SIKE - PQC based on isogenies

Simon Pohmann

University of Passau

July 23, 2021

Contents

Elliptic Curves

Let K be a field of characteristic $\neq 2, 3$.

Definition

A (possibly non-smooth) *elliptic curve* E is the zero set

$$\{(x, y) \mid F(x, y) = 0\} \subseteq \bar{K}^2$$

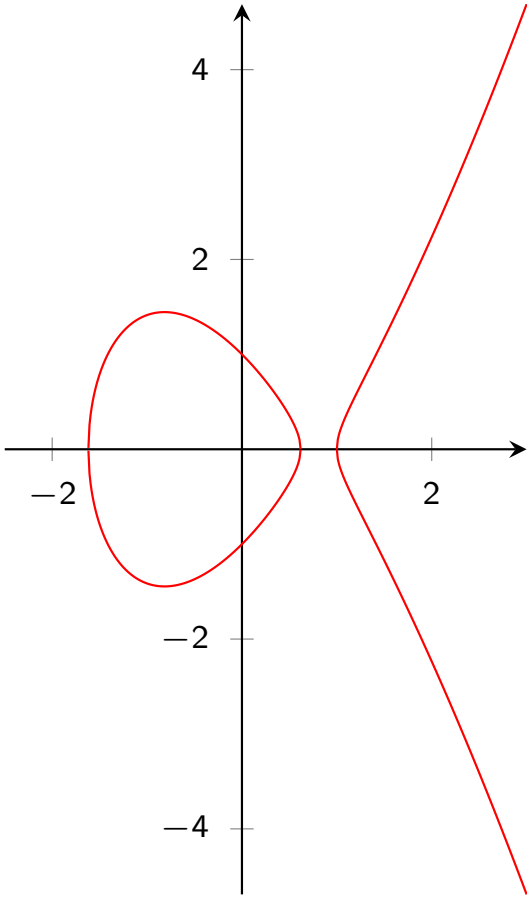
of some irreducible polynomial $F(x, y) = y^2 - x^3 - Ax - B \in K[x, y]$ together with a point $\mathcal{O} = \infty$ at infinity.

Definition

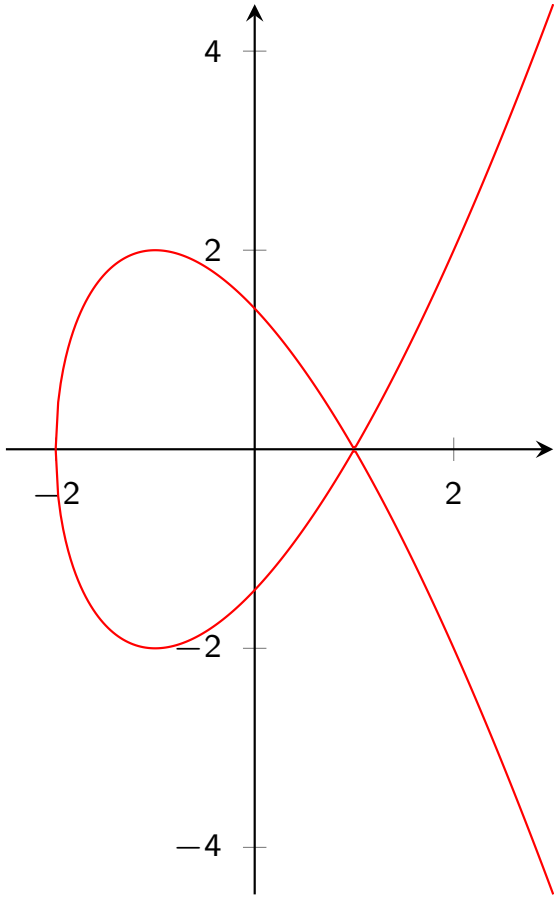
An elliptic curve $E : y^2 = x^3 + Ax + B$ is called smooth, if the *discriminant*

$$\Delta(E) := -16(27B^2 + 4A^3) \neq 0$$

Examples



points of $E : y^2 = x^3 - 2x + 1$ in $\mathbb{R}^2$



points of $E : y^2 = x^3 - 3x + 2$ in $\mathbb{R}^2$

Coordinate ring

Definition

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve. Then

$$K[E] := K[x, y]/(F), \quad F(x, y) = y^2 - x^3 - Ax - B$$

is the *coordinate ring* of E.

$f \in K[E]$ are the "polynomial functions" defined on E

Definition

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve. Then define the function field $K(E)$ as the quotient field of $K[E]$.

Rational functions - Example

Consider $E : y^2 = x^3 - x + 1$ and $f = \frac{(y-1)(x+1)}{x(x+1)} \in K(E)$.

We want to evaluate f.

- at $(1,1) \quad \Rightarrow \quad f(1,1) = 0$
- at $(-1,-1) \quad \Rightarrow \quad f(1,1) = 2$
- at $(0,1) \quad \Rightarrow \quad f(0,1) = -\frac{1}{2}$

However: $\frac{1}{x} \in K(E)$ cannot be defined at $(0,1)$.

Morphisms

Now we consider maps $E \to E'$ for elliptic curves E, E'.

$$\phi : E \to E', \quad (x, y) \mapsto (f(x, y),\ g(x, y)) \quad \text{for } f, g \in \bar{K}(E)$$

These are called *morphisms*.

- $f(x, y), g(x, y)$ must satisfy the equation of E' for all $(x, y) \in E$
  $\Rightarrow$ f, g satisfy the equation of E' in $K(E)$ (Hilbert's Nullstellensatz)
- Define $\mathcal{O} := (\frac{\neq 0}{0}, *) = (*, \frac{\neq 0}{0}) = (\frac{\neq 0}{0}, \frac{\neq 0}{0})$
  $\Rightarrow$ one can always define $f(x, y),\ g(x, y) \in E'$
- Write $\phi = [f, g]$
- What about $\phi(\mathcal{O})$?

Isogenies

Let E, E' be elliptic curves.

Definition

A morphism $E \to E'$ that maps $\mathcal{O}$ to $\mathcal{O}$ is called *isogeny*.

Definition

A bijective isogeny $E \to E'$ whose inverse is an isogeny is called *isomorphism*.

Isogenies - Example

Let $E : y^2 = x^3 - x + 1$ and $E' : y^2 = x^3 - 4x + 8$.

$$\phi : E \to E', \quad \mathcal{O} \mapsto \mathcal{O}, \ (x, y) \mapsto (2x, \sqrt{8}y)$$

Have

$$(\sqrt{8}y)^2 = (2x)^3 - 4(2x) + 8 \text{ in } K[E]$$

So ϕ is a well-defined isogeny.
Its inverse is

$$\phi^{-1} : E' \to E, \quad \mathcal{O} \mapsto \mathcal{O}, \ (x, y) \mapsto (\frac{1}{2}x, \frac{1}{\sqrt{8}}y)$$

So ϕ is an isomorphism.

j-invariant

Let $E : y^2 = x^3 - x + 1$ and $E' : y^2 = x^3 - 4x + 8$. Then

$$\phi : E \to E', \quad \mathcal{O} \mapsto \mathcal{O}, \ (x, y) \mapsto (2x, \sqrt{8}y)$$

is an isomorphism.
Recall the discriminant

$$\Delta(E) := -16(27B^2 + 4A^3) \neq 0$$

Definition

The *j-invariant* is

$$j(E) := \frac{(-48A)^3}{\Delta(E)}$$

$$j(E) = \frac{110592}{-368} = \frac{6912}{23}, \quad j(E') = \frac{7077888}{-23552} = \frac{6912}{23}$$

j-invariant

Definition

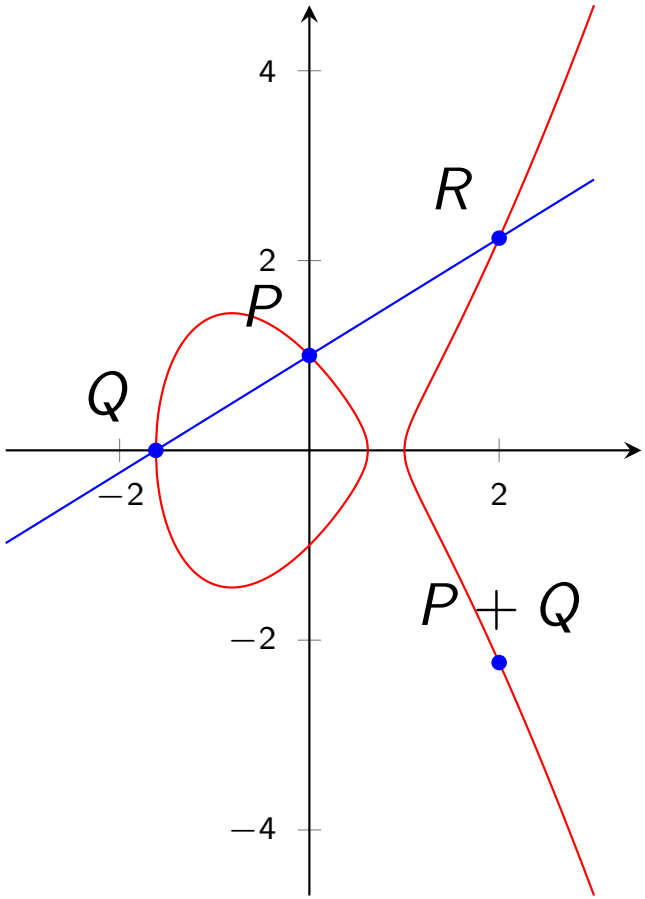
The *j-invariant* is

$$j(E) := \frac{(-48A)^3}{\Delta(E)} = \frac{(-48A)^3}{-16(27B^2 + 4A^3)}$$

Theorem

$E \cong E'$ if and only if $j(E) = j(E')$

Geometric Group Structure



Theorem

Each line meets E in exactly three points (with multiplicity)

Define $P +_{\text{geo}} Q$ by

- $L :=$ line through P, Q
  - If $P = Q$ use tangent
- $R :=$ third intersection point of L and E
- $P +_{\text{geo}} Q := -R$
  - $-(x, y) := (x, -y)$

Set $\mathcal{O} +_{\text{geo}} P = P +_{\text{geo}} \mathcal{O} = P$.

Algebraic Group Structure

From Cryptanalysis we know:

Theorem

The coordinate ring $K[E]$ is a Dedekind domain.

Theorem

There is a bijection

$$\rho : E \to \mathrm{Cl}(\bar{K}[E]), \quad \mathcal{O} \mapsto \overline{\bar{K}[E]},\ (\lambda, \mu) \mapsto \overline{\langle x - \lambda, y - \mu \rangle}$$

where $\mathrm{Cl}(\bar{K}[E])$ is the ideal class group of $\bar{K}[E]$.

Definition

Define $+_{\mathrm{alg}}$ on E by $P +_{\mathrm{alg}} Q = \rho^{-1}(\rho P \cdot \rho Q)$.

Rational Group Structure

Let $E : y^2 = x^3 + Ax + B$. For $P = (x_1, y_1),\ Q = (x_2, y_2) \neq -P$ define

$$\lambda := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + A}{2y_1} & \text{otherwise} \end{cases}$$

$$x_3 := -x_1 - x_2 + \lambda^2$$

$$y_3 := -y_1 + \lambda(x_1 - x_3)$$

$$P +_{\text{poly}} Q := (x_3, y_3)$$

Further $P +_{\text{poly}} (-P) := \mathcal{O}$.

Elliptic Curves as Groups

Theorem

Let E be an elliptic curve. Then $+ := +_{\text{geo}} = +_{\text{alg}} = +_{\text{poly}}$.

Corollary

Let E be an elliptic curve. Then

- *E with $+$ is a group*
- *E is abelian*
- *E has neutral element $\mathcal{O}$*

For fields $\bar{K}|L|K$ let $E(L) := E \cap L^2 \cup \{\mathcal{O}\}$ be the L-rational points.

Corollary

$E(L)$ is a subgroup of E

Isogenies

Let E, E' be elliptic curves. [Sil09] shows

Theorem

A nonconstant isogeny is a group homomorphism with finite kernel.

Theorem

Let $\Phi \leq E$ be a finite subgroup. Then there is a unique elliptic curve $\tilde{E}$ and a (separable) isogeny $\phi : E \to \tilde{E}$ with $\ker \phi = \Phi$ (up to isomorphism).

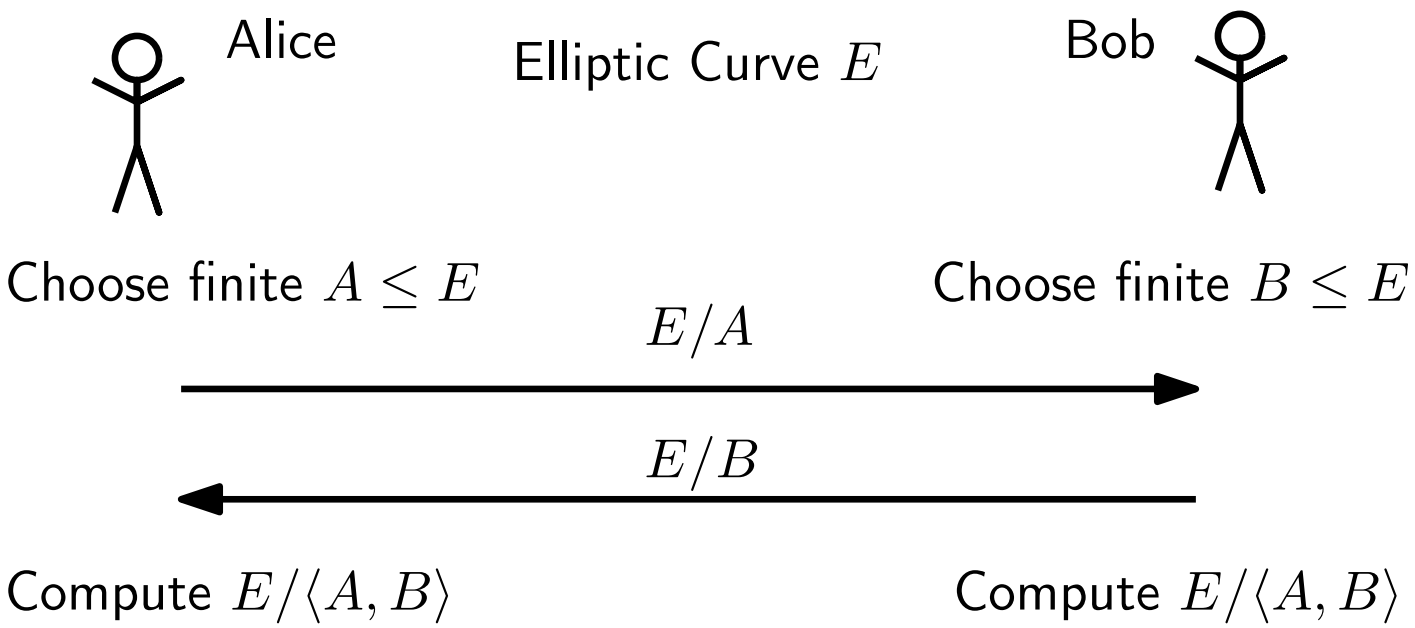
Write $E/\Phi = \tilde{E}$

Problem (Isogeny Path)

Given elliptic curves E, E' defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$, find an isogeny $E \to E'$ of smooth degree ($\deg\phi := \#\ker\phi$).

smooth $\sim$ only small factors

Idea



How to compute $E/\langle A, B\rangle$?

Supersingular Curves

Definition

Define $\mathrm{End}(E) := \{\phi : E \to E \mid \phi \text{ isogeny}\}$, equipped with addition $+$ and composition $\circ$.

Definition

Assume $\mathrm{char}(K) \neq 0$. Then E is called supersingular, if $\mathrm{End}(K)$ is not commutative.

Theorem

Let E be supersingular, defined over $\mathbb{F}_{p^2}$. If $j(E) \neq 0, 1728$ then

$$E\left(\mathbb{F}_{p^2}\right) \cong (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2$$

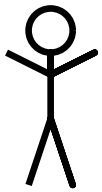
We also need $E[n] := \left\{P \in E\left(\mathbb{F}_{p^2}\right) \;\middle|\; \mathrm{ord}P \mid n\right\} \leq E\left(\mathbb{F}_{p^2}\right)$

Supersingular Isogeny Diffie-Hellman

Theorem

Let E be supersingular, defined over $\mathbb{F}_{p^2}$. If $j(E) \neq 0, 1728$ then

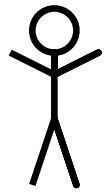
$$E\left(\mathbb{F}_{p^2}\right) \cong (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2$$



Alice

$E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z})^2$

Bob



$E[2^{e_A}] = \langle P_A, Q_A \rangle$

$E[3^{e_B}] = \langle P_B, Q_B \rangle$

Choose $m_A, n_A \in \mathbb{Z}$

$A := m_A P_A + n_A Q_A$

$\alpha : E \to E/\langle A \rangle$

Choose $m_B, n_B \in \mathbb{Z}$

$B := m_B P_B + n_B Q_B$

$\beta : E \to E/\langle B \rangle$

$E/\langle A \rangle, \alpha(P_B), \alpha(Q_B)$ →

← $E/\langle B \rangle, \beta(P_A), \beta(Q_A)$

$E/\langle B \rangle/\langle A' \rangle, \quad A' = m_A \beta(P_A) + n_A \beta(Q_A)$

Claim: $E/\langle A, B \rangle \cong E/\langle B \rangle/\langle A' \rangle$

Computing Isogenies

- E, P_A, Q_A, P_B, Q_B are fixed, namely $E : y^2 = x^3 + 6x^2 + x$
- nP using "double-and-add"
- So its left to compute $E/\langle A \rangle$ and $E \to E/\langle A \rangle$

Theorem (Vélu's formulas)

Let $G \leq E$ be finite and $\phi : E \to E/G$. With $G' = G \setminus \{0\}$ have

- $E/G : y^2 = x^3 + A'x + B'$ *where*

$$A' := A - 5 \sum_{(x,y) \in G'} 3x^2 + A, \quad B' := B - 7 \sum_{(x,y) \in G'} 5x^3 + 3Ax + B$$

- *For $P \notin G$, $\phi(P)$ is*

$$\left(x(P) + \sum_{Q \in G'} x(P+Q) - x(Q), \quad y(P) + \sum_{Q \in G'} y(P+Q) - y(Q) \right)$$

Computing Isogenies

Theorem (Vélu's formulas)

Let $G \leq E$ be finite and $\phi : E \to E/G$. With $G' = G \setminus \{0\}$ have

- $E/G : y^2 = x^3 + A'x + B'$ *where*

$$A' := A - 5 \sum_{(x,y) \in G'} 3x^2 + A, \quad B' := B - 7 \sum_{(x,y) \in G'} 5x^3 + 3Ax + B$$

- *For $P \notin G$, $\phi(P)$ is*

$$\left(x(P) + \sum_{Q \in G'} x(P+Q) - x(Q), \quad y(P) + \sum_{Q \in G'} y(P+Q) - y(Q) \right)$$

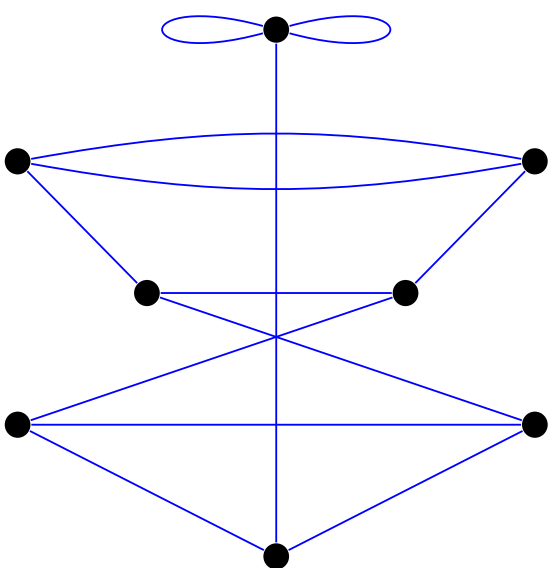
However, $\#G = 2^{e_A}$ resp. $\#G = 3^{e_B}$ is exponential
$\Rightarrow$ Decompose $\phi = \phi_1 \circ \ldots \circ \phi_e$ where $\#\ker \phi_i = 2$ resp. 3

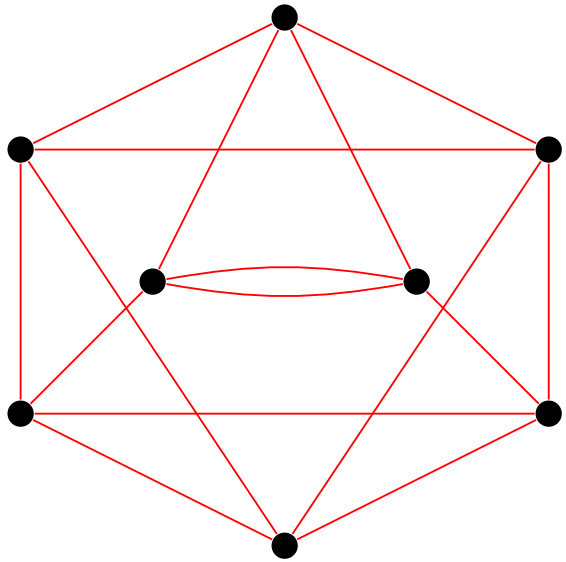
Isogeny Path

Decompose $\phi = \phi_1 \circ ... \circ \phi_e$ where $\ker \phi_i = 2$ resp. 3

Problem (Isogeny Path)

Given elliptic curves E, E' defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$, find an isogeny $E \to E'$ of smooth degree ($\deg\phi := \#\ker\phi$).





nodes $\sim$ j-invariants

edges $\sim$ isogenies

2 resp. 3-isogeny graph of $\mathbb{F}_{97^2}$ from [Feo17]

References

Luca De Feo. *Mathematics of Isogeny Based Cryptography*. 2017. arXiv: 1711.04062 [cs.CR].

Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

Thank you for your attention!