between E_0 and E.

This is a necessary hard problem, because in this (naive) setting, it corresponds exactly to recovering the secret keys from public keys. The hardness of this problem does not imply the security of the cryptosystem, though. In particular, we will show how gaining ‘one bit’ of information about the secret key still allows us to break the DDH assumption in some settings.

Depending on the setting, we may be asked to find an isogeny of a particular degree (e.g. a power of 2 or 3 in SIKE, or of a smooth degree in CSIDH), with prescribed values (in SIKE, images of certain torsion points are a part of the public key). But often, any isogeny will do.

3 Elliptic curves with complex multiplication

Let E be an elliptic curve over $\mathbb{F}_q$. Then the number of rational points is given by

$$\#E(\mathbb{F}_q) = q + 1 - t, \qquad |t| \leq 2\sqrt{q},$$

where $|t|$ is bounded by the Hasse-Weil bound.

The integer t is the trace of the Frobenius: the endomorphism π satisfies

$$\pi^2 - t\pi + q = 0 \qquad \text{in } \mathrm{End}(E),$$

and note that if $f(x) = x^2 - tx + q$ is the characteristic polynomial of π (acting on the ℓ-torsion groups $E[\ell]$ for any ℓ, for instance), then

$$\#E(\mathbb{F}_q) = q + 1 - t = f(1).$$

Moreover, the number of points over an extension field is given by the following relation with the polynomial $L(x) = x^2 f(1/x) = 1 - tx + qx^2$:

$$\frac{1 - tx + qx^2}{(1-x)(1-qx)} = \sum_{n=1}^{\infty} \#E(\mathbb{F}_q^n)\frac{x^n}{n}.$$

From the Hasse-Weil bound we note that the discriminant of $\mathrm{disc}\, f = \Delta_\pi = t^2 - 4q \leq 0$, and if $\Delta_\pi \neq 0$, then $\mathbb{Z}[\pi]$ is an **order in an imaginary quadratic field** $\mathbb{Q}(\sqrt{\Delta_\pi})$.

The case $\Delta_\pi = 0$ corresponds to $t = \pm 2\sqrt{q}$ and this can only happen for supersingular curves defined over even degree extensions of $\mathbb{F}_p$. Moreover, in this case, the endomorphism ring is a maximal order in a quaternion algebra. Such is the setting for the SIDH/SIKE protocols.

If the discriminant $\Delta_\pi \neq 0$, then for all the endomorphisms of E which are defined over $\mathbb{F}_q$, that is, the ring $\mathrm{End}_{\mathbb{F}_q}(E)$, we have the following inclusions:

$$\mathbb{Z}[\pi] \subset \mathrm{End}_{\mathbb{F}_q}(E) \subset \mathcal{O}_K \subset \mathbb{Q}(\sqrt{\Delta_\pi})$$

From now on, we will be in this case:

$$\mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O} \quad \text{is an order in an imaginary quadratic field}$$

3.1 From ideals to isogenies

Recall the notation: E is an elliptic curve over $\mathbb{F}_q$ with $q + 1 - t$ points, $t^2 - 4q = \Delta_\pi$ and we have the following inclusions $\mathbb{Z}[\pi] \subset \mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{\Delta_\pi})$.

For any ideal $\mathfrak{a} \subset \mathcal{O}$ we can produce a finite subgroup

$$E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \ker \alpha,$$

by intersecting all the kernels of endomorphisms in the ideal $\mathfrak{a}$.

Example: consider the ideal $(m, \pi - 1) \subset \mathcal{O}$. It is enough to compute the intersection of the kernels of the generators, that is, $E[(m, \pi - 1)] = \ker[m] \cap \ker(\pi - 1)$.

The kernel $\ker[m] = E[m]$ is the subgroup of points of order dividing m. The group $\ker(\pi - 1) = E[\pi - 1]$ is the subgroup on which π acts like identity: the subgroup of points (x, y) such that $(x, y) = (x^q, y^q)$. But this means that $x, y \in \mathbb{F}_q$. So we get

$$E[\pi - 1] = E(\mathbb{F}_q)$$

Finally, $E[(m, \pi - 1)] = E[m] \cap E(\mathbb{F}_q) = E(\mathbb{F}_q)[m]$ is the m-torsion of the group $E(\mathbb{F}_q)$, which can be any subset of $\subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Assume further that $\mathfrak{a}$ is an invertible ideal. From the finite subgroup $E[\mathfrak{a}]$, we can compute an isogeny

$$\varphi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}] \qquad \ker \varphi_{\mathfrak{a}} = E[\mathfrak{a}].$$

Then the degree turns out to be exactly the norm:

$$\varphi_{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})$$

Moreover, if $\mathfrak{a}$ is invertible, then $E/E[\mathfrak{a}]$ has the same endomorphism ring $\mathcal{O}$ and trace t. And if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same class in $\mathrm{cl}(\mathcal{O})$, then we end up with $\mathbb{F}_q$-isomorphic curves:

$$E/E[\mathfrak{a}] \cong_{\mathbb{F}_q} E/E[\mathfrak{b}].$$

This leads us to consider the set of elliptic curves of fixed endomorphism ring and trace, up to $\mathbb{F}_q$-isomorphism:

$$\mathcal{E}\!\ell\!\ell_q(\mathcal{O}, t) = \{\text{ elliptic curves } E/\mathbb{F}_q \mid \mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O} \text{ and } \mathrm{tr}\, \pi = t\,\}/ \cong_{\mathbb{F}_q}.$$

Theorem 3.1 ('Main theorem of complex multiplication')**.** *The mapping*

$$\begin{aligned} \mathrm{cl}(\mathcal{O}) \times \mathcal{E}\!\ell\!\ell(\mathcal{O}, t) &\to \mathcal{E}\!\ell\!\ell(\mathcal{O}, t) \\ ([\mathfrak{a}], E) &\mapsto [\mathfrak{a}] \star E = E/E[\mathfrak{a}] \end{aligned}$$

(where $\mathfrak{a}$ is any representative of $[\mathfrak{a}]$) is a free and transitive group action.

4 Commutative isogeny-based cryptography

The action of $\mathrm{cl}(\mathcal{O})$ on $\mathcal{E}\!\ell\!\ell_q(\mathcal{O}, t)$ is free and transitive:

- every two elliptic curves $E_0, E \in \mathcal{E}\!\ell\!\ell_q(\mathcal{O}, t)$ are connected by a unique ideal class $[\mathfrak{a}]$:

$$E = [\mathfrak{a}] \star E_0$$

The secret isogeny $\phi : E_0 \to E$ is obtained by the group action

$$E_0 \to E = [\mathfrak{a}] \star E_0.$$

The class group action allows us to transport the structure from the group $\mathrm{cl}(\mathcal{O})$ to the set $\mathcal{E}\!\ell\!\ell_q(\mathcal{O}, t)$. While abelian groups are susceptible to the Shor's algorithm for computing discrete logarithms (and thus computing secret keys from public keys), it is assumed that the group action hides enough of the structure of $cl(\mathcal{O})$ that it is no longer possible to apply Shor's algorithm.

The problem of revealing the secret class $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$ from the two elliptic curves E_0, E is called the vectorization problem (analogous finding a vector connecting two points in an affine space) or the group action inverse problem (GAIP).

We will show that, surprisingly, the group action does not hide all the structure of $\mathrm{cl}(\mathcal{O})$. This will not break vectorization/GAIP, but a related computational assumption.

For concreteness, we dicuss the specific choices of different proposals in this area.

Setting: Choose q and t and $\mathcal{O}$ and a starting curve $E_0 \in \mathcal{E}\!\ell\!\ell_q(\mathcal{O}, t)$. Secret keys: choose a random class $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$; public key: compute

$$E = [\mathfrak{a}] \star E_0.$$

- Couveignes [4] and Rostovstev and Stolbunov [7] allow ordinary elliptic curves over any $\mathbb{F}_q$, any t and $\mathcal{O}$. This leads to an extremely inefficient protocol.
- de Feo, Kieffer and Smith [5] use ordinary elliptic curves over a prime field $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p+1-t$ divisible by lots of small primes (for efficiency). However, it is not easy to find suitable parameters.

- Castryck, Lange, Martindale, Panny, and Renes in CSIDH [2] use supersingular elliptic curves ($t = 0$) over $\mathbb{F}_p$ with $p \equiv 3 \mod 8$, order $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ and $\#E(\mathbb{F}_p) = p + 1$ divisible by lots of small primes and obtain a fairly efficient scheme.

- Cstryck and Decru in CSURF [1] and also Fan, Tian, Li, and Xu [6] use supersingular elliptic curves over $\mathbb{F}_p$ with $p \equiv 7 \mod 8$, order $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\#E(\mathbb{F}_p) = p+1$ divisible by lots of small primes. This results in some gains in performance over CSIDH.

5 How do we study isogenies?

We have two elliptic curves which are isogenous via an (unknown) isogeny $\varphi : E \to E'$.

To obtain information about the degree of φ, we use pairings:

The (reduced) Tate pairing (assume that $\mu_m \subset \mathbb{F}_q$):

$$\begin{tikzcd}
T_m : & E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) \arrow[r] & \mu_m \subset \mathbb{F}_q \\
& (P, Q) \arrow[r, mapsto] & T_m(P, Q)
\end{tikzcd}$$

is a non-degenerate bilinear pairing which is compatible with isogenies as follows:

$$T_m(\varphi(P), \varphi(Q)) = T_m(P, Q)^{\deg(\varphi)}.$$

Since the pairings are always m-th roots of unity, whenever they are non-trivial we can compare the exponents and obtain $\deg \varphi \bmod m$. Unlike the Weil-pairing, there can be non-trivial self-pairings $T_m(P, P) \neq 1$. So we only need to find an image $\varphi(P)$ for a point $P \in E(\mathbb{F}_q)[m]$ to be able to reveal the degree $\deg \varphi \bmod m$.

Obstructions: we do not know anything about the secret isogeny $\varphi : E \to E'$.

1. By rationality, we note that
$$\varphi(E(\mathbb{F}_q)[m]) \subset E'(\mathbb{F}_q)[m]$$
but we cannot pinpoint the exact image of a single point.

Fix 1 Look for $P \in E$ and $P' \in E'$ with $\varphi(P) \in \langle P' \rangle$. This is easier to arrange but we will lose information: we will only be able to conclude whether $\deg \varphi$ is a square $\pmod m$ or not.

2. There are infinitely many such isogenies: for any representative $\mathfrak{a}$ of $[\mathfrak{a}]$ there is an isogeny $\varphi_{\mathfrak{a}} : E \to E'$. The degree of the isogeny $\varphi_{\mathfrak{a}}$ is $\mathrm{N}(()\mathfrak{a})$.

Fix 2 If we can conclude whether $\deg \varphi$ is a square $\mathrm{mod} m$ or not, since we do not get to choose one specific isogeny, this answer needs to be the same for every isogeny possible. In particular, the answer is the same for all ideals $\mathfrak{a} \in [\mathfrak{a}]$. Moreover, since degrees are multiplicative, we would obtain a (quadratic) character of $\mathrm{cl}(\mathcal{O})$. Genus theory supplies values of m such that $[\mathfrak{a}] \mapsto \left(\frac{\mathrm{N}(\mathfrak{a})}{m}\right)$ is a quadratic character on $\mathrm{cl}(\mathcal{O})$.

First we explain why we lose information with Fix 1. Suppose $P \in E(\mathbb{F}_q)[m]$ and $P' \in E'(\mathbb{F}_q)[m]$ with $\varphi(P) \in \langle P' \rangle$, that is, $\varphi(P) = kP'$ for some k. Assume also $T_m(P, P) \neq 1$ and m odd prime.

Then we can compute
$$T_m(\varphi(P), \varphi(P)) = T_m(P, P)^{\deg(\varphi)}$$
$$T_m(\varphi(P), \varphi(P)) = T_m(kP', kP') = T_m(P', P')^{k^2}$$

And conclude
$$T_m(P, P)^{\deg(\varphi)} = T_m(P', P')^{k^2}$$

But $T_m(P,P) = \zeta_m$ and $T_m(P',P') = \zeta'_m$ are m-th roots of unity, so

$$\zeta'_m = \zeta_m^e$$

for some integer e and so

$$\deg(\varphi) \equiv k^2 \cdot e \pmod{m}$$

for the unknown k. Since we can compute e but we do not know k, we can determine $\deg\varphi$ only up to squares $\bmod m$.

5.1 Fix 1

How do we find $P \in E(\mathbb{F}_q)[m]$ and $P' \in E'(\mathbb{F}_q)[m]$ with $\varphi(P) \in \langle P' \rangle$?

This is the case when $\mathrm{val}_m(\#E(\mathbb{F}_q)) = 1$: since m^1 is the only power dividing $\#E(\mathbb{F}_q)$ (and since $E'(\mathbb{F}_q)$) has to have the same number of points, by Tate's theorem), the $\mathbb{F}_q$-rational m-torsion is:

$$E(\mathbb{F}_q)[m] \cong \mathbb{Z}/m\mathbb{Z}, \qquad \text{and} \qquad E'(\mathbb{F}_q)[m] \cong \mathbb{Z}/m\mathbb{Z},$$

and we've already noted for any isogeny φ with $\gcd(\deg\varphi, m) = 1$:

$$\varphi(E(\mathbb{F}_q)[m]) \subset E'(\mathbb{F}_q)[m] = \langle P' \rangle.$$

The reduced Tate pairing is non-trivial (assume $\mu_m \subset \mathbb{F}_q$):

$$T_m : E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) \to \mu_m \subset \mathbb{F}_q$$

and $E(\mathbb{F}_q)[m]$ is a set of representatives of $E(\mathbb{F}_q)/mE(\mathbb{F}_q)$.

So under conditions $m|q-1$ and $\mathrm{val}_m(\#E(\mathbb{F}_q)) = 1$ we succeed.

In the paper we argue that these conditions are not necessary and deal with all possible cases:

- if there is no m-torsion or $\mu_m \not\subset \mathbb{F}_q$, then we move to an extension of the field $\mathbb{F}_q$;
- using walks on isogeny-volcanoes, we can control the m-torsion and so we can assume that $E(\mathbb{F}_q)[m^\infty]$ is cyclic, generated by a point Q;
- it is no longer enough to consider self-pairings, instead, we use points $P \in E(\mathbb{F}_q)[m]$ and $Q \in E(\mathbb{F}_q)[m^\nu]$ such that $m^{\nu-1}Q = P$.

5.2 How to do Fix 2

Recall the problem: There are infinitely many isogenies

$$\varphi : E \to E' = [\mathfrak{a}] \star E,$$

one for each representative $\mathfrak{a}$ of the ideal class $[\mathfrak{a}]$, the degrees of the isogenies are the norms $\mathrm{N}(\mathfrak{a})$.

Using the m-th Tate pairing evaluated at special points, we hope to determine whether $\deg\varphi = \mathrm{N}(()\mathfrak{a})$ is a square $\bmod m$. This answer has to be the same for all isogenies, so the answer is a property of $[\mathfrak{a}]$ and gives a quadratic character on the class group $\mathrm{cl}(\mathcal{O})$. But quadratic characters are described by genus theory.

Theorem 5.1 (Genus theory)**.** *Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field. Write $\Delta = -2^a \cdot b$ and $b = \prod_{i=1}^r m_i^{e_i}$ for distinct odd primes m_i. All quadratic characters of $\mathrm{cl}(\mathcal{O})$ are given by (products of):*

- *for every odd prime $m|\Delta$:*

$$\chi_m : \mathrm{cl}(\mathcal{O}) \to \{\pm 1\} \qquad [\mathfrak{a}] \mapsto \left(\frac{\mathrm{N}(\mathfrak{a})}{m}\right)$$

where $\mathfrak{a}$ is any representative of $[\mathfrak{a}]$ satisfying $\gcd(m, \mathrm{N}(\mathfrak{a})) = 1$.

- *Define*
$$\delta : \mathfrak{a} \mapsto (-1)^{(\mathrm{N}(\mathfrak{a})-1)/2} \qquad \varepsilon : \mathfrak{a} \mapsto (-1)^{(\mathrm{N}(\mathfrak{a})^2-1)/8}$$
if $\Delta = -4n$, extend the set of characters by
  1. *δ if $n \equiv 1, 4, 5 \pmod 8$,*
  2. *ε if $n \equiv 6 \pmod 8$,*
  3. *$\delta\varepsilon$ if $n \equiv 2 \pmod 8$.*

There is one relation between these characters:

$$\chi_{m_1}^{e_1} \cdot \dots \cdot \chi_r^{e_r} \cdot \delta^{\frac{b+1}{2} \bmod 2} \cdot \varepsilon^{a \bmod 2} \equiv 1 \quad \textit{on} \ \ \mathrm{cl}(\mathcal{O}).$$

6 Conclusions

We have elliptic curves $E, E' \in \mathcal{E}\ell\ell(\mathcal{O}, t)$ connected by a secret isogeny class $E' = [\mathfrak{a}] \star E$ for some $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$.

If we have for an odd prime $m|\Delta$:

- such that χ_m is non-trivial,

  whenever $\Delta \neq -m, -4m$ for a prime $m \equiv 3 \mod 4$,

- there is a pair of points $P \in E(\mathbb{F}_q)[m]$ and $P' \in E'(\mathbb{F}_q)[m]$ satisfying $P \mapsto kP'$,

  e.g. whenever $\mathrm{val}(\#E(\mathbb{F}_q)) = 1$,

- and the self-pairing $T_m(P, P) \neq 1$ is non-trivial,

  e.g. whenever $\mathrm{val}(\#E(\mathbb{F}_q)) = 1$ and $m|q-1$,

then we can compute
$$\chi_m([\mathfrak{a}]) = \left(\frac{\mathrm{N}(\mathfrak{a})}{m}\right)$$

just from the elliptic curves E and E': even though we need to find suitable torsion points, compute Tate pairings and compute a discrete logarithm on roots of unity, we are not using any information about the ideal class $[\mathfrak{a}]$ or even about the class group $\mathrm{cl}(\mathcal{O})$. The class group $\mathrm{cl}(\mathcal{O})$ can be completely unknown for us.

This result is surprising because the group action is supposed to hide the structure of the class group, but we are able to compute information about the group: genus theory characters allow us to compute the 2-torsion of the class group. Equivalently, we determine the coset in $\mathrm{cl}(\mathcal{O})/\,\mathrm{cl}(\mathcal{O})^2$ of the class $[\mathfrak{a}]$.

These computations cannot be used to attack the vectorization/GAIP problem, but they can be successfully used to attack schemes based on the Decisional Diffie-Hellman problem for the class group actions, e.g. [5]. The running time depends on m: it is in $O(m \cdot \mathrm{polylog}(p))$. The attack runs in polynomial time in $\log p$ in the following cases:

1. ordinary curves [4, 7, 5]: whenever $\#\,\mathrm{cl}(\mathcal{O})$ is even and there is a small odd divisor of $\mathrm{disc}(\mathcal{O})$, which is (heuristically) a density 1 set of orders $\mathcal{O}$. In particular, it works for all setups proposed in [5],

2. supersingular curves: whenever $p \equiv 1 \mod 4$. This is not the case for CSIDH [2] or CSURF [1, 6] (they use $p \equiv 3 \mod 4$).

References

[1] Wouter Castryck and Thomas Decru. Csidh on the surface. Cryptology ePrint Archive, Report 2019/1404, 2019.

[2] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Report 2018/383, 2018.

[3] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. Cryptology ePrint Archive, Report 2020/151, 2020.

[4] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006.

[5] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. Cryptology ePrint Archive, Report 2018/485, 2018.

[6] Xuejun Fan, Song Tian, Bao Li, and Xiu Xu. Csidh on other form of elliptic curves. Cryptology ePrint Archive, Report 2019/1417, 2019. https://eprint.iacr.org/2019/1417.

[7] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, April 2006.