Isogeny-basd cryptography IV

Math details

Tanja Lange
(with lots of slides by Lorenz Panny)

Eindhoven University of Technology

SAC – Post-quantum cryptography

Isogenies and endomorphism rings

An isogeny of elliptic curves is a non-zero map $\varphi : E \to E'$

- given by rational functions
- that is a group homomorphism.

The degree d of a separable isogeny is the size of its kernel $d = \ker(\varphi)$.

For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.

The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

An endomorphism is an isogeny from a curve E to itself.

The set of endomorphisms forms a ring $\mathrm{End}(E)$ under $+$ and $\circ$.

The ring of k-rational endomorphisms of E/k is denoted $\mathrm{End}_k(E)$.

Elliptic curves over finite fields

We now focus on curves over finite fields $\mathbb{F}_q, q = p^k$.

There are only finitely many pairs (x, y) that can satisfy the curve equation, thus there are only finitely many points on $E(\mathbb{F}_q)$.

Elliptic curves over finite fields

We now focus on curves over finite fields $\mathbb{F}_q, q = p^k$.

There are only finitely many pairs (x, y) that can satisfy the curve equation, thus there are only finitely many points on $E(\mathbb{F}_q)$.

Hasse Interval:

$$\#E(\mathbb{F}_q) \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

Elliptic curves over finite fields

We now focus on curves over finite fields $\mathbb{F}_q, q = p^k$.

There are only finitely many pairs (x, y) that can satisfy the curve equation, thus there are only finitely many points on $E(\mathbb{F}_q)$.

Hasse Interval:

$$\#E(\mathbb{F}_q) \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

The following are equivalent definitions of *supersingular* curves:

- $\#E(\mathbb{F}_q) = q + 1 - t$ with $t \equiv 0 \bmod p$.
- $E[p] = \{\infty\}$.
  Note that $E[n] = \{P \in E(\overline{\mathbb{F}_p}) \mid nP = \infty\}$.

Elliptic curves over finite fields

We now focus on curves over finite fields $\mathbb{F}_q, q = p^k$.

There are only finitely many pairs (x, y) that can satisfy the curve equation, thus there are only finitely many points on $E(\mathbb{F}_q)$.

Hasse Interval:

$$\#E(\mathbb{F}_q) \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

The following are equivalent definitions of *supersingular* curves:

- $\#E(\mathbb{F}_q) = q + 1 - t$ with $t \equiv 0 \bmod p$.
- $E[p] = \{\infty\}$.
  Note that $E[n] = \{P \in E(\overline{\mathbb{F}_p}) \mid nP = \infty\}$.

For $p > 3$ the only $t \in [-2\sqrt{p}, 2\sqrt{p}]$ with $t \equiv 0 \bmod p$ is $t = 0$.

Elliptic curves over finite fields

We now focus on curves over finite fields $\mathbb{F}_q, q = p^k$.

There are only finitely many pairs (x, y) that can satisfy the curve equation, thus there are only finitely many points on $E(\mathbb{F}_q)$.

Hasse Interval:

$$\#E(\mathbb{F}_q) \in [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

The following are equivalent definitions of *supersingular* curves:

- $\#E(\mathbb{F}_q) = q + 1 - t$ with $t \equiv 0 \bmod p$.
- $E[p] = \{\infty\}$.
  Note that $E[n] = \{P \in E(\overline{\mathbb{F}_p}) \mid nP = \infty\}$.

For $p > 3$ the only $t \in [-2\sqrt{p}, 2\sqrt{p}]$ with $t \equiv 0 \bmod p$ is $t = 0$.
Thus $\#E(\mathbb{F}_p) = p + 1$, $\#E(\mathbb{F}_{p^2}) \in \{(p-1)^2, p^2 + 1, (p+1)^2\}$ for supersingular curves and $p > 3$.

Quadratic twists

E'/k is a twist of elliptic curve E/k if E' is isomorphic to E over $\bar{k}$.

For $E : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$
$E' : -y^2 = x^3 + Ax^2 + x$ is isomorphic to E via

$$(x, y) \mapsto (x, \sqrt{-1}y).$$

This map is defined over $\mathbb{F}_{p^2}$, so this is a quadratic twist.

Quadratic twists

E'/k is a twist of elliptic curve E/k if E' is isomorphic to E over $\bar{k}$.

For $E : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$
$E' : -y^2 = x^3 + Ax^2 + x$ is isomorphic to E via

$$(x, y) \mapsto (x, \sqrt{-1}y).$$

This map is defined over $\mathbb{F}_{p^2}$, so this is a quadratic twist.

E' is not in Weierstrass form (does not have the right shape).
E' is isomorphic to $E'' : y^2 = x^3 - Ax^2 + x$ via $(x, y) \mapsto (-x, y)$ over $\mathbb{F}_p$.

Quadratic twists

E'/k is a twist of elliptic curve E/k if E' is isomorphic to E over $\bar{k}$.

For $E : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$
$E' : -y^2 = x^3 + Ax^2 + x$ is isomorphic to E via

$$(x, y) \mapsto (x, \sqrt{-1}y).$$

This map is defined over $\mathbb{F}_{p^2}$, so this is a quadratic twist.

E' is not in Weierstrass form (does not have the right shape).
E' is isomorphic to $E'' : y^2 = x^3 - Ax^2 + x$ via $(x, y) \mapsto (-x, y)$ over $\mathbb{F}_p$.

Each $x \in \mathbb{F}_p$ satisfies one of

- $x^3 + Ax^2 + x$ is a square in $\mathbb{F}_p$, thus there are two points $(x, \pm\sqrt{x^3 + Ax^2 + x})$ in $E(\mathbb{F}_p)$.
- $x^3 + Ax^2 + x$ is not a square in $\mathbb{F}_p$, thus there are two points $(x, \pm\sqrt{-(x^3 + Ax^2 + x)})$ in $E'(\mathbb{F}_p)$.
- $x^3 + Ax^2 + x = 0$, thus $(x, 0)$ is a point in $E(\mathbb{F}_p)$ and in $E'(\mathbb{F}_p)$.

Quadratic twists

E'/k is a twist of elliptic curve E/k if E' is isomorphic to E over $\bar{k}$.

For $E : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p \equiv 3 \bmod 4$
$E' : -y^2 = x^3 + Ax^2 + x$ is isomorphic to E via

$$(x, y) \mapsto (x, \sqrt{-1}y).$$

This map is defined over $\mathbb{F}_{p^2}$, so this is a quadratic twist.

E' is not in Weierstrass form (does not have the right shape).
E' is isomorphic to $E'' : y^2 = x^3 - Ax^2 + x$ via $(x, y) \mapsto (-x, y)$ over $\mathbb{F}_p$.

Each $x \in \mathbb{F}_p$ satisfies one of

- $x^3 + Ax^2 + x$ is a square in $\mathbb{F}_p$, thus there are two points $(x, \pm\sqrt{x^3 + Ax^2 + x})$ in $E(\mathbb{F}_p)$.
- $x^3 + Ax^2 + x$ is not a square in $\mathbb{F}_p$, thus there are two points $(x, \pm\sqrt{-(x^3 + Ax^2 + x)})$ in $E'(\mathbb{F}_p)$.
- $x^3 + Ax^2 + x = 0$, thus $(x, 0)$ is a point in $E(\mathbb{F}_p)$ and in $E'(\mathbb{F}_p)$.

$\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2p + 2$, thus
$\#E(\mathbb{F}_p) = p + 1 - t$ implies $\#E'(\mathbb{F}_p) = p + 1 + t$.

Isogenies and kernels

For any finite subgroup G of E, there exists a unique[1] separable isogeny $\varphi_G\colon E \to E'$ with kernel G.

The curve E' is called E/G. ($\approx$ quotient groups)

If G is defined over k, then φ_G and E/G are also defined over k.

[1](up to isomorphism of E')

Isogenies and kernels

For any finite subgroup G of E, there exists a unique[1] separable isogeny $\varphi_G \colon E \to E'$ with kernel G.

The curve E' is called E/G. ($\approx$ quotient groups)

If G is defined over k, then φ_G and E/G are also defined over k.

Vélu '71:
Formulas for computing E/G and evaluating φ_G at a point.

Complexity: $\Theta(\#G)$ $\rightsquigarrow$ only suitable for small degrees.

[1](up to isomorphism of E')

Isogenies and kernels

For any finite subgroup G of E, there exists a unique[1]
separable isogeny $\varphi_G \colon E \to E'$ with kernel G.

The curve E' is called E/G. ($\approx$ quotient groups)

If G is defined over k, then φ_G and E/G are also defined over k.

Vélu '71:
Formulas for computing E/G and evaluating φ_G at a point.

Complexity: $\Theta(\#G)$ $\rightsquigarrow$ only suitable for small degrees.

Vélu operates in the field where the points in G live.

$\rightsquigarrow$ need to make sure extensions stay small for desired G

$\rightsquigarrow$ this is why we use special p and curves with $p+1$ points!

Not all k-rational points of E/G are in the image of k-rational points on E; but $\#E(k) = \#((E/G)(k))$.

[1] (up to isomorphism of E')

Vélu's formulas

Let P have prime order ℓ on E_A.
For $1 \leq i < \ell$ let x_i be the x-coordinate of iP.
Let

$$\tau = \prod_{i=1}^{\ell-1} x_i, \quad \sigma = \sum_{i=1}^{\ell-1} \left(x_i - \frac{1}{x_i}\right), \quad f(x) = x \prod_{i=1}^{\ell-1} \frac{x x_i - 1}{x - x_i}.$$

Then the ℓ-isogeny with kernel $\langle P \rangle$ is given by

$$\varphi_\ell : E_A \to E_B, (x, y) \mapsto (f(x), c_0 y f'(x))$$

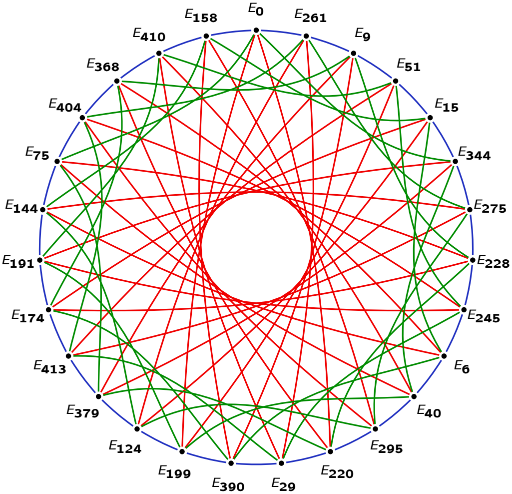
where $B = \tau(A - 3\sigma)$, and $c_0^2 = \tau$.

Main operation is to compute the x_i, just some elliptic-curve additions.
Note that $(\ell - i)P = -iP$ and both have the same x-coordinate.

Implementations often use projective formulas to avoid (or delay) inversions.

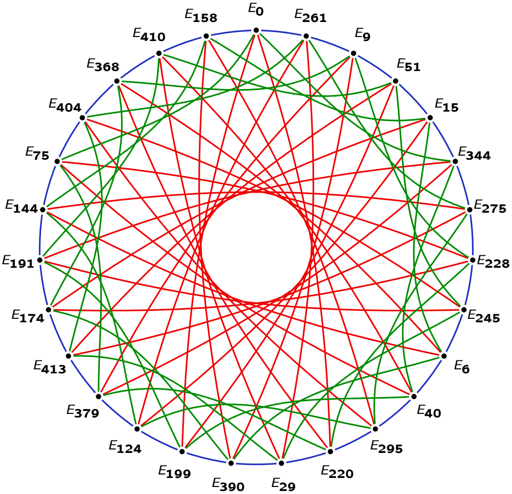
Montgomery curves have efficient arithmetic using only x-coordinates.

Graphs of elliptic curves



Nodes: Supersingular elliptic curves $E_A\colon y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.

Graphs of elliptic curves



Nodes: Supersingular elliptic curves $E_A\colon y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
Each E_A on the left has E_{-A} on the right.
Negative direction means: flip to twist, go positive direction, flip back.

Class groups for supersingular curves over $\mathbb{F}_p$

Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
All curves in X have $\mathbb{F}_p$-endomorphism ring $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Let π the Frobenius endomorphism. Ideal in $\mathcal{O}$ above ℓ_i.

$$\mathfrak{l}_i = (\ell_i, \pi - 1).$$

Moving $+$ in X with ℓ_i isogeny $\Longleftrightarrow$ action of $\mathfrak{l}_i$ on X.

Class groups for supersingular curves over $\mathbb{F}_p$

Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
All curves in X have $\mathbb{F}_p$-endomorphism ring $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Let π the Frobenius endomorphism. Ideal in $\mathcal{O}$ above ℓ_i.

$$\mathfrak{l}_i = (\ell_i, \pi - 1).$$

Moving $+$ in X with ℓ_i isogeny $\iff$ action of $\mathfrak{l}_i$ on X.

More precisely:
Subgroup corresponding to $\mathfrak{l}_i$ is $E[\mathfrak{l}_i] = E(\mathbb{F}_p)[\ell_i]$.
(Note that $\ker(\pi - 1)$ is just the $\mathbb{F}_p$-rational points!)

Subgroup corresponding to $\overline{\mathfrak{l}_i}$ is

$$E[\overline{\mathfrak{l}_i}] = \{P \in E[\ell_i] \mid \pi(P) = -P\}.$$

Class groups for supersingular curves over $\mathbb{F}_p$

Let $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
All curves in X have $\mathbb{F}_p$-endomorphism ring $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Let π the Frobenius endomorphism. Ideal in $\mathcal{O}$ above ℓ_i.

$$\mathfrak{l}_i = (\ell_i, \pi - 1).$$

Moving $+$ in X with ℓ_i isogeny $\Longleftrightarrow$ action of $\mathfrak{l}_i$ on X.

More precisely:
Subgroup corresponding to $\mathfrak{l}_i$ is $E[\mathfrak{l}_i] = E(\mathbb{F}_p)[\ell_i]$.
(Note that $\ker(\pi - 1)$ is just the $\mathbb{F}_p$-rational points!)

Subgroup corresponding to $\overline{\mathfrak{l}_i}$ is

$$E[\overline{\mathfrak{l}_i}] = \{P \in E[\ell_i] \mid \pi(P) = -P\}.$$

For supersingular Montgomery curves over $\mathbb{F}_p$, $p \equiv 3 \bmod 4$

$$E[\overline{\mathfrak{l}_i}] = \{(x, y) \in E[\ell_i] \mid x \in \mathbb{F}_p;\ y \notin \mathbb{F}_p\} \cup \{\infty\}.$$

Commutative group action

$\mathrm{cl}(\mathcal{O})$ acts on $X = \{y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ with $p+1$ points$\}$.
For most ideal classes the kernel is big and formulas are expensive to compute.

$$I = \mathfrak{l}_1^{10}\mathfrak{l}_2^{-7}\mathfrak{l}_3^{27}$$

is a "big" ideal, but we can compute the action iteratively.

$\mathrm{cl}(\mathcal{O})$ is commutative[2] so we get a commutative group action..

The choice for CSIDH:
Let $K = \{[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}] \mid (e_1, ..., e_n)$ is 'short'$\} \subseteq \mathrm{cl}(\mathcal{O})$.
The action of K on X is very efficient!
Pick K as the keyspace

[2]Important to use the $\mathbb{F}_p$-endomorphism ring.