Isogenies of elliptic curves over finite fields and genus theory

Jana Sotáková

QuSoft / University of Amsterdam

Joint work with Wouter Castryck and Frederik Vercauteren
Breaking the decisional Diffie-Hellman problem for class group actions using genus theory

https://eprint.iacr.org/2020/151

Elliptic curves and isogenies

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

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

Points of E: pairs $P = (x_P, y_P) \in (\overline{\mathbb{F}}_q)^2$ satisfying the equation and the point at infinity O_E.

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 $\varphi : E \to E'$

$$(x, y) \mapsto (f(x, y), g(x, y))$$

for some $f, g \in \mathbb{F}_q(x, y)$ which is also a group homomorphism.

Example: multiplication by m: denoted $[m] : E \to E$

$$P \mapsto [m]P$$

What else do we need to know about isogenies

E elliptic curve over $\mathbb{F}_q$. We can add isogenies, compose isogenies.
We have an endomorphism ring $\mathrm{End}(E)$.

Isogenies have a finite kernel:

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

as abelian groups, $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

From any finite subgroup $H \subset E$ we can construct an isogeny

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

The degree of the isogeny φ is the size of the kernel:

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

Exception: the Frobenius endomorphism

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

has degree q but kernel $\ker \pi = \{O_E\}$.

‘Isogeny-based cryptography’

From a chosen starting curve $E_0/\mathbb{F}_q$, 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.

Depending on the setting: find isogeny of a specific degree, with prescribed values (say, $Q \mapsto Q'$), or any isogeny will do.

Elliptic curves with complex multiplication

Let E be an elliptic curve over $\mathbb{F}_q$. Then

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

This t is the trace of Frobenius: the endomorphism π satisfies

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

And since $\Delta_\pi = t^2 - 4q \leq 0$, then $\mathbb{Z}[\pi]$ is an **order in an imaginary quadratic field** $\mathbb{Q}(\sqrt{\Delta_\pi})$. (ignore the case $\Delta_\pi = 0$)

Fact: unless $\Delta_\pi = 0$, (happens for some cases of supersingular elliptic curves)

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

From now on, we will be in this case:

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

From ideals to isogenies

E elliptic curve over $\mathbb{F}_q$ with $q+1-t$ points, $t^2-4q=\Delta_\pi$,
$\mathbb{Z}[\pi] \subset \mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{\Delta_\pi})$.

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

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

Example: ideal $(m, \pi - 1) \subset \mathcal{O}$

We compute $E[(m, \pi-1)] = \ker[m] \cap \ker(\pi - 1)$.

Then $\ker[m] = E[m]$ 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 1 (identity):

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

So $E[(m, \pi-1)] = E[m] \cap E(\mathbb{F}_q) = E(\mathbb{F}_q)[m] \subset \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Constructing isogenies from the kernel

E elliptic curve over $\mathbb{F}_q$ with $q+1-t$ points, $t^2-4q=\Delta_\pi$,
$\mathbb{Z}[\pi] \subset \mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{\Delta_\pi})$, and $\mathfrak{a} \subset \mathcal{O}$ (invertible) ideal of $\mathcal{O}$.

Once we have the subgroup $E[\mathfrak{a}]$, we can compute an isogeny

$$\varphi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}] \qquad \ker\varphi_{\mathfrak{a}} = E[\mathfrak{a}], \quad \deg\varphi_{\mathfrak{a}} = \mathrm{norm}(\mathfrak{a})$$

Then $E/E[\mathfrak{a}]$ has the same endomorphism ring $\mathcal{O}$ and trace t.

Fact: if $\mathfrak{a}$ and $\mathfrak{b}$ are in the same class in $\mathrm{Cl}(\mathcal{O})$, then

$$E/E[\mathfrak{a}] \cong E/E[\mathfrak{b}]$$

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

Theorem ('Main theorem of complex multiplication')

The mapping

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

is a free and transitive group action.

Going back to our problem

E elliptic curve over $\mathbb{F}_q$ with $q+1-t$ points, $t^2-4q=\Delta_\pi$,
$\mathbb{Z}[\pi] \subset \mathrm{End}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{\Delta})$, and $\mathfrak{a} \subset \mathcal{O}$ (invertible) ideal of $\mathcal{O}$.
$\mathcal{E}\ell\ell_q(\mathcal{O},t) = \{$ elliptic curves $E/\mathbb{F}_q \mid \mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O}$ and $\mathrm{tr}\,\pi = t\,\}/\cong_{\mathbb{F}_q}$.

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

- every two elliptic curves $E, E' \in \mathcal{E}\ell\ell_q(\mathcal{O},t)$ are connected by a unique ideal class $[\mathfrak{a}]$: $\quad E' = [\mathfrak{a}] \star E$

Transport the structure from the group $\mathrm{Cl}(\mathcal{O})$ to the set $\mathcal{E}\ell\ell_q(\mathcal{O},t)$.

‘Commutative’ isogeny-based cryptography

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

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

Zoology of proposals

Setting: [C'06, RS'06, dFKS'18, CSIDH, CSURF]

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

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

- C'06, RS'06 allow ordinary elliptic curves over $\mathbb{F}_q$, any t and $\mathcal{O}$.
- dFKS'18 use ordinary elliptic curves over a prime field $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = q + 1 - t$ divisible by lots of small primes (for efficiency).
- CSIDH uses 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.
- CSURF uses 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.

How do we study isogenies?

Two elliptic curves isogenous via an (unknown) isogeny $\varphi : E \to E'$.

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

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

$$T_m : \quad E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) \longrightarrow \mu_m \subset \mathbb{F}_q$$
$$(P, Q) \longmapsto T_m(P, Q)$$

is a non-degenerate bilinear pairing with the following compatibility property:

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

There can be non-trivial self-pairings $T_m(P, P) \neq 1$;

We need to find an image $\varphi(P)$ for a point $P \in E(\mathbb{F}_q)[m]$ to be able to reveal the degree $\deg \varphi \pmod{m}$.

Will this work?

Assume $\gcd(\deg\varphi, m) = 1$ and m odd. If we know the image $\varphi(P) \in E'[m]$ of $P \in E[m]$, we can compare the m-th roots of unity $T_m(\varphi(P), \varphi(P)) = T_m(P, P)^{\deg(\varphi)}$ and obtain $\deg\varphi \mod m$.

We do not know 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 $\varphi(P) \in \langle P' \rangle$.

Can only 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 $\mathrm{norm}(\mathfrak{a})$.

Fix 2 Genus theory supplies values of m such that $[\mathfrak{a}] \mapsto \left(\frac{\mathrm{norm}(\mathfrak{a})}{m}\right)$ is a quadratic character on $\mathrm{Cl}(\mathcal{O})$.

Fix 1 - why only up to squares?

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

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

and so

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

for the unknown k.

How to do 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 $\mathrm{val}_m(\# E(\mathbb{F}_q)) = 1$:

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

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.

How to do Fix 2

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 $\mathrm{norm}(\mathfrak{a})$.

Using the m-th Tate pairing evaluated at special points, we hope to determine whether $\deg \varphi = \mathrm{norm}(\mathfrak{a})$ is a square $\bmod m$.

This answer has to be the same for all isogenies, so for all $\mathfrak{a} \in [\mathfrak{a}]$.

This gives a quadratic character on $\mathrm{Cl}(\mathcal{O})$.

But we know quadratic characters on $\mathrm{Cl}(\mathcal{O})$ thanks to genus theory!

Quadratic characters of the class group

Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field.
Write $\Delta = -2^a \cdot \prod_{i=1}^r m_i^{e_i}$ for distinct odd primes m_i.

Theorem (Genus theory)

All quadratic characters of $\mathrm{Cl}(\mathcal{O})$ *are given by (products of):*

- *for every odd prime* m_i*:*

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

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

- *Define* $\quad \delta : \mathfrak{a} \mapsto (-1)^{(\mathrm{norm}(\mathfrak{a})-1)/2} \qquad \varepsilon : \mathfrak{a} \mapsto (-1)^{(\mathrm{norm}(\mathfrak{a})^2-1)/8}$

  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:

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

Step back

$E, E' \in \mathcal{E}\ell\ell(\mathcal{O}, t)$ be elliptic curves with $E' = [\mathfrak{a}] \star E$.

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

$$\chi_m([\mathfrak{a}]) = \left(\frac{\mathrm{norm}(\mathfrak{a})}{m} \right)$$

just from the elliptic curves E and E'.

Most general statement

We can compute the quadratic characters $\chi_m([\mathfrak{a}])$ directly from elliptic curves $E, E' = [\mathfrak{a}] \star E$.

This can be used to attack the Decisional Diffie-Hellman problem for the class group actions.

The running time depends on m: it is in $O(m \cdot \mathrm{polylog}(p))$. So when does the attack run in polynomial time in $\log p$?

This attack works

1. for ordinary curves [C'06, RS'06, dFKS'18]: 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 praticular, it works for all setups proposed in [DKS'18],
2. for supersingular curves: whenever $p \equiv 1 \mod 4$. This is not the case for CSIDH or CSURF (they use $p \equiv 3 \mod 4$).

Thank you!

Breaking the decisional Diffie-Hellman problem for class group actions using genus theory

Wouter Castryck and Jana Sotáková and Frederik Vercauteren

https://eprint.iacr.org/2020/151