Elliptic Curve Cryptography

an introduction which is entirely too short

by Giacomo Fenzi (ETH Zurich)
on 6 January 2022

2022-01-07

Elliptic Curve Cryptography

Elliptic Curve Cryptography
an introduction which is entirely too short
by Giacomo Fenzi (ETH Zurich)
on 6 January 2022

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

» Motivation
'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

* Elliptic curves are everywhere in cryptography

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

* Elliptic curves are everywhere in cryptography

» Motivation

> *'It is possible to write endlessly on elliptic curves.*
> *(This is not a threat.)'* Serge Lang

- Elliptic curves are everywhere in cryptography
- Power $\approx 70\%$ of TLS Exchanges

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

- Elliptic curves are everywhere in cryptography
- Power $\approx 70\%$ of TLS Exchanges

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

- Elliptic curves are everywhere in cryptography
- Power $\approx 70\%$ of TLS Exchanges
- Coolest post quantum cryptography proposal

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

- Elliptic curves are everywhere in cryptography
- Power $\approx 70\%$ of TLS Exchanges
- Coolest post quantum cryptography proposal

» Motivation

‘It is possible to write endlessly on elliptic curves.
(This is not a threat.)’ Serge Lang

- Elliptic curves are everywhere in cryptography
- Power $\approx 70\%$ of TLS Exchanges
- Coolest post quantum cryptography proposal
- Fascinating mathematically

» Motivation

‘It is possible to write endlessly on elliptic curves.
(This is not a threat.)’ Serge Lang

- Elliptic curves are everywhere in cryptography
- Power $\approx 70\%$ of TLS Exchanges
- Coolest post quantum cryptography proposal
- Fascinating mathematically

» Outline

* Historical Notes

» Outline

* Historical Notes

» Outline

- Historical Notes
- Mathematical Background

» Outline

- Historical Notes
- Mathematical Background

» Outline

- Historical Notes
- Mathematical Background
- Addition on Elliptic Curves

» Outline
- Historical Notes
- Mathematical Background
- Addition on Elliptic Curves

» Outline

* Historical Notes
* Mathematical Background
* Addition on Elliptic Curves
* Discrete Logarithm and Diffie Hellman

» Outline

* Historical Notes
* Mathematical Background
* Addition on Elliptic Curves
* Discrete Logarithm and Diffie Hellman

» Outline

- Historical Notes
- Mathematical Background
- Addition on Elliptic Curves
- Discrete Logarithm and Diffie Hellman
- Pairings

» Outline

- Historical Notes
- Mathematical Background
- Addition on Elliptic Curves
- Discrete Logarithm and Diffie Hellman
- Pairings

» Outline

- Historical Notes
- Mathematical Background
- Addition on Elliptic Curves
- Discrete Logarithm and Diffie Hellman
- Pairings
- Isogenies

» Outline

- Historical Notes
- Mathematical Background
- Addition on Elliptic Curves
- Discrete Logarithm and Diffie Hellman
- Pairings
- Isogenies

» Diophantine Equations

Historically originated in the context of solving Diophantine equations such as

$$X^n + Y^n = Z^n, \quad X, Y, Z \in \mathbb{Z}$$

» Diophantine Equations
Historically originated in the context of solving Diophantine equations such as
$X^n + Y^n = Z^n, \quad X, Y, Z \in \mathbb{Z}$

1. Very easy over the reals, hard otherwise
2. Solvable? How many solutions?
3. Undecidable in 11 variables already

» Diophantine Equations

Historically originated in the context of solving Diophantine equations such as

$$X^n + Y^n = Z^n, \quad X, Y, Z \in \mathbb{Z}$$

or equivalently

$$x^n + y^n = 1, \quad x, y \in \mathbb{Q}$$

» Diophantine Equations

Historically originated in the context of solving Diophantine equations such as

$X^n + Y^n = Z^n, \quad X, Y, Z \in \mathbb{Z}$

or equivalently

$x^n + y^n = 1, \quad x, y \in \mathbb{Q}$

1. Very easy over the reals, hard otherwise
2. Solvable? How many solutions?
3. Undecidable in 11 variables already

» Diophantine Equations

Historically originated in the context of solving Diophantine equations such as

$$X^n + Y^n = Z^n, \quad X, Y, Z \in \mathbb{Z}$$

or equivalently

$$x^n + y^n = 1, \quad x, y \in \mathbb{Q}$$

Often very hard, and in general undecidable!
Let us see what we can do...

1. Very easy over the reals, hard otherwise
2. Solvable? How many solutions?
3. Undecidable in 11 variables already

» One variable

$$a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a = 0$$

» One variable
$a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a = 0$

1. Uses Gauss' Lemma

» One variable

$$a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a = 0$$

Quite easy! We can show that:

Theorem

Let $\frac{p}{q} \in \mathbb{Q}$ be a solution of the above equation. Then q divides a_n and p divides a_0.

» One variable

$a_n x^n + a_{n-1} x^{n-1} + \dots a_1 x + a = 0$

Quite easy! We can show that:

Theorem

Let $\frac{p}{q} \in \mathbb{Q}$ be a solution of the above equation. Then q divides a_n and p divides a_0.

1. Uses Gauss' Lemma

» One variable

$$a_n x^n + a_{n-1}x^{n-1} + \dots a_1 x + a = 0$$

Quite easy! We can show that:

Theorem

Let $\frac{p}{q} \in \mathbb{Q}$ be a solution of the above equation. Then q divides a_n and p divides a_0.

Check the finite list of candidates.
Alternatively, solve numerically and find candidate of form $\frac{b}{a_n}$

» One variable

$$a_n x^n + a_{n-1}x^{n-1} + \dots a_1 x + a = 0$$

Quite easy! We can show that:

Theorem

Let $\frac{p}{q} \in \mathbb{Q}$ be a solution of the above equation. Then q divides a_n and p divides a_0.

Check the finite list of candidates.
Alternatively, solve numerically and find candidate of form $\frac{b}{a_n}$

1. Uses Gauss' Lemma

» Linear and Quadratic

$$ax + by = c$$

» Linear and Quadratic
$ax + by = c$

1. Take the rational point, draw a line
2. Hasse = Local to Global: Solvable in rational iff in reals and p-adic for every p

» Linear and Quadratic

$$ax + by = c$$

Theorem

Has infinitely many rational solution. If $\gcd(a, b)$ does not divide c, then no integers solutions. Else, infinitely many.

» Linear and Quadratic

$ax + by = c$

Theorem

Has infinitely many rational solution. If $\gcd(a, b)$ does not divide c, then no integers solutions. Else, infinitely many.

1. Take the rational point, draw a line
2. Hasse = Local to Global: Solvable in rational iff in reals and p-adic for every p

» Linear and Quadratic

$$ax + by = c$$

Theorem

Has infinitely many rational solution. If $\gcd(a, b)$ does not divide c, then no integers solutions. Else, infinitely many.

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

» Linear and Quadratic

$ax + by = c$

Theorem

Has infinitely many rational solution. If $\gcd(a, b)$ does not divide c, then no integers solutions. Else, infinitely many.

$ax^2 + bxy + cy^2 + dx + ey + f = 0$

1. Take the rational point, draw a line
2. Hasse = Local to Global: Solvable in rational iff in reals and p-adic for every p

» Linear and Quadratic

$$ax + by = c$$

Theorem

Has infinitely many rational solution. If $\gcd(a, b)$ *does not divide* c*, then no integers solutions. Else, infinitely many.*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

These are rational points on a conic.

- Given a rational point, all of them can be found geometrically
- Hasse principle allows us to test if a rational point exists

» Linear and Quadratic
$ax + by = c$
Theorem
Has infinitely many rational solution. If $\gcd(a, b)$ does not divide c, then no integers solutions. Else, infinitely many.
$ax^2 + bxy + cy^2 + dx + ey + f = 0$
These are rational points on a conic.
Given a rational point, all of them can be found geometrically
Hasse principle allows us to test if a rational point exists

1. Take the rational point, draw a line
2. Hasse = Local to Global: Solvable in rational iff in reals and p-adic for every p

» Cubics

What about:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \text{ ?}$$

» Cubics
What about:
$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$?

1. Local to global fails
2. Originated in computation of arc length of ellipse

» Cubics

What about:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \ ?$$

This is the general form of an elliptic curve!

» Cubics

What about:

$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$?

This is the general form of an elliptic curve!

1. Local to global fails
2. Originated in computation of arc length of ellipse

» Cubics

What about:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\ ?$$

This is the general form of an elliptic curve! We have that

Theorem (Mordell)

If the curve is non singular, and it has a rational point then the group of rational points is finitely generated

» Cubics
What about:
$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\ ?$
This is the general form of an elliptic curve! We have that
Theorem (Mordell)
If the curve is non singular, and it has a rational point then the group of rational points is finitely generated

1. Local to global fails
2. Originated in computation of arc length of ellipse

» Cubics

What about:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \; ?$$

This is the general form of an elliptic curve! We have that

Theorem (Mordell)

If the curve is non singular, and it has a rational point then the group of rational points is finitely generated

But no equivalent of Hasse principle!

» Cubics
What about:
$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$?
This is the general form of an elliptic curve! We have that
Theorem (Mordell)
If the curve is non singular, and it has a rational point then the group of rational points is finitely generated
But no equivalent of Hasse principle!

1. Local to global fails
2. Originated in computation of arc length of ellipse

» Cubics

What about:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\ ?$$

This is the general form of an elliptic curve! We have that

Theorem (Mordell)

If the curve is non singular, and it has a rational point then the group of rational points is finitely generated

But no equivalent of Hasse principle!

Elliptic Curves $\neq$ Ellipse

» Cubics
What about:
$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\ ?$
This is the general form of an elliptic curve! We have that
Theorem (Mordell)
If the curve is non singular, and it has a rational point then the group of rational points is finitely generated
But no equivalent of Hasse principle!
Elliptic Curves $\neq$ Ellipse

1. Local to global fails
2. Originated in computation of arc length of ellipse

» Fields

Definition

A field K is set together with two operations $+, \cdot$ such that

* K is an abelian group under $+$ with identity 0
* $K - \{0\}$ is an abelian group under multiplication with identity 1.
* For every $a, b, c \in K$ we have that $a(b + c) = ab + ac$
* $0 \neq 1$

» Fields
Definition
A field K is set together with two operations $+, \cdot$ such that
K is an abelian group under $+$ with identity 0
$K - \{0\}$ is an abelian group under multiplication with identity 1.
For every $a, b, c \in K$ we have that $a(b + c) = ab + ac$
$0 \neq 1$

» Fields

Definition

A field K is set together with two operations $+, \cdot$ such that

* K is an abelian group under $+$ with identity 0
* $K - \{0\}$ is an abelian group under multiplication with identity 1.
* For every $a, b, c \in K$ we have that $a(b+c) = ab + ac$
* $0 \neq 1$

Informally, we can add, subtract, multiply and divide non zero elements.

» Fields

Definition

A field K is set together with two operations $+, \cdot$ such that

* K is an abelian group under $+$ with identity 0
* $K - \{0\}$ is an abelian group under multiplication with identity 1.
* For every $a, b, c \in K$ we have that $a(b+c) = ab + ac$
* $0 \neq 1$

Informally, we can add, subtract, multiply and divide non zero elements.

» Finite Fields

We are mostly interested in finite fields.:

Theorem

For every prime p, and every $n \in \mathbb{Z}^+$ there is an unique field of size p^n, which we denote by either $\mathbb{GF}(p^n)$ or $\mathbb{F}_{p^n}$

» Finite Fields

We are mostly interested in finite fields.:

Theorem

For every prime p, and every $n \in \mathbb{Z}^+$ there is an unique field of size p^n, which we denote by either $\mathbb{GF}(p^n)$ or $\mathbb{F}_{p^n}$

1. $\mathbb{F}_8 = \mathbb{F}_2[X]/(x^3 + x + 1)$

» Finite Fields

We are mostly interested in finite fields.:

Theorem

For every prime p, and every $n \in \mathbb{Z}^+$ there is an unique field of size p^n, which we denote by either $\mathbb{GF}(p^n)$ or $\mathbb{F}_{p^n}$

If $n = 1$, then $\mathbb{F}_p = \mathbb{Z}_p$, if not we can write them as

$$\mathbb{F}_{p^n} = \frac{\mathbb{F}_p[X]}{(f(x))}$$

where $f(x)$ is an irreducible polynomial of degree n.

» Finite Fields

We are mostly interested in finite fields.:

Theorem

For every prime p, and every $n \in \mathbb{Z}^+$ there is an unique field of size p^n, which we denote by either $\mathbb{GF}(p^n)$ or $\mathbb{F}_{p^n}$

If $n = 1$, then $\mathbb{F}_p = \mathbb{Z}_p$, if not we can write them as

$$\mathbb{F}_{p^n} = \frac{\mathbb{F}_p[X]}{(f(x))}$$

where $f(x)$ is an irreducible polynomial of degree n.

1. $\mathbb{F}_8 = \mathbb{F}_2[X]/(x^3 + x + 1)$

» Characteristic

For any field, $\mathrm{char}(\mathbb{F})$ is the least integer ℓ such that

$$\underbrace{1 + \ldots 1}_{\ell \text{ times}} = 0,$$

or ∞ if no such integer exists. We have that $\mathrm{char}(\mathbb{F}_{p^n}) = p$.

» Characteristic

For any field, $\mathrm{char}(\mathbb{F})$ is the least integer ℓ such that

$$\underbrace{1 + \ldots 1}_{\ell \text{ times}} = 0,$$

or ∞ if no such integer exists. We have that $\mathrm{char}(\mathbb{F}_{p^n}) = p$.

1. If two fields have different char, no map between them (apart 0)
2. Freshman's dream

» Field Extensions

Let k, K be two fields. If there is an homomorphism $k \to K$, we can identify k with a subfield of K. In that case, K is a **field extension** of k which we denote by $k \subseteq K$.

» Field Extensions

Let k, K be two fields. If there is an homomorphism $k \to K$, we can identify k with a subfield of K. In that case, K is a **field extension** of k which we denote by $k \subseteq K$.

1. Closures are always infinite
2. Can approximate $\bar{\mathbb{F}}$ with $\mathbb{F}_{p^{n!}}$
3. Base of Galois theory

» Field Extensions

Let k, K be two fields. If there is an homomorphism $k \to K$, we can identify k with a subfield of K. In that case, K is a **field extension** of k which we denote by $k \subseteq K$.
Given any field K we can construct the algebraic closure $\overline{K}$ which is the smallest algebraically closed extension containing K.
Some examples:

* $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
* $\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3} \cdots \subseteq \overline{\mathbb{F}}_p$

» Field Extensions

Let k, K be two fields. If there is an homomorphism $k \to K$, we can identify k with a subfield of K. In that case, K is a **field extension** of k which we denote by $k \subseteq K$.
Given any field K we can construct the algebraic closure $\overline{K}$ which is the smallest algebraically closed extension containing K.
Some examples:
$\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3} \cdots \subseteq \overline{\mathbb{F}}_p$

1. Closures are always infinite
2. Can approximate $\overline{\mathbb{F}}$ with $\mathbb{F}_{p^{n!}}$
3. Base of Galois theory

» Weierstrass Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

4-Much easier to manage!

» Weierstrass Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

4-Much easier to manage!

1. Weierstrass most common (academically)
2. Other models exist
3. Montgomery curves (x-only)
4. Edwards curves (Complete addition formula)
5. Legendre curves

» Weierstrass Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$
$$\downarrow$$
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

4-Much easier to manage!

» Weierstrass Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$
$$\downarrow$$
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

4-Much easier to manage!

1. Weierstrass most common (academically)
2. Other models exist
3. Montgomery curves (x-only)
4. Edwards curves (Complete addition formula)
5. Legendre curves

» Weierstrass Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$
$$\downarrow$$
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$
$$\Big\downarrow \ \mathrm{char}(K) \neq 2, 3$$
$$y^2 = x^3 + ax + b$$

4-Much easier to manage!

» Weierstrass Form

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$
$$y^2 + axy + by = x^3 + cx^2 + dx + e$$
$$\mathrm{char}(K) \neq 2, 3$$
$$y^2 = x^3 + ax + b$$

4-Much easier to manage!

1. Weierstrass most common (academically)
2. Other models exist
3. Montgomery curves (x-only)
4. Edwards curves (Complete addition formula)
5. Legendre curves

» Elliptic Curves

Definition

Let k be a field. An elliptic curve E over k (denoted by E/k) is given by

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

for $a, b \in k$.

» Elliptic Curves

Definition

Let k be a field. An elliptic curve E over k (denoted by E/k) is given by

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

for $a, b \in k$.

1. Projective closure
2. Point at infinity correspond to $(0 : 1 : 0)$

» Elliptic Curves

Definition

Let k be a field. An elliptic curve E over k (denoted by E/k) is given by

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

for $a, b \in k$. For any extension $k \subseteq K$ we define

$$E(K) = \left\{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

» Elliptic Curves

Definition

Let k be a field. An elliptic curve E over k (denoted by E/k) is given by

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

for $a, b \in k$. For any extension $k \subseteq K$ we define

$$E(K) = \left\{(x, y) \in K \times K \mid y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

1. Projective closure
2. Point at infinity correspond to $(0 : 1 : 0)$

» Elliptic Curves

Definition

Let k be a field. An elliptic curve E over k (denoted by E/k) is given by

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

for $a, b \in k$. For any extension $k \subseteq K$ we define

$$E(K) = \left\{ (x, y) \in K \times K \mid y^2 = x^3 + ax + b \right\} \cup \{\infty\}$$

Mathematicians are often interested with $E(\mathbb{Q}) \subseteq E(\mathbb{R}) \subseteq E(\mathbb{C})$ but we mostly consider the finite case.

» Elliptic Curves

Definition

Let k be a field. An elliptic curve E over k (denoted by E/k) is given by

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

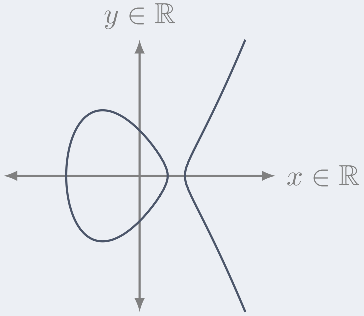
for $a, b \in k$. For any extension $k \subseteq K$ we define

$$E(K) = \left\{ (x, y) \in K \times K \mid y^2 = x^3 + ax + b \right\} \cup \{\infty\}$$

Mathematicians are often interested with $E(\mathbb{Q}) \subseteq E(\mathbb{R}) \subseteq E(\mathbb{C})$ but we mostly consider the finite case.

1. Projective closure
2. Point at infinity correspond to $(0 : 1 : 0)$

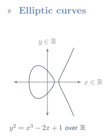
» Elliptic curves



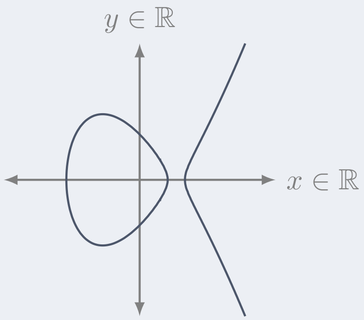
$y^2 = x^3 - 2x + 1$ over $\mathbb{R}$

2022-01-07

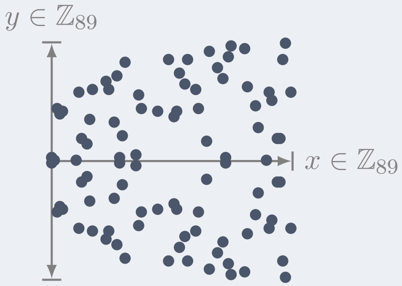
Elliptic Curve Cryptography
└ Elliptic Curves
  └ Representation and Group Law
    └ Elliptic curves



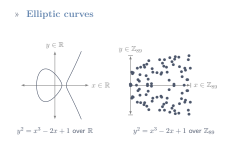
» Elliptic curves



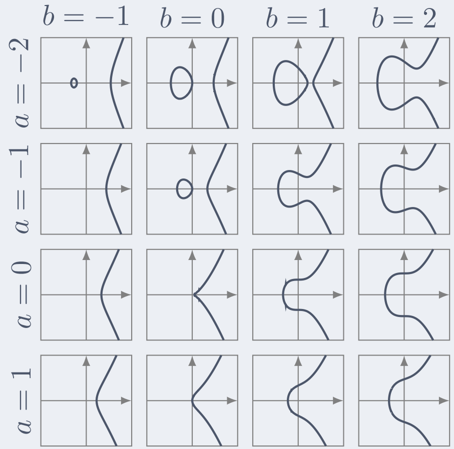
$y^2 = x^3 - 2x + 1$ over $\mathbb{R}$



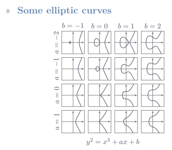
$y^2 = x^3 - 2x + 1$ over $\mathbb{Z}_{89}$



» Some elliptic curves

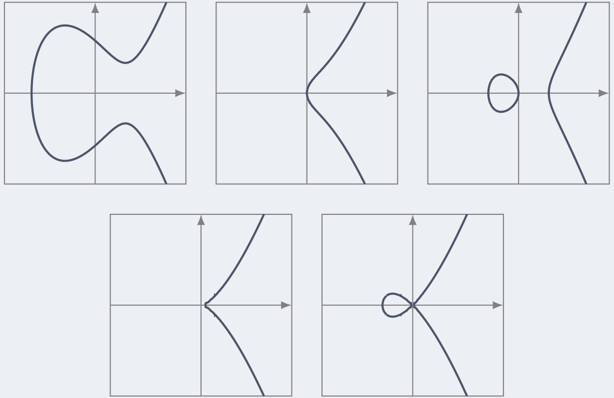


$$y^2 = x^3 + ax + b$$



» More elliptic curves

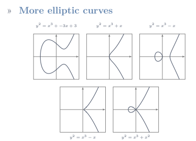
$y^2 = x^3 + -3x + 3$ $\quad$ $y^2 = x^3 + x$ $\quad$ $y^2 = x^3 - x$



$y^2 = x^3 - x$ $\quad$ $y^2 = x^3 + x^2$

2022-01-07

Elliptic Curve Cryptography
└─Elliptic Curves
  └─Representation and Group Law
    └─More elliptic curves



1. Top are non singular
2. First singular has cusp
3. Second has a node

» Discriminant

Definition

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is

$$\Delta = -16(4a^3 + 27b^2)$$

A curve is **singular** if $\Delta = 0$.

» Discriminant
Definition
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is
$$\Delta = -16(4a^3 + 27b^2)$$
A curve is **singular** if $\Delta = 0$.

» Discriminant

Definition

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is

$$\Delta = -16(4a^3 + 27b^2)$$

A curve is **singular** if $\Delta = 0$.

Alternatively, let $E : y^2 = f(x)$, and let x_1, x_2, x_3 be the roots of f.

$$\Delta = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

i.e. $\Delta = 0 \iff f$ has a repeated root.

» Discriminant

Definition

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is

$$\Delta = -16(4a^3 + 27b^2)$$

A curve is **singular** if $\Delta = 0$.

Alternatively, let $E : y^2 = f(x)$, and let x_1, x_2, x_3 be the roots of f.

$$\Delta = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

i.e. $\Delta = 0 \iff f$ has a repeated root.

» Discriminant

Definition

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is

$$\Delta = -16(4a^3 + 27b^2)$$

A curve is **singular** if $\Delta = 0$.

Alternatively, let $E : y^2 = f(x)$, and let x_1, x_2, x_3 be the roots of f.

$$\Delta = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

i.e. $\Delta = 0 \iff f$ has a repeated root.
From now on, all curves are assumed non singular.

2022-01-07

» Discriminant

Definition

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is

$$\Delta = -16(4a^3 + 27b^2)$$

A curve is **singular** if $\Delta = 0$.

Alternatively, let $E : y^2 = f(x)$, and let x_1, x_2, x_3 be the roots of f.

$$\Delta = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

i.e. $\Delta = 0 \iff f$ has a repeated root.
From now on, all curves are assumed non singular.

» j-invariant

Definition

The j-**invariant** of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta}$$

» j-invariant

Definition

The j-**invariant** of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta}$$

» j-invariant

Definition

The j-**invariant** of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta}$$

In fact, an isomorphism from a curve in short Weierstrass form must necessarily be:

$$(x, y) \mapsto (u^2 x, u^3 y)$$

for $u \in \overline{K}^*$

» j-invariant
Definition
The j-invariant of E is
$j(E) = -1728\frac{(4A)^3}{\Delta}$
In fact, an isomorphism from a curve in short Weierstrass form must necessarily be:
$(x, y) \mapsto (u^2 x, u^3 y)$
for $u \in \overline{K}^*$

» j-invariant

Definition

The j-**invariant** of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta}$$

In fact, an isomorphism from a curve in short Weierstrass form must necessarily be:

$$(x, y) \mapsto (u^2x, u^3y)$$

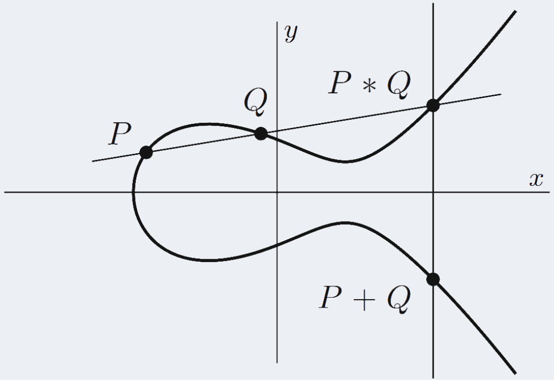
for $u \in \overline{K}^*$ and this yields:

Theorem

Let E, E' be two elliptic curves over K. Then $E \cong E'$ over $\overline{K}$ if and only if $j(E) = j(E')$.

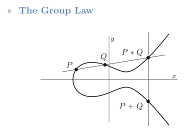
» j-invariant
Definition
The j-**invariant** of E is
$$j(E) = -1728\frac{(4A)^3}{\Delta}$$
In fact, an isomorphism from a curve in short Weierstrass form must necessarily be:
$$(x, y) \mapsto (u^2x, u^3y)$$
for $u \in \overline{K}^*$ and this yields:
Theorem
Let E, E' be two elliptic curves over K. Then $E \cong E'$ over $\overline{K}$ if and only if $j(E) = j(E')$.

» The Group Law



2022-01-07

Elliptic Curve Cryptography
└─Elliptic Curves
  └─Representation and Group Law
    └─The Group Law



» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$.

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$.

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

» The Group Law: Formulae
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define
$-P_0 = (x_0, -y_0)$

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

Now, for $P_1 + P_2$:

» The Group Law: Formulae
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define
$$-P_0 = (x_0, -y_0)$$
Now, for $P_1 + P_2$:

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

Now, for $P_1 + P_2$:

* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$

» The Group Law: Formulae
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define
$$-P_0 = (x_0, -y_0)$$
Now, for $P_1 + P_2$:
* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

Now, for $P_1 + P_2$:

* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.

2022-01-07

» The Group Law: Formulae
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define
$$-P_0 = (x_0, -y_0)$$
Now, for $P_1 + P_2$:
* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

Now, for $P_1 + P_2$:

* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.
* Let $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where λ is:

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

» The Group Law: Formulae
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define
$$-P_0 = (x_0, -y_0)$$
Now, for $P_1 + P_2$:
* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.
* Let $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where λ is:
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1}, & \text{otherwise} \end{cases}$$

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

Now, for $P_1 + P_2$:

* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.
* Let $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where λ is:

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

This makes E into an abelian group with identity ∞

» The Group Law: Formulae
Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define
$$-P_0 = (x_0, -y_0)$$
Now, for $P_1 + P_2$:
* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.
* Let $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where λ is:
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1}, & \text{otherwise} \end{cases}$$
This makes E into an abelian group with identity ∞

» Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$. We then extend the notation by letting $[0]P = \infty$ and $[-n]P = [n](-P)$.

» Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$. We then extend the notation by letting $[0]P = \infty$ and $[-n]P = [n](-P)$.

» Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$. We then extend the notation by letting $[0]P = \infty$ and $[-n]P = [n](-P)$.
We can compute $[n]P$ in $\Theta(\log n)$ group operations using double and add.

» Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$. We then extend the notation by letting $[0]P = \infty$ and $[-n]P = [n](-P)$.
We can compute $[n]P$ in $\Theta(\log n)$ group operations using double and add.

» Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$. We then extend the notation by letting $[0]P = \infty$ and $[-n]P = [n](-P)$.
We can compute $[n]P$ in $\Theta(\log n)$ group operations using double and add.
For $m \in \mathbb{Z}$ we define a map $[m] : E \to E$ accordingly, and write:

$$E[m] := \ker[m]$$

to be the m-**torsion subgroup** of E.

» Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n \text{ times}}$. We then extend the notation by letting $[0]P = \infty$ and $[-n]P = [n](-P)$.
We can compute $[n]P$ in $\Theta(\log n)$ group operations using double and add.
For $m \in \mathbb{Z}$ we define a map $[m] : E \to E$ accordingly, and write:

$$E[m] := \ker[m]$$

to be the m-**torsion subgroup** of E.

» Number of Points on a curve

Heuristically, we expect $\approx q + 1$ points

» Number of Points on a curve

Heuristically, we expect $\approx q + 1$ points

1. Each value of x yields at most two of y
2. a random element has 50% of being quadratic residue

» Number of Points on a curve

Heuristically, we expect $\approx q+1$ points

Theorem (Hasse)

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

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

» Number of Points on a curve

Heuristically, we expect $\approx q+1$ points

Theorem (Hasse)

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

$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$

1. Each value of x yields at most two of y
2. a random element has 50% of being quadratic residue

» Number of Points on a curve

Heuristically, we expect $\approx q+1$ points

Theorem (Hasse)

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

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

Exact value can be efficiently found using Schoof's algorithm in $O((\log q)^8)$.

» Number of Points on a curve

Heuristically, we expect $\approx q+1$ points

Theorem (Hasse)

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

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

Exact value can be efficiently found using Schoof's algorithm in $O((\log q)^8)$.

1. Each value of x yields at most two of y
2. a random element has 50% of being quadratic residue

» Discrete Logarithm

Cryptography relies on hardness assumptions.

» Discrete Logarithm
Cryptography relies on hardness assumptions.

» Discrete Logarithm

Cryptography relies on hardness assumptions.

Definition

Let $\mathrm{Gen}(1^\lambda)$ be a p.p.t. algorithm that returns a group description $\mathbb{G} = (+, P, q)$, where $\mathbb{G} = \langle P \rangle$ and $q = \#\mathbb{G}$. For an attacker $\mathcal{A}$, define

$$\mathsf{Adv}^{\mathrm{dlp}}_{\mathcal{A}}(\lambda) = \Pr\left[\mathcal{A}\left(1^\lambda, \mathbb{G}, [k]P\right) = k \;\middle|\; \begin{array}{c} \mathbb{G} \leftarrow\!\$\, \mathrm{Gen}(1^\lambda) \\ k \leftarrow\!\$\, \mathbb{Z}_q \end{array}\right]$$

We say that the **discrete logarithm assumption** hold with respect to Gen if, for every p.p.t. attacker $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{dlp}}_{\mathcal{A}}(\cdot)$ is negligible.

2022-01-07

Elliptic Curve Cryptography
└Elliptic Curves
└Discrete Log Crypto
└Discrete Logarithm

» Discrete Logarithm

Cryptography relies on hardness assumptions.

Definition

Let $\mathrm{Gen}(1^\lambda)$ be a p.p.t. algorithm that returns a group description $\mathbb{G} = (+, P, q)$, where $\mathbb{G} = \langle P \rangle$ and $q = \#\mathbb{G}$. For an attacker $\mathcal{A}$, define

$$\mathsf{Adv}^{\mathrm{dlp}}_{\mathcal{A}}(\lambda) = \Pr\left[\mathcal{A}\left(1^\lambda, \mathbb{G}, [k]P\right) = k \;\middle|\; \begin{array}{c} \mathbb{G} \leftarrow\!\$\, \mathrm{Gen}(1^\lambda) \\ k \leftarrow\!\$\, \mathbb{Z}_q \end{array}\right]$$

We say that the **discrete logarithm assumption** hold with respect to Gen if, for every p.p.t. attacker $\mathcal{A}$, $\mathsf{Adv}^{\mathrm{dlp}}_{\mathcal{A}}(\cdot)$ is negligible.

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

1. In fact in some groups CDH and DLP are equivalent
2. Check $e(g^x, g^y) = e(g, g^z)$

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$

» Related Assumptions
In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.
* CHD: From $[x]P, [y]P$ compute $[xy]P$

1. In fact in some groups CDH and DLP are equivalent
2. Check $e(g^x, g^y) = e(g, g^z)$

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

1. In fact in some groups CDH and DLP are equivalent
2. Check $e(g^x, g^y) = e(g, g^z)$

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

Pairings make DDH easy on elliptic curves!

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

Pairings make DDH easy on elliptic curves!

1. In fact in some groups CDH and DLP are equivalent
2. Check $e(g^x, g^y) = e(g, g^z)$

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

Pairings make DDH easy on elliptic curves!

$$\text{DDH} \leq_R \text{CDH} \leq_R \text{DLP}$$

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

Pairings make DDH easy on elliptic curves!

$$\text{DDH} \leq_R \text{CDH} \leq_R \text{DLP}$$

1. In fact in some groups CDH and DLP are equivalent
2. Check $e(g^x, g^y) = e(g, g^z)$

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

Pairings make DDH easy on elliptic curves!

$$\mathrm{DDH} \leq_R \mathrm{CDH} \leq_R \mathrm{DLP}$$

Representation matters! $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^*$ as groups but the discrete logarithm is trivial in the former, assumed hard in the latter.

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

* CHD: From $[x]P, [y]P$ compute $[xy]P$
* DDH: Distinguish $(P, [x]P, [y]P, [xy]P)$ from $(P, [x]P, [y]P, [z]P)$

Pairings make DDH easy on elliptic curves!

DDH $\leq_R$ CDH $\leq_R$ DLP

Representation matters! $\mathbb{Z}_{p-1} \cong \mathbb{Z}_p^*$ as groups but the discrete logarithm is trivial in the former, assumed hard in the latter.

1. In fact in some groups CDH and DLP are equivalent
2. Check $e(g^x, g^y) = e(g, g^z)$

» Why elliptic curves?

» Why elliptic curves?

1. 128 bits
2. RSA public key ops are faster, private ops slower

» Why elliptic curves?

Assumption	Group	Best Algorithm	≈ Complexity
RSA	$\mathbb{Z}_N$	Number Field Sieve	$\exp(c^3\sqrt{\log N})$
DLP	$\mathbb{F}_p^*$	Number Field Sieve	$\exp(c^3\sqrt{\log p})$
DLP	$E(\mathbb{F}_p)$	Pollard Rho	$\sqrt{p}$

» Why elliptic curves?

Assumption	Group	Best Algorithm	≈ Complexity
RSA	$\mathbb{Z}_N$	Number Field Sieve	$\exp(c^3\sqrt{\log N})$
DLP	$\mathbb{F}_p^*$	Number Field Sieve	$\exp(c^3\sqrt{\log p})$
DLP	$E(\mathbb{F}_p)$	Pollard Rho	$\sqrt{p}$

1. 128 bits
2. RSA public key ops are faster, private ops slower

» Why elliptic curves?

Assumption	Group	Best Algorithm	≈ Complexity
RSA	$\mathbb{Z}_N$	Number Field Sieve	$\exp(c^3\sqrt{\log N})$
DLP	$\mathbb{F}_p^*$	Number Field Sieve	$\exp(c^3\sqrt{\log p})$
DLP	$E(\mathbb{F}_p)$	Pollard Rho	$\sqrt{p}$

Best known attacks against ECC are generic attacks

» Why elliptic curves?

Assumption	Group	Best Algorithm	≈ Complexity
RSA	$\mathbb{Z}_N$	Number Field Sieve	$\exp(c^3\sqrt{\log N})$
DLP	$\mathbb{F}_p^*$	Number Field Sieve	$\exp(c^3\sqrt{\log p})$
DLP	$E(\mathbb{F}_p)$	Pollard Rho	$\sqrt{p}$

Best known attacks against ECC are generic attacks

1. 128 bits
2. RSA public key ops are faster, private ops slower

» Why elliptic curves?

Assumption	Group	Best Algorithm	$\approx$ Complexity
RSA	$\mathbb{Z}_N$	Number Field Sieve	$\exp(c^3\sqrt{\log N})$
DLP	$\mathbb{F}_p^*$	Number Field Sieve	$\exp(c^3\sqrt{\log p})$
DLP	$E(\mathbb{F}_p)$	Pollard Rho	$\sqrt{p}$

Best known attacks against ECC are generic attacks

* Shorter keysizes (≈ 256 vs 3072 bits)
* Faster computation

» Why elliptic curves?

Assumption	Group	Best Algorithm	$\approx$ Complexity
RSA	$\mathbb{Z}_N$	Number Field Sieve	$\exp(c^3\sqrt{\log N})$
DLP	$\mathbb{F}_p^*$	Number Field Sieve	$\exp(c^3\sqrt{\log p})$
DLP	$E(\mathbb{F}_p)$	Pollard Rho	$\sqrt{p}$

Best known attacks against ECC are generic attacks
* Shorter keysizes (≈ 256 vs 3072 bits)
* Faster computation

1. 128 bits
2. RSA public key ops are faster, private ops slower

» EC Diffie Hellman Key Exchange

Let E be an elliptic curve over $\mathbb{F}_q$. Let p be a large prime dividing $\#E(\mathbb{F}_q)$ and P a point of order p.

» EC Diffie Hellman Key Exchange
Let E be an elliptic curve over $\mathbb{F}_q$. Let p be a large prime dividing $\#E(\mathbb{F}_q)$ and P a point of order p.

1. Need to check received points are on curve
2. Invalid points attacks

» EC Diffie Hellman Key Exchange

Let E be an elliptic curve over $\mathbb{F}_q$. Let p be a large prime dividing $\#E(\mathbb{F}_q)$ and P a point of order p.

Diffie Hellman

Alice		**Bob**
$x \xleftarrow{\$} \mathbb{Z}_q$		$y \xleftarrow{\$} \mathbb{Z}_q$
$Q_A = [x]P$		$Q_B = [y]P$
	$\xrightarrow{Q_A}$	
	$\xleftarrow{Q_B}$	
$K = [x]Q_B$		$K = [y]Q_A$

» EC Diffie Hellman Key Exchange

Let E be an elliptic curve over $\mathbb{F}_q$. Let p be a large prime dividing $\#E(\mathbb{F}_q)$ and P a point of order p.

Diffie Hellman

Alice Bob
$x \xleftarrow{\$} \mathbb{Z}_q$ $y \xleftarrow{\$} \mathbb{Z}_q$
$Q_A = [x]P$ $Q_B = [y]P$
$\xrightarrow{Q_A}$
$\xleftarrow{Q_B}$
$K = [x]Q_B$ $K = [y]Q_A$

1. Need to check received points are on curve
2. Invalid points attacks

» EC Diffie Hellman Key Exchange

Let E be an elliptic curve over $\mathbb{F}_q$. Let p be a large prime dividing $\#E(\mathbb{F}_q)$ and P a point of order p.

Diffie Hellman		
Alice		**Bob**
$x \leftarrow\$ \mathbb{Z}_q$		$y \leftarrow\$ \mathbb{Z}_q$
$Q_A = [x]P$		$Q_B = [y]P$
	$\xrightarrow{Q_A}$	
	$\xleftarrow{Q_B}$	
$K = [x]Q_B$		$K = [y]Q_A$

Correctness follows since:

$$K = [x]Q_B = [x][y]P = [xy]P = [y][x]P = [y]Q_A = K$$

1. Need to check received points are on curve
2. Invalid points attacks

» Easy Elliptic Curves

DLP is not equally hard on every curve!

- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$

» Easy Elliptic Curves

DLP is not equally hard on every curve!

- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$

1. Embedding degree -¿ MOV algorithm

» Easy Elliptic Curves

DLP is not equally hard on every curve!

- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$
- Curves and subgroups with small embedding degree. E.g. supersingular and anomalous curves

» Easy Elliptic Curves

DLP is not equally hard on every curve!
- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$
- Curves and subgroups with small embedding degree. E.g. supersingular and anomalous curves

1. Embedding degree -¿ MOV algorithm

» Easy Elliptic Curves

DLP is not equally hard on every curve!

- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$
- Curves and subgroups with small embedding degree. E.g. supersingular and anomalous curves
- Curves that admit pairings to small finite fields.

» Easy Elliptic Curves

DLP is not equally hard on every curve!
- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$
- Curves and subgroups with small embedding degree. E.g. supersingular and anomalous curves
- Curves that admit pairings to small finite fields.

1. Embedding degree -¿ MOV algorithm

» Easy Elliptic Curves

DLP is not equally hard on every curve!

- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$
- Curves and subgroups with small embedding degree. E.g. supersingular and anomalous curves
- Curves that admit pairings to small finite fields.
- Curves defined over $\mathbb{F}_{p^k}$ for k with small factors. GHS Method, Diem's Analysis.

» Easy Elliptic Curves

DLP is not equally hard on every curve!
- Singular curves over $\mathbb{F}_p$. Equivalent to DLP in $\mathbb{F}_p^*$ or $\mathbb{F}_p^+$
- Curves and subgroups with small embedding degree. E.g. supersingular and anomalous curves
- Curves that admit pairings to small finite fields.
- Curves defined over $\mathbb{F}_{p^k}$ for k with small factors. GHS Method, Diem's Analysis.

1. Embedding degree -¿ MOV algorithm

» Pollard Rho

Collision search for $f : S \to S$. Let $x_0 \in S$, $x_n = f(x_{n-1})$.

» Pollard Rho
Collision search for $f : S \to S$. Let $x_0 \in S$, $x_n = f(x_{n-1})$.

1. In practice, to detect cycle step one iterator by one and one by two
2. Not parallelizable, use vOW (more memory)

» Pollard Rho

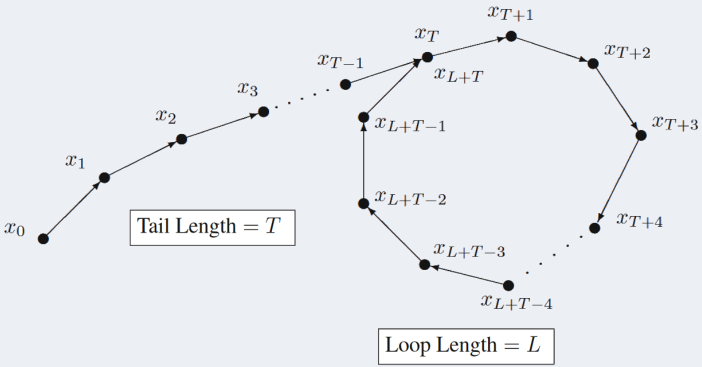
Collision search for $f : S \to S$. Let $x_0 \in S$, $x_n = f(x_{n-1})$.
Expected $\sqrt{\pi \# S/2}$ calls to f, constant memory.

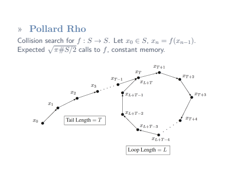
» Pollard Rho
Collision search for $f : S \to S$. Let $x_0 \in S$, $x_n = f(x_{n-1})$.
Expected $\sqrt{\pi \# S/2}$ calls to f, constant memory.

1. In practice, to detect cycle step one iterator by one and one by two
2. Not parallelizable, use vOW (more memory)

» Pollard Rho

Collision search for $f : S \to S$. Let $x_0 \in S$, $x_n = f(x_{n-1})$.
Expected $\sqrt{\pi \# S/2}$ calls to f, constant memory.





1. In practice, to detect cycle step one iterator by one and one by two
2. Not parallelizable, use vOW (more memory)

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$.

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$.

1. Nowadays functions with better mixing used
2. The $\gcd$ condition in pratice almost always true

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$.
Split $G = A \sqcup B \sqcup C$ with $\#A \approx \#B \approx \#C$.

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$.
Split $G = A \sqcup B \sqcup C$ with $\#A \approx \#B \approx \#C$.

1. Nowadays functions with better mixing used
2. The $\gcd$ condition in pratice almost always true

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$. Split $G = A \sqcup B \sqcup C$ with $\#A \approx \#B \approx \#C$. Define

$$f(X) = \begin{cases} P + X, & X \in A \\ [2]X, & X \in B \\ Q + X, & X \in C \end{cases}$$

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$. Split $G = A \sqcup B \sqcup C$ with $\#A \approx \#B \approx \#C$. Define

$$f(X) = \begin{cases} P + X, & X \in A \\ [2]X, & X \in B \\ Q + X, & X \in C \end{cases}$$

1. Nowadays functions with better mixing used
2. The $\gcd$ condition in pratice almost always true

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$. Split $G = A \sqcup B \sqcup C$ with $\#A \approx \#B \approx \#C$. Define

$$f(X) = \begin{cases} P + X, & X \in A \\ [2]X, & X \in B \\ Q + X, & X \in C \end{cases}$$

Let $X_0 = \infty$, then $X_i = [\alpha_i]P + [\beta_i]Q$ and we can track α_i, β_i. A collision $X_j = X_{j+\ell}$ with $\gcd(\beta_{j+\ell} - \beta_j, N) = 1$ allows us to solve the DLP with

$$k \equiv \frac{\alpha_j - \alpha_{j+\ell}}{\beta_{j+\ell} - \beta_j} \pmod N$$

» Pollard Rho

Let G be a group of order N. We want to find k s.t. $[k]P = Q$. Split $G = A \sqcup B \sqcup C$ with $\#A \approx \#B \approx \#C$. Define

$$f(X) = \begin{cases} P + X, & X \in A \\ [2]X, & X \in B \\ Q + X, & X \in C \end{cases}$$

Let $X_0 = \infty$, then $X_i = [\alpha_i]P + [\beta_i]Q$ and we can track α_i, β_i. A collision $X_j = X_{j+\ell}$ with $\gcd(\beta_{j+\ell} - \beta_j, N) = 1$ allows us to solve the DLP with

$$k \equiv \frac{\alpha_j - \alpha_{j+\ell}}{\beta_{j+\ell} - \beta_j} \pmod N$$

1. Nowadays functions with better mixing used
2. The $\gcd$ condition in pratice almost always true

» Pairings

Definition

Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:

» Pairings

Definition

Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:

1. The alternating not strictly in definition
2. Generalised with three groups

» Pairings

Definition

Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:

* Non degenerate:

$$e(S, T) = 1 \; \forall S \in \mathbb{G} \implies T = 0_{\mathbb{G}}$$

» Pairings
Definition
Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:
Non degenerate:
$e(S, T) = 1 \; \forall S \in \mathbb{G} \implies T = 0_{\mathbb{G}}$

1. The alternating not strictly in definition
2. Generalised with three groups

» Pairings

Definition

Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:

* Non degenerate:

$$e(S,T) = 1 \ \forall S \in \mathbb{G} \implies T = 0_{\mathbb{G}}$$

* Bilinear:

$$e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$$

$$e(S, T_1 + T_2) = e(S, T_1)e(S_2, T_2)$$

» Pairings
Definition
Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:
Non degenerate: $e(S,T) = 1 \ \forall S \in \mathbb{G} \implies T = 0_{\mathbb{G}}$
Bilinear: $e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$ $e(S, T_1 + T_2) = e(S, T_1)e(S_2, T_2)$

1. The alternating not strictly in definition
2. Generalised with three groups

» Pairings

Definition

Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:

- Non degenerate:

$$e(S,T) = 1 \; \forall S \in \mathbb{G} \implies T = 0_{\mathbb{G}}$$

- Bilinear:

$$e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$$

$$e(S, T_1 + T_2) = e(S, T_1)e(S_2, T_2)$$

- Alternating:

$$e(T,T) = 1$$

» Pairings
Definition
Let $\mathbb{G}, \mathbb{G}_T$ be two groups. A **pairing** is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ that is:
Non degenerate: $e(S,T) = 1 \; \forall S \in \mathbb{G} \implies T = 0_{\mathbb{G}}$
Bilinear: $e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$ $e(S, T_1 + T_2) = e(S, T_1)e(S_2, T_2)$
Alternating: $e(T,T) = 1$

1. The alternating not strictly in definition
2. Generalised with three groups

» Weil Pairing

Every elliptic curve E over K admits an efficiently computable pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

where μ_m is the group of m-th root of unity.

» Weil Pairing

Every elliptic curve E over K admits an efficiently computable pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

where μ_m is the group of m-th root of unity.

1. Not every curve has distorsion maps

» Weil Pairing

Every elliptic curve E over K admits an efficiently computable pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

where μ_m is the group of m-th root of unity.
It is degenerate on cyclic subgroups of $E[m]$, so use modified Weil pairing

$$\langle \cdot, \cdot \rangle : E[m] \times E[m] \to \mu_m$$
$$\langle P, Q \rangle = e_m(S, \phi(Q))$$

For $\phi : E \to E$ a distorsion map

» Weil Pairing

Every elliptic curve E over K admits an efficiently computable pairing
$e_m : E[m] \times E[m] \to \mu_m$
where μ_m is the group of m-th root of unity.
It is degenerate on cyclic subgroups of $E[m]$, so use modified Weil pairing
$\langle \cdot, \cdot \rangle : E[m] \times E[m] \to \mu_m$
$\langle P, Q \rangle = e_m(S, \phi(Q))$
For $\phi : E \to E$ a distorsion map

1. Not every curve has distorsion maps

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

2022-01-07

Elliptic Curve Cryptography
└─Elliptic Curves
└─Pairings
└─BLS Signatures

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

$$\underline{\mathrm{Gen}(1^\lambda)}$$

$$x \leftarrow\!\!\$\, \mathbb{Z}_p$$
$$pk := [x]P$$
$$sk := x$$
$$\textbf{return } (pk, sk)$$

2022-01-07

Elliptic Curve Cryptography
└Elliptic Curves
 └Pairings
  └BLS Signatures

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

$\mathrm{Gen}(1^\lambda)$

$x \leftarrow\!\!\$\, \mathbb{Z}_p$
$pk := [x]P$
$sk := x$
return (pk, sk)

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

$\mathrm{Gen}(1^\lambda)$	$\mathrm{Sign}(sk, m)$
$x \leftarrow\$ \mathbb{Z}_p$	$Q \leftarrow H(m)$
$pk := [x]P$	$\sigma \leftarrow [x]Q$
$sk := x$	$\mathbf{return}\ \sigma$
$\mathbf{return}\ (pk, sk)$	

2022-01-07

Elliptic Curve Cryptography
└Elliptic Curves
└Pairings
└BLS Signatures

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

$\text{Gen}(1^\lambda)$	$\text{Sign}(sk, m)$
$x \leftarrow\!\$\ \mathbb{Z}_p$	$Q \leftarrow H(m)$
$pk := [x]P$	$\sigma \leftarrow [x]Q$
$sk := x$	$\textbf{return } \sigma$
$\textbf{return } (pk, sk)$	

$\text{Verify}(pk, m, \sigma)$

$\textbf{return } e(\sigma, P) =_? e(H(m), [x]P)$

» BLS Signatures

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$

$\underline{\mathrm{Gen}(1^\lambda)}$	$\underline{\mathrm{Sign}(sk, m)}$
$x \leftarrow\!\$\, \mathbb{Z}_p$	$Q \leftarrow H(m)$
$pk := [x]P$	$\sigma \leftarrow [x]Q$
$sk := x$	$\mathbf{return}\ \sigma$
$\mathbf{return}\ (pk, sk)$	

$$\underline{\mathrm{Verify}(pk, m, \sigma)}$$
$$\mathbf{return}\ e(\sigma, P) =_? e(H(m), [x]P)$$

Correctness by:

$$e(\sigma, P) = e([x]Q, P) = e(Q, P)^x = e(Q, [x]P) = e(H(m), [x]P)$$

» BLS Signatures
Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p. Let P be a generator of $\mathbb{G}$, and e a non degenerate pairing. Also, let $H : \{0,1\}^* \to \mathbb{G}$
Correctness by:
$e(\sigma, P) = e([x]Q, P) = e(Q, P)^x = e(Q, [x]P) = e(H(m), [x]P)$

» Post Quantum

* Discrete logarithms, RSA, and pairings broken by Shor's algorithm

» Post Quantum

* Discrete logarithms, RSA, and pairings broken by Shor's algorithm

» Post Quantum

- Discrete logarithms, RSA, and pairings broken by Shor's algorithm
- Can we recover?

» Post Quantum

- Discrete logarithms, RSA, and pairings broken by Shor's algorithm
- Can we recover?

» Post Quantum

- Discrete logarithms, RSA, and pairings broken by Shor's algorithm
- Can we recover?
- Yes, lattices, codes, multinear maps...

» Post Quantum

- Discrete logarithms, RSA, and pairings broken by Shor's algorithm
- Can we recover?
- Yes, lattices, codes, multinear maps...

» Post Quantum

- Discrete logarithms, RSA, and pairings broken by Shor's algorithm
- Can we recover?
- Yes, lattices, codes, multinear maps...
- **Isogenies!**

» Post Quantum

- Discrete logarithms, RSA, and pairings broken by Shor's algorithm
- Can we recover?
- Yes, lattices, codes, multinear maps...
- **Isogenies!**

» Isogenies

"Nice maps" between elliptic curves.

» Isogenies
"Nice maps" between elliptic curves.

» Isogenies

"Nice maps" between elliptic curves.

Definition

Let E_1, E_2 be elliptic curves. An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

with $\phi(\infty) = \infty$. If $\phi(E_1) \neq \{\infty\}$, E_1 is **isogenous** to E_2.

» Isogenies
"Nice maps" between elliptic curves.
Definition
Let E_1, E_2 be elliptic curves. An isogeny is a morphism
$\phi : E_1 \to E_2$
with $\phi(\infty) = \infty$. If $\phi(E_1) \neq \{\infty\}$, E_1 is isogenous to E_2.

» Isogenies

"Nice maps" between elliptic curves.

Definition

Let E_1, E_2 be elliptic curves. An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

with $\phi(\infty) = \infty$. If $\phi(E_1) \neq \{\infty\}$, E_1 is **isogenous** to E_2.

For example, the curves $y^2 = x^3 + x$ and $y^2 = x^3 - 3x + 3$ are isogenous over $\mathbb{F}_{71}$ via the isogeny

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, y \cdot \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \right)$$

» Isogenies

"Nice maps" between elliptic curves.

Definition

Let E_1, E_2 be elliptic curves. An **isogeny** is a morphism

$$\phi : E_1 \to E_2$$

with $\phi(\infty) = \infty$. If $\phi(E_1) \neq \{\infty\}$, E_1 is **isogenous** to E_2.

For example, the curves $y^2 = x^3 + x$ and $y^2 = x^3 - 3x + 3$ are isogenous over $\mathbb{F}_{71}$ via the isogeny

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, y \cdot \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \right)$$

» Properties of isogenies

* Each isogeny is also a group homomorphism

» Properties of isogenies
* Each isogeny is also a group homomorphism

» Properties of isogenies

- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny

» Properties of isogenies
- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny

» Properties of isogenies

* Each isogeny is also a group homomorphism
* The map $[m] : E \to E$ is an isogeny
* You can compose isogenies

» Properties of isogenies
* Each isogeny is also a group homomorphism
* The map $[m] : E \to E$ is an isogeny
* You can compose isogenies

» Properties of isogenies

- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny
- You can compose isogenies
- Each isogeny has a degree, and it is multiplicative
  $\deg(\phi \circ \psi) = \deg(\phi) \deg(\psi)$

» Properties of isogenies
- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny
- You can compose isogenies
- Each isogeny has a degree, and it is multiplicative
  $\deg(\phi \circ \psi) = \deg(\phi) \deg(\psi)$

» Properties of isogenies

- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny
- You can compose isogenies
- Each isogeny has a degree, and it is multiplicative $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$
- Each isogeny $\phi : E_1 \to E_2$ has a unique dual $\hat{\phi} : E_2 \to E_1$ such that

$$\phi \circ \hat{\phi} = [\deg(\phi)]$$

2022-01-07

» Properties of isogenies
- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny
- You can compose isogenies
- Each isogeny has a degree, and it is multiplicative $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$
- Each isogeny $\phi : E_1 \to E_2$ has a unique dual $\hat{\phi} : E_2 \to E_1$ such that
$\phi \circ \hat{\phi} = [\deg(\phi)]$

» Properties of isogenies

- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny
- You can compose isogenies
- Each isogeny has a degree, and it is multiplicative $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$
- Each isogeny $\phi : E_1 \to E_2$ has a unique dual $\hat{\phi} : E_2 \to E_1$ such that
$$\phi \circ \hat{\phi} = [\deg(\phi)]$$
- An isogeny between two Weierstrass curves has the form
$$(x, y) \mapsto \left(\frac{f}{h^2}(x), y \cdot \frac{g}{h^3}(x)\right)$$

» Properties of isogenies
- Each isogeny is also a group homomorphism
- The map $[m] : E \to E$ is an isogeny
- You can compose isogenies
- Each isogeny has a degree, and it is multiplicative $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$
- Each isogeny $\phi : E_1 \to E_2$ has a unique dual $\hat{\phi} : E_2 \to E_1$ such that $\phi \circ \hat{\phi} = [\deg(\phi)]$
- An isogeny between two Weierstrass curves has the form $(x, y) \mapsto \left(\frac{f}{h^2}(x), y \cdot \frac{g}{h^3}(x)\right)$

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r} x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-**Frobenius isogeny**.

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r} x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-Frobenius isogeny.

1. Frobenius are very important
2. In our case they are a bit of a nuisance for a theorem later on

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r}x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-**Frobenius isogeny**. Note if $k = \mathbb{F}_{p^r}$ then $E^{(p^r)} = E$

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r}x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-Frobenius isogeny. Note if $k = \mathbb{F}_{p^r}$ then $E^{(p^r)} = E$

1. Frobenius are very important
2. In our case they are a bit of a nuisance for a theorem later on

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r}x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-**Frobenius isogeny**. Note if $k = \mathbb{F}_{p^r}$ then $E^{(p^r)} = E$

If an isogeny factors trough a Frobenius isogeny it is inseparable. If it is a Frobenius followed by an isomorphisms, it is purely inseparable.

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r}x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-**Frobenius isogeny**. Note if $k = \mathbb{F}_{p^r}$ then $E^{(p^r)} = E$

If an isogeny factors trough a Frobenius isogeny it is inseparable. If it is a Frobenius followed by an isomorphisms, it is purely inseparable.

1. Frobenius are very important
2. In our case they are a bit of a nuisance for a theorem later on

» Separable and Inseparable Isogenies

Definition

Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r}x + b^{p^r}$. The map:

$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$

is the (p^r)-**Frobenius isogeny**. Note if $k = \mathbb{F}_{p^r}$ then $E^{(p^r)} = E$

If an isogeny factors trough a Frobenius isogeny it is inseparable. If it is a Frobenius followed by an isomorphisms, it is purely inseparable. We are mostly concerned with the separable case.

» Separable and Inseparable Isogenies
Definition
Let $E/k : y^2 = x^3 + ax + b$, with $\mathrm{char}(k) = p$. Define $E^{(p^r)} : y^2 = x^3 + a^{p^r}x + b^{p^r}$. The map:
$$\pi : E \to E^{(p^r)}, (x, y) \mapsto \left(x^{p^r}, y^{p^r}\right)$$
is the (p^r)-**Frobenius isogeny**. Note if $k = \mathbb{F}_{p^r}$ then $E^{(p^r)} = E$
If an isogeny factors trough a Frobenius isogeny it is inseparable. If it is a Frobenius followed by an isomorphisms, it is purely inseparable. We are mostly concerned with the separable case.

1. Frobenius are very important
2. In our case they are a bit of a nuisance for a theorem later on

» Kernel and Velu

Theorem

There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from that curve, up to post-compostion with isomorphisms

» Kernel and Velu

Theorem

There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from that curve, up to post-compostion with isomorphisms

» Kernel and Velu

Theorem

There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from that curve, up to post-compostion with isomorphisms

$$\textit{kernels} \longleftrightarrow \textit{isogenies}$$

» Kernel and Velu

Theorem

There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from that curve, up to post-compostion with isomorphisms

kernels ⟷ isogenies

» Kernel and Velu

Theorem

There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from that curve, up to post-compostion with isomorphisms

$$\textit{kernels} \longleftrightarrow \textit{isogenies}$$

Let E/k, with k a finite field. For any subgroup $H \leq E$ we can find an isogeny with kernel H in $\Theta(\#H)$ using Velu's formulas. We denote the target of that isogeny by E/H

» Kernel and Velu

Theorem

There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from that curve, up to post-compostion with isomorphisms

kernels ⟷ isogenies

Let E/k, with k a finite field. For any subgroup $H \leq E$ we can find an isogeny with kernel H in $\Theta(\#H)$ using Velu's formulas. We denote the target of that isogeny by E/H

» Computing large degree isogenies

* Velu's formula are too slow for large degree

4- Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker \psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and

$$\begin{tikzcd} E \arrow[r, "\psi_1"] \arrow[rrrr, bend left] & E_1 \arrow[r, "\psi_2"] & \cdots \arrow[r, "\psi_{k-1}"] & E_{k-1} \arrow[r, "\psi_k"] & E/H \end{tikzcd}$$

2022-01-07

Elliptic Curve Cryptography
└Elliptic Curves
└Isogenies
└Computing large degree isogenies

» Computing large degree isogenies

* Velu's formula are too slow for large degree

4- Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker \psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and

$E \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{k-1}} E_{k-1} \xrightarrow{\psi_k} E/H$

» Computing large degree isogenies

* Velu's formula are too slow for large degree
* Decompose ℓ^k isogenies in k ℓ-isogenies

4- Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker \psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and

$$\begin{tikzcd} E \arrow[r, "\psi_1"] \arrow[rrrr, bend left] & E_1 \arrow[r, "\psi_2"] & \cdots \arrow[r, "\psi_{k-1}"] & E_{k-1} \arrow[r, "\psi_k"] & E/H \end{tikzcd}$$

» Computing large degree isogenies
Velu's formula are too slow for large degree
Decompose ℓ^k isogenies in k ℓ-isogenies
4- Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker \psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and

» Computing large degree isogenies

- Velu's formula are too slow for large degree
- Decompose ℓ^k isogenies in k ℓ-isogenies
- Speedup from $\Theta(\ell^k)$ to $\Theta(k^2\ell)$

4- Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker\psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and

$$\begin{tikzcd} E \arrow[r, "\psi_1"] \arrow[rrrr, bend left] & E_1 \arrow[r, "\psi_2"] & \cdots \arrow[r, "\psi_{k-1}"] & E_{k-1} \arrow[r, "\psi_k"] & E/H \end{tikzcd}$$

» Computing large degree isogenies
Velu's formula are too slow for large degree
Decompose ℓ^k isogenies in k ℓ-isogenies
Speedup from $\Theta(\ell^k)$ to $\Theta(k^2\ell)$
4- Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker\psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

1. Endomorphism ring is a order in a quaternion algebra

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?

1. Endomorphism ring is a order in a quaternion algebra

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?
* There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?
* There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.

1. Endomorphism ring is a order in a quaternion algebra

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?
* There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.
* A supersingular curve has $p + 1$ points.

» Supersingular Curves

Definition
A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?
* There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.
* A supersingular curve has $p + 1$ points.

1. Endomorphism ring is a order in a quaternion algebra

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

- Something something order in a quaternion algebra?
- There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.
- A supersingular curve has $p + 1$ points.
- Insecure for DLP

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

- Something something order in a quaternion algebra?
- There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.
- A supersingular curve has $p + 1$ points.
- Insecure for DLP

1. Endomorphism ring is a order in a quaternion algebra

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?
* There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.
* A supersingular curve has $p + 1$ points.
* Insecure for DLP
* Secure for CSSI (later)!

» Supersingular Curves

Definition

A curve E defined over K with $\mathrm{char}(K) = p$ is **supersingular** if $[p]$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$. A curve that is not supersingular is **ordinary**

* Something something order in a quaternion algebra?
* There are $\approx \lfloor \frac{p}{12} \rfloor$ supersingular curves over $\mathbb{F}_{p^n}$.
* A supersingular curve has $p + 1$ points.
* Insecure for DLP
* Secure for CSSI (later)!

1. Endomorphism ring is a order in a quaternion algebra

» Isogeny Problems

It is easy to find out if two curves are isogenous

» Isogeny Problems

It is easy to find out if two curves are isogenous

» Isogeny Problems

It is easy to find out if two curves are isogenous

Theorem

Two curves E_1, E_2 over a finite field k are isogenous over k if and only if $\#E_1(k) = \#E_2(k)$.

» Isogeny Problems

It is easy to find out if two curves are isogenous

Theorem

Two curves E_1, E_2 over a finite field k are isogenous over k if and only if $\#E_1(k) = \#E_2(k)$.

» Isogeny Problems

It is easy to find out if two curves are isogenous

Theorem

Two curves E_1, E_2 over a finite field k are isogenous over k if and only if $\#E_1(k) = \#E_2(k)$.

Finding the isogeny is dramatically harder:

» Isogeny Problems

It is easy to find out if two curves are isogenous

Theorem

Two curves E_1, E_2 over a finite field k are isogenous over k if and only if $\#E_1(k) = \#E_2(k)$.

Finding the isogeny is dramatically harder:

» Isogeny Problems

It is easy to find out if two curves are isogenous

Theorem

Two curves E_1, E_2 over a finite field k are isogenous over k if and only if $\#E_1(k) = \#E_2(k)$.

Finding the isogeny is dramatically harder:

Definition

The **computational supersingular isogeny problem** is as follows: Given two supersingular elliptic curves E, E', find an isogeny between them.

2022-01-07

Elliptic Curve Cryptography
└─Elliptic Curves
  └─Isogenies
    └─Isogeny Problems

» Isogeny Problems

It is easy to find out if two curves are isogenous

Theorem

Two curves E_1, E_2 over a finite field k are isogenous over k if and only if $\#E_1(k) = \#E_2(k)$.

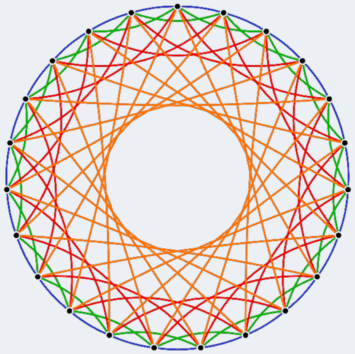
Finding the isogeny is dramatically harder:

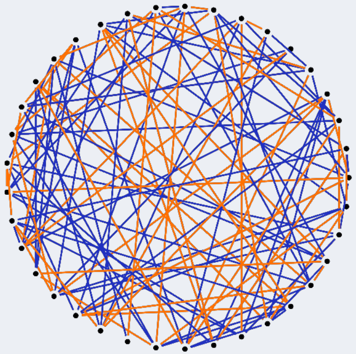
Definition

The **computational supersingular isogeny problem** is as follows: Given two supersingular elliptic curves E, E', find an isogeny between them.

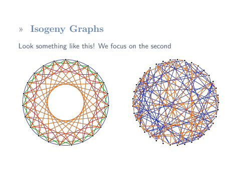
» Isogeny Graphs

Look something like this! We focus on the second





2022-01-07



1. CSIDH is pronounced Seaside

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

» Isogeny Graphs
Let p, ℓ be a primes, K a field of characteristic p.

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

- Vertices: Supersingular Elliptic curves over K

4- Both up to isomorphisms (i.e. vertices are j-invariants)

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

- Vertices: Supersingular Elliptic curves over K

4- Both up to isomorphisms (i.e. vertices are j-invariants)

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

* Vertices: Supersingular Elliptic curves over K
* Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-supersingular isogeny graph has as:

* Vertices: Supersingular Elliptic curves over K
* Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

* Vertices: Supersingular Elliptic curves over K
* Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

» Isogeny Graphs
Let p, ℓ be a primes, K a field of characteristic p.
Definition
The ℓ-**supersingular isogeny graph** has as:
Vertices: Supersingular Elliptic curves over K
Edges: Separable isogenies from $E \to E'$
4- Both up to isomorphisms (i.e. vertices are j-invariants)

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

- Vertices: Supersingular Elliptic curves over K
- Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

- We can represent vertices as elements of $\mathbb{F}_{p^2}$

» Isogeny Graphs
Let p, ℓ be a primes, K a field of characteristic p.
Definition
The ℓ-supersingular isogeny graph has as:
Vertices: Supersingular Elliptic curves over K
Edges: Separable isogenies from $E \to E'$
4- Both up to isomorphisms (i.e. vertices are j-invariants)
We can represent vertices as elements of $\mathbb{F}_{p^2}$

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

- Vertices: Supersingular Elliptic curves over K
- Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

- We can represent vertices as elements of $\mathbb{F}_{p^2}$
- Graph is directed

» Isogeny Graphs
Let p, ℓ be a primes, K a field of characteristic p.
Definition
The ℓ-supersingular isogeny graph has as:
Vertices: Supersingular Elliptic curves over K
Edges: Separable isogenies from $E \to E'$
4- Both up to isomorphisms (i.e. vertices are j-invariants)
We can represent vertices as elements of $\mathbb{F}_{p^2}$
Graph is directed

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

* Vertices: Supersingular Elliptic curves over K
* Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

* We can represent vertices as elements of $\mathbb{F}_{p^2}$
* Graph is directed
* Graph has good mixing properties

» Isogeny Graphs
Let p, ℓ be a primes, K a field of characteristic p.
Definition
The ℓ-supersingular isogeny graph has as:
Vertices: Supersingular Elliptic curves over K
Edges: Separable isogenies from $E \to E'$
4- Both up to isomorphisms (i.e. vertices are j-invariants)
We can represent vertices as elements of $\mathbb{F}_{p^2}$
Graph is directed
Graph has good mixing properties

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

- Vertices: Supersingular Elliptic curves over K
- Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

- We can represent vertices as elements of $\mathbb{F}_{p^2}$
- Graph is directed
- Graph has good mixing properties
- Can walk in the graph with Velu's method

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-supersingular isogeny graph has as:

- Vertices: Supersingular Elliptic curves over K
- Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

- We can represent vertices as elements of $\mathbb{F}_{p^2}$
- Graph is directed
- Graph has good mixing properties
- Can walk in the graph with Velu's method

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

The ℓ-**supersingular isogeny graph** has as:

- Vertices: Supersingular Elliptic curves over K
- Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

- We can represent vertices as elements of $\mathbb{F}_{p^2}$
- Graph is directed
- Graph has good mixing properties
- Can walk in the graph with Velu's method
- Most vertices have degree $\ell + 1$

» Isogeny Graphs

Let p, ℓ be a primes, K a field of characteristic p.

Definition

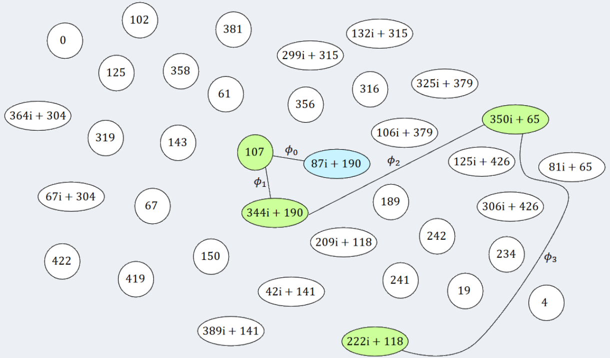
The ℓ-supersingular isogeny graph has as:

- Vertices: Supersingular Elliptic curves over K
- Edges: Separable isogenies from $E \to E'$

4- Both up to isomorphisms (i.e. vertices are j-invariants)

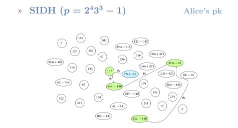
- We can represent vertices as elements of $\mathbb{F}_{p^2}$
- Graph is directed
- Graph has good mixing properties
- Can walk in the graph with Velu's method
- Most vertices have degree $\ell + 1$

» SIDH ($p = 2^4 3^3 - 1$) Alice's pk

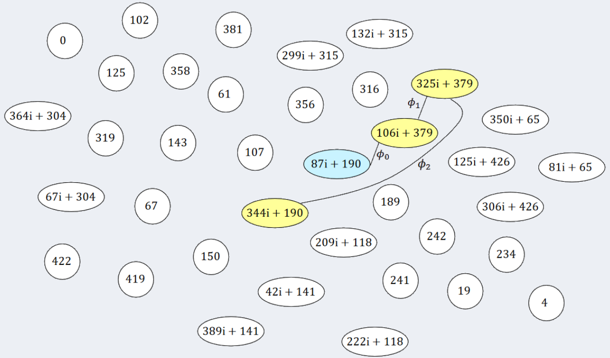


2022-01-07

Elliptic Curve Cryptography
└Elliptic Curves
└Isogenies
└SIDH ($p = 2^4 3^3 - 1$)

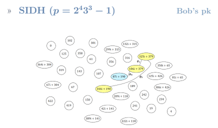


» SIDH ($p = 2^4 3^3 - 1$) Bob's pk

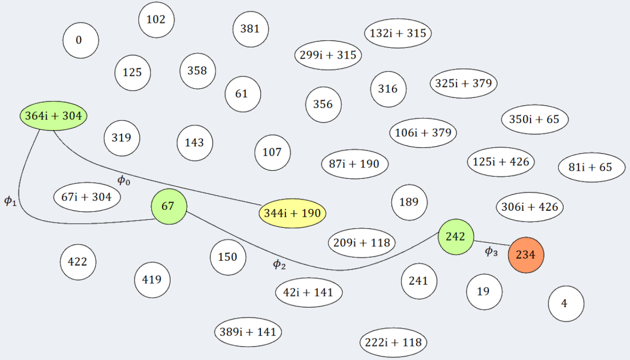


2022-01-07

Elliptic Curve Cryptography
└─Elliptic Curves
  └─Isogenies
    └─SIDH ($p = 2^4 3^3 - 1$)

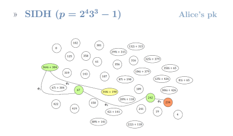


» SIDH ($p = 2^4 3^3 - 1$) Alice's pk

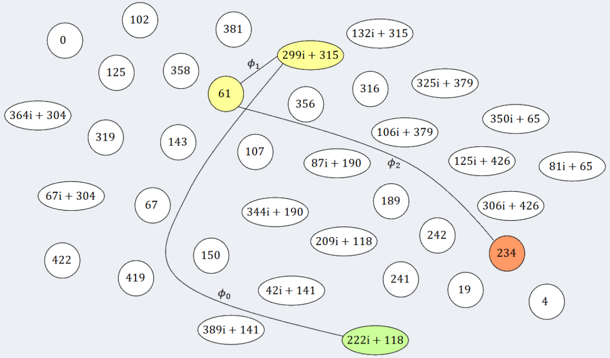


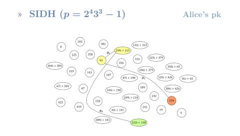
2022-01-07

Elliptic Curve Cryptography
└Elliptic Curves
  └Isogenies
    └SIDH ($p = 2^4 3^3 - 1$)



» SIDH ($p = 2^4 3^3 - 1$) Alice's pk





» SIDH

Picture to keep in mind:

$$
\begin{tikzcd}
E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & E/\langle A\rangle \arrow[d, "\phi'_B"] \\
E/\langle B\rangle \arrow[r, "\phi'_A"'] & E/\langle A,B\rangle
\end{tikzcd}
$$

Details will follow

» SIDH

Picture to keep in mind:

Details will follow

1. Alice computes the left to right ones
2. Bob computes the down arrows

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime,

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime,

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$,

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$,

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.
* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A \rangle = E[2^{e_A}], \langle P_B, Q_B \rangle = E[3^{e_B}]$.

- Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
- Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A \rangle = E_A$

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A \rangle = E[2^{e_A}], \langle P_B, Q_B \rangle = E[3^{e_B}]$.
- Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
- Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A \rangle = E_A$

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A\rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B\rangle = E_B$

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.
* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A\rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B\rangle = E_B$

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A\rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B\rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.
* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A\rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B\rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A \rangle = E[2^{e_A}], \langle P_B, Q_B \rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$\, \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$\, \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A \rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B \rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$
* Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_A : E_B \to E/\langle S'_A \rangle = E_{AB}$

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A \rangle = E[2^{e_A}], \langle P_B, Q_B \rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$\, \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$\, \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A \rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B \rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$
* Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_A : E_B \to E/\langle S'_A \rangle = E_{AB}$

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A\rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B\rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$
* Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_A : E_B \to E/\langle S'_A\rangle = E_{AB}$
* Bob computes $S'_B = P'_A + [n_B]Q'_A$, and an isogeny $\phi'_B : E_A \to E/\langle S'_B\rangle = E_{BA}$

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A\rangle = E[2^{e_A}], \langle P_B, Q_B\rangle = E[3^{e_B}]$.
* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A\rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B\rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$
* Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_A : E_B \to E/\langle S'_A\rangle = E_{AB}$
* Bob computes $S'_B = P'_A + [n_B]Q'_A$, and an isogeny $\phi'_B : E_A \to E/\langle S'_B\rangle = E_{BA}$

» SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A \rangle = E[2^{e_A}], \langle P_B, Q_B \rangle = E[3^{e_B}]$.

* Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
* Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A \rangle = E_A$
* Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B \rangle = E_B$
* The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$
* Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_A : E_B \to E/\langle S'_A \rangle = E_{AB}$
* Bob computes $S'_B = P'_A + [n_B]Q'_A$, and an isogeny $\phi'_B : E_A \to E/\langle S'_B \rangle = E_{BA}$
* The final secret is $j(E_{AB}) = j(E_{BA})$

» SIDH
Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve $E/\mathbb{F}_{p^2}$, four points P_A, P_B, Q_A, Q_B s.t. $\langle P_A, Q_A \rangle = E[2^{e_A}], \langle P_B, Q_B \rangle = E[3^{e_B}]$.
Alice, Bob sample $n_A \leftarrow\$ \mathbb{Z}_{2^{e_A}}, n_B \leftarrow\$ \mathbb{Z}_{3^{e_B}}$, and compute $S_X = P_X + [n_X]Q_X$
Alice computes the 2^{e_A} isogeny $\phi_A : E \to E/\langle S_A \rangle = E_A$
Bob computes the 3^{e_B} isogeny $\phi_B : E \to E/\langle S_B \rangle = E_B$
The public keys are $\mathrm{pk}_X = (E_X, P'_X = \phi_X(P_X), Q'_X = \phi_X(Q_X))$
Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_A : E_B \to E/\langle S'_A \rangle = E_{AB}$
Bob computes $S'_B = P'_A + [n_B]Q'_A$, and an isogeny $\phi'_B : E_A \to E/\langle S'_B \rangle = E_{BA}$
The final secret is $j(E_{AB}) = j(E_{BA})$

» SIDH and SIKE

* SIDH is vulnerable to active attacks

» SIDH and SIKE

* SIDH is vulnerable to active attacks

» SIDH and SIKE

* SIDH is vulnerable to active attacks
* SIKE uses the Fujisaki-Okamoto transform to fix this
* SIKE in the Alternate Candidates of Round 3 of the NIST PQC competion

» SIDH and SIKE

* SIDH is vulnerable to active attacks
* SIKE uses the Fujisaki-Okamoto transform to fix this
* SIKE in the Alternate Candidates of Round 3 of the NIST PQC competion

» SIDH and SIKE

- SIDH is vulnerable to active attacks
- SIKE uses the Fujisaki-Okamoto transform to fix this
- SIKE in the Alternate Candidates of Round 3 of the NIST PQC competion
- Very short keys
- Currently a bit on the slow side

» SIDH and SIKE

- SIDH is vulnerable to active attacks
- SIKE uses the Fujisaki-Okamoto transform to fix this
- SIKE in the Alternate Candidates of Round 3 of the NIST PQC competion
- Very short keys
- Currently a bit on the slow side

» SIDH and SIKE

* SIDH is vulnerable to active attacks
* SIKE uses the Fujisaki-Okamoto transform to fix this
* SIKE in the Alternate Candidates of Round 3 of the NIST PQC competion
* Very short keys
* Currently a bit on the slow side
* Best known attack is classical

» SIDH and SIKE

* SIDH is vulnerable to active attacks
* SIKE uses the Fujisaki-Okamoto transform to fix this
* SIKE in the Alternate Candidates of Round 3 of the NIST PQC competion
* Very short keys
* Currently a bit on the slow side
* Best known attack is classical

» Security

Best attack is on CSSI problem.

» Security

Best attack is on CSSI problem.

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$.

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$.

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$. Let $k \approx a/2$ and

$$S_{i,k} := \left\{ H \leq E_i[\ell^k] \mid H \text{ cyclic}, |H| = \ell^k \right\}$$
$$S := (\{0\} \times S_{0,k}) \sqcup (\{1\} \times S_{1,k})$$
$$g : S \to \mathbb{F}_{p^2},\ (i, H) \mapsto j(E_i/H)$$

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$. Let $k \approx a/2$ and

$$S_{i,k} := \left\{ H \leq E_i[\ell^k] \mid H \text{ cyclic}, |H| = \ell^k \right\}$$
$$S := (\{0\} \times S_{0,k}) \sqcup (\{1\} \times S_{1,k})$$
$$g : S \to \mathbb{F}_{p^2},\ (i, H) \mapsto j(E_i/H)$$

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$. Let $k \approx a/2$ and

$$S_{i,k} := \left\{ H \leq E_i[\ell^k] \mid \ H \text{ cyclic}, |H| = \ell^k \right\}$$
$$S := (\{0\} \times S_{0,k}) \sqcup (\{1\} \times S_{1,k})$$
$$g : S \to \mathbb{F}_{p^2},\ (i, H) \mapsto j(E_i/H)$$

A collision $g(0,H) = g(1,H')$ will solve CSSI.

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$. Let $k \approx a/2$ and

$$S_{i,k} := \left\{ H \leq E_i[\ell^k] \mid \ H \text{ cyclic}, |H| = \ell^k \right\}$$
$$S := (\{0\} \times S_{0,k}) \sqcup (\{1\} \times S_{1,k})$$
$$g : S \to \mathbb{F}_{p^2},\ (i, H) \mapsto j(E_i/H)$$

A collision $g(0,H) = g(1,H')$ will solve CSSI.

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$. Let $k \approx a/2$ and

$$S_{i,k} := \left\{ H \leq E_i[\ell^k] \mid H \text{ cyclic}, |H| = \ell^k \right\}$$
$$S := (\{0\} \times S_{0,k}) \sqcup (\{1\} \times S_{1,k})$$
$$g : S \to \mathbb{F}_{p^2}, \ (i, H) \mapsto j(E_i/H)$$

A collision $g(0, H) = g(1, H')$ will solve CSSI. To enable Pollard-Rho style methods, let $h : \mathbb{F}_{p^2} \to S$ be a hash function, and let:

$$f : S \to S, \ f := h \circ g$$

» Security

Best attack is on CSSI problem. Suppose we want to find an ℓ^a-isogeny between $E_0 \to E_1$, both supersingular and over $\mathbb{F}_{p^2}$. Let $k \approx a/2$ and

$$S_{i,k} := \left\{ H \leq E_i[\ell^k] \mid H \text{ cyclic}, |H| = \ell^k \right\}$$
$$S := (\{0\} \times S_{0,k}) \sqcup (\{1\} \times S_{1,k})$$
$$g : S \to \mathbb{F}_{p^2}, \ (i, H) \mapsto j(E_i/H)$$

A collision $g(0, H) = g(1, H')$ will solve CSSI. To enable Pollard-Rho style methods, let $h : \mathbb{F}_{p^2} \to S$ be a hash function, and let:

$$f : S \to S, \ f := h \circ g$$

» Security

h maps a set $\approx p/12$ to S which has size $\approx p^{1/4}$ so introduces a lot of collisions.

» Security

h maps a set $\approx p/12$ to S which has size $\approx p^{1/4}$ so introduces a lot of collisions.

» Security

h maps a set $\approx p/12$ to S which has size $\approx p^{1/4}$ so introduces a lot of collisions. To find a 'golden' one we use the van Oorschot Wiener (vOW) algorithm.

» Security

h maps a set $\approx p/12$ to S which has size $\approx p^{1/4}$ so introduces a lot of collisions. To find a 'golden' one we use the van Oorschot Wiener (vOW) algorithm.

» Security

h maps a set $\approx p/12$ to S which has size $\approx p^{1/4}$ so introduces a lot of collisions. To find a 'golden' one we use the van Oorschot Wiener (vOW) algorithm. When using m processors and w memory cells, time complexity is

$$\frac{2.5}{m}\sqrt{\#S^3/w} \cdot t = O(p^{3/8})$$

» Security

h maps a set $\approx p/12$ to S which has size $\approx p^{1/4}$ so introduces a lot of collisions. To find a 'golden' one we use the van Oorschot Wiener (vOW) algorithm. When using m processors and w memory cells, time complexity is

$$\frac{2.5}{m}\sqrt{\#S^3/w} \cdot t = O(p^{3/8})$$

Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!

» Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!

» Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!
- ECDH base of most of the web's key exchanges

» Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!
- ECDH base of most of the web's key exchanges

» Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!
- ECDH base of most of the web's key exchanges
- BLS Pairing based signatures both efficient and secure

» Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!
- ECDH base of most of the web's key exchanges
- BLS Pairing based signatures both efficient and secure

» Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!
- ECDH base of most of the web's key exchanges
- BLS Pairing based signatures both efficient and secure
- SIKE leverages isogenies for post quantum security

» Conclusion

- Elliptic curves are pretty damn cool
- We only scratched the surface!
- ECDH base of most of the web's key exchanges
- BLS Pairing based signatures both efficient and secure
- SIKE leverages isogenies for post quantum security

» Resources

0 J.H. Silverman, J.T. Tate, Rational Points on Elliptic Curves
1 .H. Silverman, The Arithmetic of Elliptic Curves[1]
2 D.A. Cox, Primes of the form $x^2 + ny^2$
3,4 L. Panny, notes: [intro] [isogenies problems]
5 C. Costello, Supersingular isogeny key exchange for beginners
6 R. Granger, A. Joux, Computing Discrete Logarithms [5.2, 5.3]
7 P. Aluffi, Algebra: Chapter 0
8 S. Galbraith, Mathematics of Public Key Cryptography

[1] The bible

2022-01-07

Elliptic Curve Cryptography
└─Resources
└─Resources

» Resources

0 J.H. Silverman, J.T. Tate, Rational Points on Elliptic Curves
1 .H. Silverman, The Arithmetic of Elliptic Curves[1]
2 D.A. Cox, Primes of the form $x^2 + ny^2$
3,4 L. Panny, notes: [intro] [isogenies problems]
5 C. Costello, Supersingular isogeny key exchange for beginners
6 R. Granger, A. Joux, Computing Discrete Logarithms [5.2, 5.3]
7 P. Aluffi, Algebra: Chapter 0
8 S. Galbraith, Mathematics of Public Key Cryptography

[1] The bible

» Detailed References & Credits

- Historical Notes follow mostly [0, Introduction]
- Origin of the name elliptic can be found [here]
- Fields discussed in [7, III.1.14, VII]
- Weierstrass form in [1, III.1]
- Definition of elliptic curve [1, III.2.2, III.3] or [0, 2.2]
- Elliptic curves diagram from [iacr] and curves from [1, Fig 3.1, 3.2]
- Discriminant, j-invariant formula from [1, III.1]
- Discriminant interpretation [0, 2.3]
- Isomorphism form [1, III.3.1b]
- Theorem j-invariance [1, III.1.4b]

2022-01-07

Elliptic Curve Cryptography
└─Resources
  └─Detailed References
    └─Detailed References & Credits

» Detailed References & Credits
- Historical Notes follow mostly [0, Introduction]
- Origin of the name elliptic can be found [here]
- Fields discussed in [7, III.1.14, VII]
- Weierstrass form in [1, III.1]
- Definition of elliptic curve [1, III.2.2, III.3] or [0, 2.2]
- Elliptic curves diagram from [iacr] and curves from [1, Fig 3.1, 3.2]
- Discriminant, j-invariant formula from [1, III.1]
- Discriminant interpretation [0, 2.3]
- Isomorphism form [1, III.3.1b]
- Theorem j-invariance [1, III.1.4b]

» Detailed References & Credits

- Group Law diagram [0, Fig 1.16]
- Formulae [1, III.2.3]
- Scalar multiplication notation [1, III.2]
- Multiplication isogeny [1, III.4.1]
- Double and add [1, XI.1]
- Torsion subgroup [1, III.4]
- Hasse's theorem [1, V.1.1]
- Schoof's algorithm [1, XI.3]
- DLP and related assumption [8. III.13]
- Partial Equivalence of CHD and DLP in [Maurer] [Fifield]

» Detailed References & Credits

- Group Law diagram [0, Fig 1.16]
- Formulae [1, III.2.3]
- Scalar multiplication notation [1, III.2]
- Multiplication isogeny [1, III.4.1]
- Double and add [1, XI.1]
- Torsion subgroup [1, III.4]
- Hasse's theorem [1, V.1.1]
- Schoof's algorithm [1, XI.3]
- DLP and related assumption [8. III.13]
- Partial Equivalence of CHD and DLP in [Maurer] [Fifield]

» Detailed References & Credits

- Representation example expanded in [6, 5.3.1]
- Complexity estimates from [0, 4.5] and [1, XI.4]
- Diffie Hellman from [everywhere?]
- Singular curves are bad [0, 3.15] and [1, III.2.5] and [6, 5.3.3]
- Small Embedding degree ECDLP [1, XI.6] and [6, 5.2.2]
- Supersingular curves breaking ECDLP [1, XI.6.4] and [6, 5.2.2]
- Anomalous curves breaking ECDLP [1, XI.6.5] and [6, 5.2.2] and [6, 5.3.3]
- Descent methods in [6, 5.2.2]
- Pollard Rho description [1, XI.5.3-5.4]
- Pairings adapted from [1, III.8.1]
- Weil Pairing computation [1, XI.8]
- Modified Weil Pairing and Distorsion map [1, XI.7]

» Detailed References & Credits
- Representation example expanded in [6, 5.3.1]
- Complexity estimates from [0, 4.5] and [1, XI.4]
- Diffie Hellman from [everywhere?]
- Singular curves are bad [0, 3.15] and [1, III.2.5] and [6, 5.3.3]
- Small Embedding degree ECDLP [1, XI.6] and [6, 5.2.2]
- Supersingular curves breaking ECDLP [1, XI.6.4] and [6, 5.2.2]
- Anomalous curves breaking ECDLP [1, XI.6.5] and [6, 5.2.2] and [6, 5.3.3]
- Descent methods in [6, 5.2.2]
- Pollard Rho description [1, XI.5.3-5.4]
- Pairings adapted from [1, III.8.1]
- Weil Pairing computation [1, XI.8]
- Modified Weil Pairing and Distorsion map [1, XI.7]

» Detailed References & Credits

- BLS Signatures [1, XI.7.4]
- Isogeny definition [1, III.4]
- Isogeny Example from [3, 2.1]
- Isogeny properties (summary) [3, 2.1]
- Isogeny and Group Hom. [1, III.4.8]
- Isogeny composition, degree and multiplicativity [1, III.4]
- Dual Isogeny [1, III.6]
- Frobenius isogeny and separability [3, 2.1.2]
- Kernels and Velu [3, 2.2] and [1, III.4.12]
- Supersingular curves [1, V.3.1]
- Number of curves [1, V.4.1c]
- Points of supersingular curve [3, 1.8]

» Detailed References & Credits
- BLS Signatures [1, XI.7.4]
- Isogeny definition [1, III.4]
- Isogeny Example from [3, 2.1]
- Isogeny properties (summary) [3, 2.1]
- Isogeny and Group Hom. [1, III.4.8]
- Isogeny composition, degree and multiplicativity [1, III.4]
- Dual Isogeny [1, III.6]
- Frobenius isogeny and separability [3, 2.1.2]
- Kernels and Velu [3, 2.2] and [1, III.4.12]
- Supersingular curves [1, V.3.1]
- Number of curves [1, V.4.1c]
- Points of supersingular curve [3, 1.8]

» Detailed References & Credits

- Isogenous with same number of points [1, Ex. 5.4]
- Graphs from L. Panny's [lekenpraatje]
- Vertices as elements of $\mathbb{F}_{p^2}$ from [1, V.3.1]
- Good mixing properties from [CGL06]
- SIDH diagrams and description from [5]
- SIKE [sike]
- vOW function from [4, 3.1] and [ACV+18]
- vOW description [4, 3.2] and [vOW98]

» Detailed References & Credits

- Isogenous with same number of points [1, Ex. 5.4]
- Graphs from L. Panny's [lekenpraatje]
- Vertices as elements of $\mathbb{F}_{p^2}$ from [1, V.3.1]
- Good mixing properties from [CGL06]
- SIDH diagrams and description from [5]
- SIKE [sike]
- vOW function from [4, 3.1] and [ACV+18]
- vOW description [4, 3.2] and [vOW98]

» Further Reading

* Attacks on SIDH [torsion] [GPST]
* Mathematics of Isogeny Based Cryptography [deFeo17]
* vOW attack estimation [vOW98] [ACV+18] [CLN+19] [LWS20]
* Verifiable Delay Functions from Isogenies and Pairings [dFMPS19]
* Delfs-Galbraith attack [DG16] [SCS21]

» Further Reading

* Attacks on SIDH [torsion] [GPST]
* Mathematics of Isogeny Based Cryptography [deFeo17]
* vOW attack estimation [vOW98] [ACV+18] [CLN+19] [LWS20]
* Verifiable Delay Functions from Isogenies and Pairings [dFMPS19]
* Delfs-Galbraith attack [DG16] [SCS21]