an introduction which is entirely too short

by Giacomo Fenzi (ETH Zurich)
on 6 January 2022



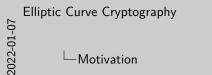
Conclusion
o

Resource0
00000
0

» Motivation

'It is possible to write endlessly on elliptic curves.

(This is not a threat.)' Serge Lang





Conclusion
o

Resources

» Motivation

'It is possible to write endlessly on elliptic curves.

(This is not a threat.)' Serge Lang

* Elliptic curves are everywhere in cryptography

Elliptic Curve Cryptography CO-10-2000 Motivation



c Curves

nclusion

Resources 0 00000 0

» 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

Elliptic Curve Cryptography Color Motivation

Power ≈ 70% of TLS Exchanges

'It is possible to write endlessly on elliptic curves.

(This is not a threat.)' Sery

Elliptic curves are everywhere in cryptography

» Motivation

ground Elliptic Ct

onclusion

Resources
0
00000
0

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

Elliptic Curve Cryptography

Motivation

This possible to write endlessly on elliptic curves.

(This is not a threat.)*

Elliptic curves are everywhere in crystography
Power = 70% of TLS berchanges
Coolest pool quantum crystography proposal

» Motivation

ackground

c Curves

nclusion

Resources

0

00000

2022-01-07

» 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

Elliptic Curve Cryptography --Motivation

'It is possible to write endlessly on elliptic curves.

(This is not a threat.)'

Elliptic curves are everywhere in cryptography

Power ≈ 70% of TLS Exchanges

Coolest post quantum cryptography proposal

Fascinating mathematically

» Motivation

lliptic Curves

onclusion

cooo

2022-01-07

Elliptic Curve Cryptography

» Outline

• Historical Notes

Outline

» Outline

* Historical Notes



- * Historical Notes
- * Mathematical Background

Elliptic Curve Cryptography 2022-01-07

└─Outline

 Historical Notes Mathematical Background

» Outline

History Backgrou

lliptic Curves

Conclusion
o

Resource 0 00000 0

0000

Outline

- * Historical Notes
- * Mathematical Background
- * Addition on Elliptic Curves

Elliptic Curve Cryptography

» Outline

Historical Notes
 Mathematical Background
 Addition on Elliptic Curves

2022-01-07

└─Outline

History Backgro

cound Elliptic Curves

Conclusion

o

Resources

2022-01-07

Elliptic Curve Cryptography

└─Outline

Mathematical Background
 Addition on Eliptic Curves
 Uncrete Logarithm and Diffe Hellman

» Outline

Historical Notes

» Outline

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

listory Backgr

Elliptic Curves
0000000000
0000000

Conclusion

O

Resources 0 00000 0

Outline

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

Elliptic Curve Cryptography

2022-01-07

└─Outline

» Outline

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

iscrete Logarithm a airings History Backgro

Elliptic Curves
00000000000
0000000

nclusion

Resources 0 00000 0

Outline

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

Elliptic Curve Cryptography

2022-01-07

└─Outline

» Outline

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

- Pairings - Isogenies



ackground

ptic Curves

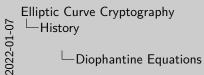
nclusion

Resources

Diophantine Equations

Historically originated in the context of solving Diophantine equations such as

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





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

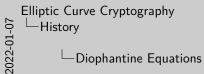
» Diophantine Equations

Historically originated in the context of solving Diophantine equations such as

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

or equivalently

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





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

» Diophantine Equations

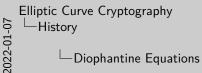
Historically originated in the context of solving Diophantine equations such as

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

or equivalently

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

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



Historically originated in the context of solving Diophantine equations such as $X^n+Y^n=Z^n,\ X,Y,Z\in \mathbb{Z}$ or equivalently $x^n+y^n=1,\ x,y\in \mathbb{Q}$

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

» Diophantine Equations

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



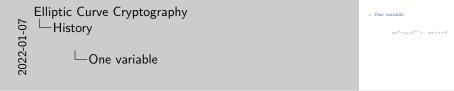
Background 1000 liptic Curves
000000000
00000

nclusion

Resource

» One variable

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



1. Uses Gauss' Lemma

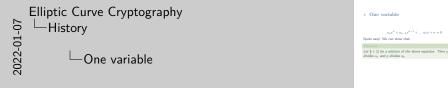
» One variable

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

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 .



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 $\frac{b}{a_n}$

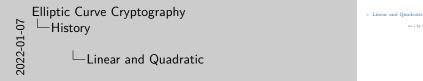


1. Uses Gauss' Lemma



Linear and Quadratic

$$ax + by = c$$



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

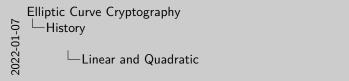
ax + by = c

» 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 Therein Hamiltonian Hamiltonian

- 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.

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



- 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

- 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

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

ptic Curves
00000000

onclusion

Resource

» 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

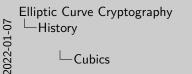
What about:

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

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 $a^2 + b^2 y + cyy^2 + dy^4 + cz^2 + fxy + yy^2 + hx + iy + j = 0.7$ This is the general form of an elliptic curved. We have that $a^2 + b^2 y + cxy^2 + dy^4 + cz^2 + fxy + yy^2 + hx + iy + j = 0.7$ This is the general form of an elliptic curved. We have that $a^2 + b^2 y + cxy^2 + dy^4 + cz^2 + fxy + yy^2 + hx + iy + j = 0.7$ This is the general form of an elliptic curved. We have that $a^2 + b^2 y + cxy^2 + dy^4 + cz^2 + fxy + yy^2 + hx + iy + j = 0.7$ This is the general form of an elliptic curved. We have that $a^2 + b^2 y + cxy^2 + dy^4 + cz^2 + fxy + yy^2 + hx + iy + j = 0.7$ This is the general form of an elliptic curved. We have that

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

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

What about:

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

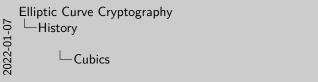
This is the general form of an elliptic curve! We have that

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 ≠ **Ellipse**



s. Cublics. What about: $a^2+b^2y+cyp^2+hy^2+cx^2+fxy+gy^2+hx+iy+j=0.7$ This is the general form of an elliptic cover! We have that [Execus : [Execus : A] excession global, and if has a settional point from they grow of existing points of first the grow of existing points of first points of grow of the existing points of first grow grow of existing points of first grow grow of existing points of first grow of grow of existing points of first grow of existing points of first grow of existing points of

Elliptic Curves + 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

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





Background

•000

otic Curves

nclusion

Resources

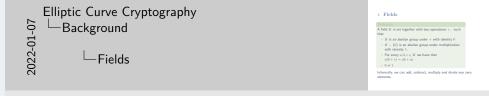
» Fields

Definition

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

- $\ast~K$ is an abelian group under + with identity 0
- * $K-\{0\}$ is an abelian group under multiplication with identity 1.
- \ast 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.:

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

2022-01-07

» 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.

Elliptic Curve Cryptography
Background
Finite Fields

» Finite Fields We are mostly interested in finite fields. $For every prime p, and every n \in \mathbb{Z}^+ \text{ then } k \text{ art unique} \\ field of size p^*, which we denote by where <math>G(\mathbb{P}_p)$ or \mathbb{P}_p in one was case them as $\mathbb{F}_p = \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p \mathbb{F}_$

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

» Characteristic

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

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

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



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

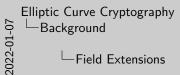


Background ○○○● tic Curves 0000000 000 nclusion

Resources

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 $k\subseteq K$.

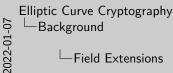
- 1. Closures are always infinite
- 2. Can approximate $\bar{\mathbb{F}}$ with $\mathbb{F}_{p^n!}$
- 3. Base of Galois theory

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 K which is the smallest algebraically closed extension containing K. Some examples:

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



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:

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

* $\mathbb{F}_{a} \subseteq \mathbb{F}_{a^{2}} \subseteq \mathbb{F}_{a^{2}} \dots \subseteq \mathbb{F}_{a}$

» Field Extensions

-Field Extensions

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

0000

Weierstrass Form

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

4-Much easier to manage!



» Weierstrass Form $\alpha x^2 + bx^2y + cxy^2 + dy^2 + cx^2 + fxy + gy^2 + hx + iy + j = 0$

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

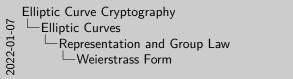
Weierstrass Form

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

$$\downarrow$$

$$y^{2} + axy + by = x^{3} + cx^{2} + dx + e$$

4-Much easier to manage!



» Weierstrass Form $ax^2+bx^2y+cxy^2+dy^3+cx^2+fxy+gy^2+hx+iy+j=0$ $y^2+axy+by=x^2+cx^2+dx+\epsilon$

4-Much easier to managel

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

Weierstrass Form

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

$$\downarrow$$

$$y^{2} + axy + by = x^{3} + cx^{2} + dx + e$$

$$\downarrow \operatorname{char}(K) \neq 2, 3$$

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

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)
- 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 Curve Cryptography
Color Elliptic Curves
Representation and Group Law
Elliptic Curves



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

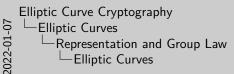
Definition

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

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



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

Definition

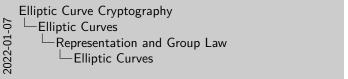
Let k be a field. An elliptic curve E over k (denoted by E/k) is given by

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

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

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

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 $E.k.b.a.s. fold. An elliptic curve E over k (denoted by E/k) is given by <math display="block">E:y^2=y^2+ax+b$ for $a,b\in k$. For any estamion $k\in K$ we define $E(K)=\{(x,y)\in K: K\mid y^2=x^2+ax+b\}\cup \{\infty\}$ Mathematicies are often interested with $E(0)\subseteq E(K)\subseteq E(0)$ but we multiy consider the finite case.

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

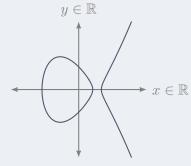
Background

Elliptic Curves

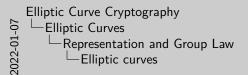
onclusion

Resource

Elliptic curves

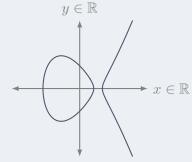


$$y^2 = x^3 - 2x + 1 \text{ over } \mathbb{R}$$

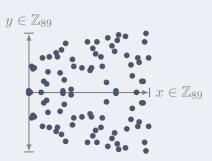




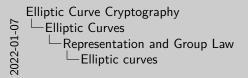
Elliptic curves

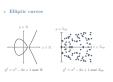


$$y^2 = x^3 - 2x + 1 \text{ over } \mathbb{R}$$

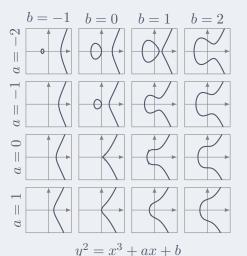


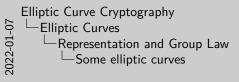
$$y^2 = x^3 - 2x + 1 \text{ over } \mathbb{Z}_{89}$$





» Some elliptic curves





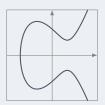


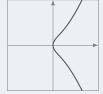
More elliptic curves

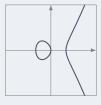
$$y^2 = x^3 + -3x + 3 \qquad \qquad y^2 = x^3 + x$$

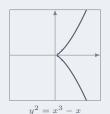
$$u^2 = 1$$

$$y^2 = x^3 - x$$











Elliptic Curve Cryptography 2022-01-07 Elliptic Curves -Representation and Group Law └─More elliptic curves



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

» Discriminant

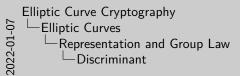
Definition

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 $\Delta = 0$.





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.

Elliptic Curve Cryptography

Elliptic Curves

Representation and Group Law
Discriminant

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.

Elliptic Curve Cryptography
Co-10
Representation and Group Law
Discriminant

* Discriminant

Let $E: y^2 = x^2 + xx + h$ is an elliptic curve.

The discriminant of E is $\Delta = -16(4x^2 + 27x^2)$ A curve is singular if $\Delta = 0$.

Alternatively, let $E: y^2 = (1/2, and \text{ for } x_1, x_2, x_3 \text{ is the works})$ $F = -2x^2 = (-1/2, -2x^2)^2(x_2 - x^2)^2$ i.e. $\Delta = 0$ or = f has a superiori root.

From now on, all curves are assumed non ningular.

ackground

onclusion

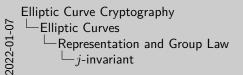
Resources

\rightarrow j-invariant

Definition

The j-invariant of E is

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





» j-invariant

Definition

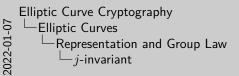
The j-invariant of E is

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

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

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

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





\gg 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

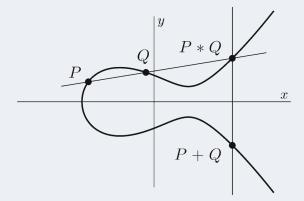
Let E, E' be two elliptic curves over K. Then $E \cong E'$ over \overline{K} if and only if j(E) = j(E').

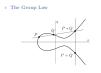
Elliptic Curve Cryptography $\begin{tabular}{l} \begin{tabular}{l} \b$

by j-invariant [Statement of E is The j-invariant of E is The j-invariant of E is $f(E) = -172(\frac{44}{\Delta})^2$. In fact, an isomorphism from source in other Weiserbrass form must necessity $(E, y_j) + (u^2, u^2, u^2)$ for $u \in \mathbb{R}^n$ and this yields:

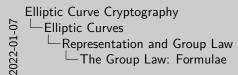
Let $E \in \mathbb{R}^n$ be no elliptic curves over K. Then $E \cong E'$ over K = B and $u^2 \neq f(E) = f(E)$.

» The Group Law





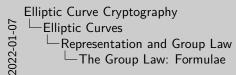
Let $E: y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$.



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

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 $-P_0=(x_0,-y_0)$

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 $P_1 + P_2$:

Elliptic Curve Cryptography

Elliptic Curves

Representation and Group Law

The Group Law: Formulae

» 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 $-P_0 = (x_0, -y_0)$

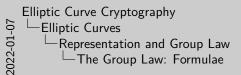
Now, for $P_1 + P_2$:

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 $E\colon y^2=x^3+ax+b$ be an elliptic curve. Let $P_1=(x_i,y_i)\in E(K).$ Define $-P_0=(x_0,-y_0)$

Now, for P_1+P_2 : $*\ \ \mbox{If } x_1=x_2 \ \mbox{and} \ \ y_1=-y_2, \ \mbox{then} \ \ P_1+P_2=\infty$

Elliptic Curves 00000000000

» 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.

Elliptic Curve Cryptography 2022-01-07 Elliptic Curves Representation and Group Law The Group Law: Formulae

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

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

Elliptic Curve Cryptography
Color Elliptic Curves
Representation and Group Law
The Group Law: Formulae

» The Group Law: Formulae Let $E: y^2 = x^2 + ax + b$ be an elliptic curve. Let $P_1 = (x_1, y_1) \in E(K)$. 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 viscoursa. Let $x_3=\lambda^2-x_1-x_2$, $y_3=\lambda(x_1-x_3)-y_1$ where λ is:

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

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 $E\colon y^2=x^3+ax+b$ be an elliptic curve. Let $P_1=(x_1,y_0)\in E(K).$ Define $-P_0=(x_0,-y_0)$

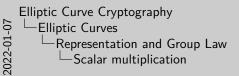
Now, for $P_1 + P_2$: • If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$ • If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.

Let $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where λ is: $\lambda = \begin{cases} \frac{2x - y_1}{2x_1^2 + y_2}, & x_1 \neq x_2 \\ \frac{2x_1^2 + y_2}{2x_1^2}, & \text{otherwise} \end{cases}$

This makes E into an abelian group with identity ∞

Scalar multiplication

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



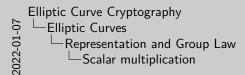
» Scalar multiplication For $n > 0, P \in E$ we write $[n]P = P + \cdots + P$. We then extend the notation by letting $[0]P = \infty$ and [-n]P = [n](-P).

Scalar multiplication

For $n > 0, P \in E$ we write $[n]P = \underbrace{P + \dots + P}_{n \text{ times}}$. 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 $[n]P=\underbrace{P+\cdots+P}_{n\text{ triese}}$. 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 $[n]P = \underbrace{P + \dots + P}_{n \text{ times}}$. 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.

Elliptic Curve Cryptography
Color Elliptic Curves
Representation and Group Law
Color Scalar multiplication

» Scalar multiplication

For n > 0, $P \in E$ we write $[n]P = \underbrace{P + \cdots + P}_{n-1}$. We then extend the notation by letting $[0]P = \infty$ and $\frac{1^{n}m}{n}P = [n](P - P)$. We can compute [n]P in $\Theta(\log n)$ group operations using double and add.

For $m \in \mathbb{Z}$ we define a $\max_{n} [n] : E \to E$ accordingly, and write: $\mathbb{E}[n] = \max_{n} [n]$

to be the m-torsion subgroup of E.

ackground

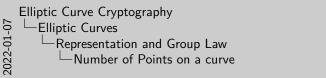
Elliptic Curves

nclusion

Resources
0
00000

Number of Points on a curve

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



» Number of Points on a curve $\label{eq:heavistically, we expect} \text{Heuristically, we expect} \approx q+1 \text{ points}$

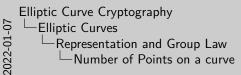
- 1. Each value of x yields at most two of y
- 2. a random element has 50% of being quadratic residue

Number of Points on a curve

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

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

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





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

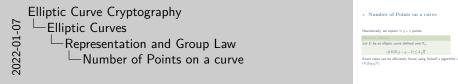
Heuristically, we expect $\approx q+1$ points

Theorem (Hasse

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

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

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



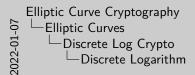
kground Elliptic Curves

Conclusion 0

Resource

» 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

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

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

Elliptic Curve Cryptography

Elliptic Curves

Elliptic Curves

Discrete Log Crypto

Discrete Logarithm

a Discrete Logarithm Crystopulyr risks on hardness manuspican. Let $Cu(1)^{-1}$ be a pair, algorithm that returns a group discrete $(-1)^{-1}$ be a pair, algorithm to the risks of -1 pair of -1 pairs of -1



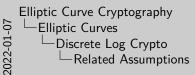
ckground

onclusion

Resources
0
00000
0

» Related Assumptions

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



» Related Assumptions

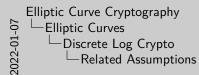
In practice, we make stronger assumptions, such as Computational Diffie Hellman and Decisional Diffie Hellman.

- 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 $e(g^x, g^y) = e(g, g^z)$

ckground

nclusion

Resources

0

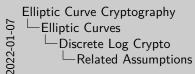
00000

0

» 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.
+ CHIO. From [2/P, [0] P Compute [xxi]P

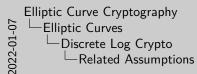
- 1. In fact in some groups CDH and DLP are equivalent
- 2. Check $e(g^x, g^y) = e(g, g^z)$

» 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 Hillman and Discissional Diffie Hellman. \vdash CHD: Γ From $[2|\Gamma_0[p]P]$ compute $[xy_0]P$ \vdash DDH: Distinguish $(P, [x]P, [y_0]P, [xy_0]P)$ from $(P, [x]P, [y_0]P, [x]P)$. Pairins was Max DDH asso on ellibric curved

- 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!

$$DDH \leq_R CDH \leq_R DLP$$

Elliptic Curve Cryptography
Co-10 — Elliptic Curves
— Discrete Log Crypto
— Related Assumptions

» Related Assumptions

In practice, we make stronger assumptions, such as Computational Driffs Hilmann and Decisional Driffs Hilmann.

CHD: From $[x]P_i[y]P$ compute [xy]PDRH: Distinguish $P_i[x]P_i[x]P_j[x]P_j$ from $([x], [x], [y]P_i]P_j]P_j$ Patrings make DDH says on elliptic curved DDH \leq CDH \leq DLP \leq DLP

- 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!

$$DDH <_R CDH <_R DLP$$

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.

Elliptic Curve Cryptography

Elliptic Curves

Elliptic Curves

Elliptic Curve Cryptography

Related Assumptions

» Related Assumptions

In practice, we make stronger assumptions, such as Computational DIffie Hellman and Decisional DIffie Hellman. \vdash CHD. From [x]P, [y]P compute [xy]P = DDH: Distinguish (P, [x]P, [y]P, [xy]P) from (P, [x]P, [y]P, [x]P)Pairings make DDH easy on elliptic curved

 $DDH \leq_R CDH \leq_R DLP$ 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.

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

History

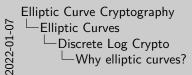
ackground

Elliptic Curves

Conclusion o

Resourc

Why elliptic curves?



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

» Why elliptic curves?

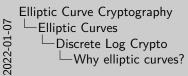
listory Backg

bund Elliptic Curves

onclusion

Resources

Why elliptic curves?



 $\label{eq:basic_problem} \begin{array}{lll} \text{Why elliptic curves?} \\ \\ \text{Assumption} & \text{Group} & \text{Best Algorithm} & \approx \text{Compteol} \\ \text{RSA} & Z_N & \text{Number Field Sieve} & \text{exp($c^{1}\sqrt{\log}$)} \\ \text{DLP} & E(\mathbb{F}_p) & \text{Number Field Sieve} & \text{exp($c^{1}\sqrt{\log}$)} \\ \text{DLP} & E(\mathbb{F}_p) & \text{Pollard Rhoo} \\ \end{array}$

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



Conclusion

Resources
0
00000



Best known attacks against ECC are generic attacks

Elliptic Curve Cryptography
Color Elliptic Curves
Discrete Log Crypto
Why elliptic curves?

» Why elliptic curves?
Assumption Group Bast Algorithm \approx Complete RSA $Z_{\mathcal{F}}$ Number Field Stove $\exp(\sqrt{\epsilon}/\sqrt{\log \epsilon})$ DLP $E(\mathcal{F}_{\mathcal{F}})$ Number Field Stove $\exp(\sqrt{\epsilon}/\sqrt{\log \epsilon})$ Best known attacks against ECC are generic attacks

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



Conclusion

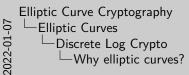
Resources
0
00000

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	$E(\hat{\mathbb{F}}_p)$	Pollard Rho	\sqrt{p}

Best known attacks against ECC are generic attacks

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



Assumption Group Best Algorithm \approx Complexity RSA \mathbb{Z}_N Number Field Sove $\exp(\sqrt{\log R})$ CUP $= \mathbb{F}_N^2$ Number Field Sove $\exp(\sqrt{\log R})$ General Sove $\exp(\sqrt{\log R})$ Pollared Not \sqrt{p} Best known attacks against ECC are generic attacks - Shorter loyisize ($\approx 250 \times 3072$ bits) - Faites comparation

» Why elliptic curves?

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

Resource

» 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		
$x \leftarrow \mathbb{Z}_q$	$y \leftarrow \mathbb{Z}_q$		
$Q_A = [x]P$	$Q_B = [y]P$		
Q.	\xrightarrow{A}		
$\stackrel{Q_B}{\longleftarrow}$			
$K = [x]Q_B$	$K = [y]Q_A$		

Elliptic Curve Cryptography

Elliptic Curves

Elliptic Curves

Elliptic Curves

Elliptic Curve Cryptography

Elliptic Curve Cryptography

Elliptic Curve Cryptography

Elliptic Curve Cryptography

» EC Diffie Hellman Key Exchange Let E be a suffect cove over T_e Let F be a large prime dividing $\#E(F)_e$ and F a control of other F.

Diffie Hellman

And

Diffie Hellman $A_{e,e} = \frac{B_{e,e}}{C_e}$ $C_{e,e} = \frac{B_{e,e}}{C_e}$

- 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.

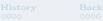
Diffie Hellman Alice $x \leftarrow \mathbb{Z}_q$ $y \leftarrow \mathbb{Z}_q$ $Q_A = [x]P$ $Q_B = [y]P$ $Q_A \rightarrow Q_B$ $X \leftarrow \mathbb{Z}_q$ $Q_B = [y]P$ $Q_A \rightarrow Q_B$ $Q_B \rightarrow Q_B$ $X \leftarrow \mathbb{Z}_q$ $Q_B \rightarrow \mathbb{Z}_q$ $Q_B \rightarrow \mathbb{Z}_q$ $Q_B \rightarrow \mathbb{Z}_q$

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



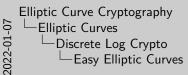
Conclusion
o

Resources
0
00000

» 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

Elliptic Curves

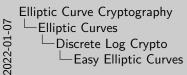
onclusion

Resources
0
00000
0

» 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



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

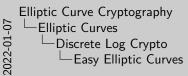
» Easy Elliptic Curves

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.



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 aromalous curves.

Curves that damin pairings to small finite fields.

» Easy Elliptic Curves

1. Embedding degree -¿ MOV algorithm

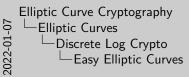
nclusion

Resources
0
00000

» 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.



DLP is not equally hard on every curve! • Singular curves over \overline{x}_p . Equivalent to DLP in \overline{x}_p^n or \overline{x}_p^n . • Curves and subgroups with small embedding degree. E.g. superingular and anomalous curves. • Curves that admit pairings to email finite fields. • Curves defined over \overline{x}_p for \overline{x}_p with small factors. GMS

» Easy Elliptic Curves

1. Embedding degree -; MOV algorithm

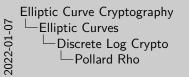
Elliptic Curves

nclusion

Resource0
00000
0

» Pollard Rho

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



In practice, to detect cycle step one iterator by one and one by two

» Pollard Rho

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

2. Not parallelizable, use vOW (more memory)

History

ockground

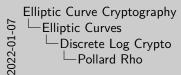
Elliptic Curves

nclusion

Resource0
00000
0

» 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)

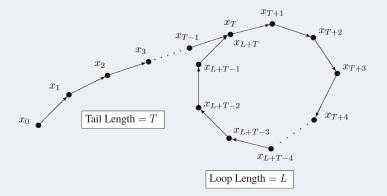
Elliptic Curves

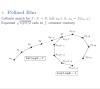
nclusion

Resources

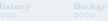
» Pollard Rho

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)

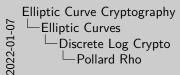


Conclusion
o

Resource

» Pollard Rho

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

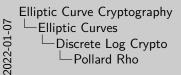


» ${f Pollard\ Rho}$ Let G be a group of order N. We want to find k s.t. [k]P=Q.

- 1. Nowadays functions with better mixing used
- $2. \ \, \mbox{The} \ {\rm gcd}$ 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 $\#A\approx \#B\approx \#C$.



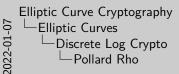
» Pollard Rho Let G be a group of order N. We want to find k s.t. [k]P=Q. Split $G=A\sqcup B\sqcup C$ with $\#A\approx \#B\approx \#C$.

- 1. Nowadays functions with better mixing used
- $2. \ \, \text{The} \, \gcd$ 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

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





- 1. Nowadays functions with better mixing used
- $2. \ \, \mbox{The} \ {\rm gcd}$ condition in pratice almost always true

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

clusion

Resource:
0 00000

» 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

Elliptic Curves

clusion

Resources

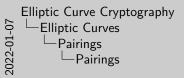
» Pairings

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

clusion

Resources

» 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:

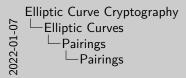
* Non degenerate:

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

* 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

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:

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

Elliptic Curve Cryptography
Co-To-Control
Control
Cont



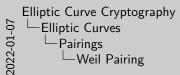
- 1. The alternating not strictly in definition
- 2. Generalised with three groups

» Weil Pairing

Every elliptic curve ${\cal E}$ over ${\cal K}$ 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 ${\cal E}$ over ${\cal K}$ 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

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 G, G_T be cyclic groups of prime order p. Let P be a generator of 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 $H: \{0,1\}^* \to \mathbb{G}$

$$\frac{\operatorname{Gen}(1^{\lambda})}{x \leftarrow \$ \mathbb{Z}_p}$$

$$pk \coloneqq [x]P$$

$$sk \coloneqq x$$

$$\mathbf{return} \ (pk, sk)$$

```
Elliptic Curve Cryptography
Color Elliptic Curves
Pairings
BLS Signatures
```

BLS Signatures

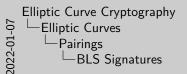
Let \mathbb{G} , \mathbb{G}_T be cyclic groups of prime order p. Let P be a generator of \mathbb{G} , and e a non degenerate pairing. Also, let $H: \{0,1\}^* \to \mathbb{G}$

$$\frac{\mathrm{Gen}(1^{\lambda})}{x \leftarrow \$ \mathbb{Z}_p} \frac{\mathrm{Sign}(sk, m)}{Q \leftarrow H(m)}$$

$$pk \coloneqq [x]P \qquad \sigma \leftarrow [x]Q$$

$$sk \coloneqq x \qquad \mathbf{return} \ \sigma$$

$$\mathbf{return} \ (pk, sk)$$



» BLS Signatures

Let G, G_T be cyclic groups of prime order p. Let P be a generator of G, and a non degenerate gaining. Also, let $H: \{0,1\}^n \to \mathbb{G}$ $G = \{0,1\}^n \}$ $G = \{0,1\}^$

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 $H: \{0,1\}^* \to \mathbb{G}$

$$\frac{\operatorname{Gen}(1^{\lambda})}{x \leftarrow \$ \mathbb{Z}_{p}} \frac{\operatorname{Sign}(sk, m)}{Q \leftarrow H(m)}$$

$$pk \coloneqq [x]P \qquad \sigma \leftarrow [x]Q$$

$$sk \coloneqq x \qquad \mathbf{return} \ \sigma$$

$$\mathbf{return} \ (pk, sk)$$

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

Elliptic Curve Cryptography
Co-10 — 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 $H:\{0,1\}^*\to\mathbb{G}$

$$\frac{\operatorname{Gen}(1^{\lambda})}{x \leftarrow \$ \mathbb{Z}_{p}} \frac{\operatorname{Sign}(sk, m)}{Q \leftarrow H(m)}$$

$$pk \coloneqq [x]P \qquad \sigma \leftarrow [x]Q$$

$$sk \coloneqq x \qquad \mathbf{return} \ \sigma$$

$$\mathbf{return} \ (pk, sk)$$

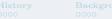
$$\frac{\operatorname{Verify}(pk, m, \sigma)}{\operatorname{return} \ e(\sigma, P) =_{?} e(H(m), [x]P)}$$

Correctness by:

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

Elliptic Curve Cryptography 2022-01-07 Elliptic Curves -Pairings ☐BLS Signatures

» BLS Signatures Let G, G_T be cyclic groups of prime order p. Let P be a generator return $e(\sigma, P) \Longrightarrow e(H(m), [x|P)$ Correctness by:



ground Elliptic Curves

onclusion

Resource0 00000

Post Quantum

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

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



nclusion

Resources
0
00000
0

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 war recover?

Elliptic Curves

•000000000000000000

nclusion

Resources
0
00000
0

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?
 Yss. lattices, codes, multinear maps...

Elliptic Curves

•000000000000000000

onclusion

Resources
0
00000
0

Post Quantum

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

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

Vol. battless enable multipless make

» Post Quantum

History

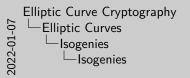
ackground

Conclusion o

Resource
0
000000
0



"Nice maps" between elliptic curves.



» Isogenies
"Nice maps" between elliptic curves.

└─ Isogenies

Isogenies

"Nice maps" between elliptic curves.

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

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

Elliptic Curve Cryptography

Elliptic Curves

Isogenies

Isogenies

Isogenies

Isogenies

Elliptic Curves

Conclusion
o

Resourc

0

» Properties of isogenies

* Each isogeny is also a group homomorphism

Elliptic Curve Cryptography
Color Elliptic Curves
Isogenies
Properties of isogenies

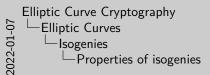
Properties of isogenies
 Each isogeny is also a group homomorphism

Conclusion

Resource

> Properties of isogenies

- * Each isogeny is also a group homomorphism
- \ast 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

Elliptic Curves 000000000000000000

» Properties of isogenies

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

Elliptic Curve Cryptography 2022-01-07 Elliptic Curves -Isogenies Properties of isogenies

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

nclusion

Resource 0 000000 0

» 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 $\deg(\phi \circ \psi) = \deg(\phi) \deg(\psi)$

Elliptic Curve Cryptography

Elliptic Curves

Isogenies

Properties of isogenies

» Properties of isogenies
Each isogeny is also a group homomorphism
The map [m] : E → E is an isogeny
You can compose isogenies
Each isogeny has a degree, and it is multiplicative deg(φ o y) → deg(φ) (deg(φ)

» 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 $\begin{array}{ll} \hbox{$+$ $Each isogeny is also a group homomorphism} \\ \hbox{$-$ $The map}[m]: E--E is a isogeny \\ \hbox{$+$ $Voc cas composite isogenies} \\ \hbox{$-$ $Each isogeny has a degree, and it is multiplicative} \\ \hbox{$-$ $deg}(\phi\circ v) - dog(\phi) dog(\psi) \\ \hbox{$-$ $Each isogeny $\rho\circ E]} - \delta E_0 has a unique doul <math>\hat{\phi}\colon E_2 \to E_1 \end{array}$

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

» 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

$$(x,y) \mapsto \left(\frac{f}{h^2}(x), y \cdot \frac{g}{h^3}(x)\right)$$

Elliptic Curve Cryptography

-Elliptic Curves

-Isogenies

-Properties of isogenies

» Properties of isogenies

• Each inegery is also a group homomorphism

• The map $[0] \in T - E$ is an inegery

• You can compose inegenies

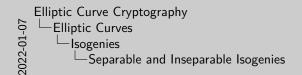
• Each inegery has a deper, and it is multiplicative diegle $0 < 0 - \deg(c) \deg(c)$ • Each ineger 0 < E - d is at a surjent dead d < E - d. In this dieger 0 < E - d is the surjent dead d < E - d. In this dieger 0 < E - d is 0 < d in the d in th

 $(x, y) \mapsto \left(\frac{f}{i^{2}}(x), y \cdot \frac{g}{i^{2}}(x)\right)$

Let $E/k: y^2 = x^3 + ax + b$, with 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.





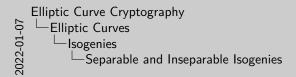
- Frobenius are very important
- In our case they are a bit of a nuisance for a theorem later on

Separable and Inseparable Isogenies

Let $E/k: y^2 = x^3 + ax + b$, with 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 $E^{(p^r)} = E$





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

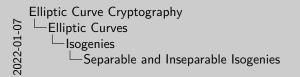
Definition

Let $E/k: y^2=x^3+ax+b$, with ${\rm char}(k)=p$. 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 $(p^r)\text{-}\mathbf{Frobenius}$ 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.





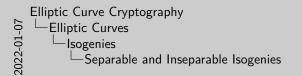
- 1. Frobenius are very important
- 2. In our case they are a bit of a nuisance for a theorem later on

Let $E/k: y^2 = x^3 + ax + b$, with 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.



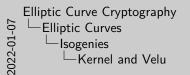


- Frobenius are very important
- In our case they are a bit of a nuisance for a theorem later on

Elliptic Curves 0000 00000000000000000

» Kernel and Velu

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 There is a one to one correspondence between finite subgroups of elliptic curves and separable isogenies from

ackground

Elliptic Curves

nclusion

Resources 0 00000 0

» 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

Elliptic Curve Cryptography

Elliptic Curves

Isogenies

Kernel and Velu

» Kernel and Velu

There is a one to one correspondence between finite
subgroups of elliptic curves and superable inagenies from
that curve, up to poic-composition with inomorphisms
karnels → inogenies

onclusion

Resources

» 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

Elliptic Curve Cryptography
Co-10-255

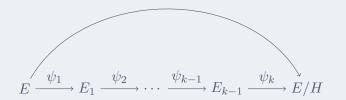
Kernel and Velu

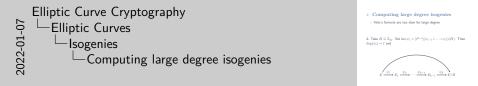
» Kernel and Velu

There is a one to one correspondence between finite sudgroups of eligible covers and signable suggested from that every get to price country. It is a support to the same place of the same

* Velu's formula are too slow for large degree

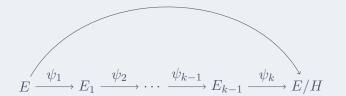
4- Take $H \cong \mathbb{Z}_{\ell^k}$. Set $\ker \psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then $\deg(\psi_i) = \ell$ and



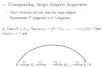


- * Velu's formula are too slow for large degree
- * Decompose ℓ^k isogenies in k ℓ -isogenies

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



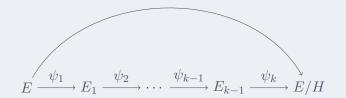
Elliptic Curve Cryptography 2022-01-07 Elliptic Curves -Isogenies -Computing large degree isogenies



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



Elliptic Curve Cryptography 2022-01-07 Elliptic Curves -Isogenies -Computing large degree isogenies

» Computing large degree isogenies Speedup from Θ(ℓ^k) to Θ(k²ℓ) 4- Take $H \cong \mathbb{Z}_m$. Set $\ker \psi_i = [\ell^{k-i}](\psi_{i-1} \circ \cdots \circ \psi_1)(H)$. Then Elliptic Curves

nclusion

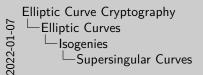
Resources

» 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

000000 0000000000000



» Supersingular Curves $\begin{array}{ll} \text{(Definition)} \\ \text{A curve } \text{Eddind over } K \text{ with } \text{char}(K) = p \text{ is} \\ \text{supersingular } f[g] \text{ is purely inseparable and} \\ g(E) \in \mathbb{F}_p. \text{ A curve that is not supersingular is ordinary} \end{array}$

Elliptic Curves

nclusion

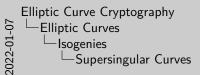
Resources
0
00000
0

» 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?



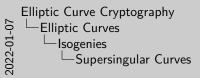
 $\label{eq:supersingular Curves} Supersingular Curves $$ \frac{|K_{max}|_{K}}{K} = p \text{ is a supersingular } T_j \text{ is a purely imparable and } T_j \text{ if a purely imparable purely } Something something order in a quaternion algebra <math>T$

» 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} .



nclusion

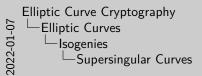
Resource

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 $\approx \left| \frac{p}{12} \right|$ supersingular curves over \mathbb{F}_{p^n} .
- * A supersingular curve has p+1 points.



* Supersingular Curves $\sum_{i=1}^{n} a_i a_i = 0 , \quad a_i = 0 , \quad$

nclusion

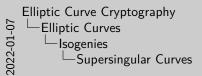
Resources

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 $\approx \left| \frac{p}{12} \right|$ supersingular curves over \mathbb{F}_{p^n} .
- * A supersingular curve has p+1 points.
- * Insecure for DLP



Definition

A curve E defined over K with char(K) = p is supersingular d [p is purely interparable and $p(E) \in \mathbb{F}_p^{n-1}$. A curve that is not supersingular is ordinary.

Something something order in a quaternion algebra?

There are s [$\frac{1}{2}$] is supersingular curves over $\mathbb{F}_{p^{n-1}}$. A supersingular curve has p + p interparable p and p is a supersingular curve bay p + p interparable p in p

» Supersingular Curves

» 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 $\approx \left| \frac{p}{12} \right|$ supersingular curves over \mathbb{F}_{p^n} .
- * A supersingular curve has p+1 points.
- * Insecure for DLP
- * Secure for CSSI (later)!

```
Elliptic Curve Cryptography

Elliptic Curves

Isogenies

Supersingular Curves
```

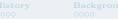
Definition

A curve E defined over K with char(K) = p is supersingular ℓ [p] is purely inseparable and $j(E) \in \mathbb{F}_p^{r_s}$. A curve that is not supersingular is ordinary + Something sortenting order in a quaternin algebra?

Then $g = \infty$ [E] supersimplified curves over E g.

A supersingular curve has p + 1 points. Insecure for DLP Secure for CSSI (later)!

» Supersingular Curves



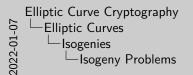
Elliptic Curves

onclusion

Resource

» 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

nclusion

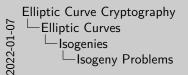
Resources

» 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 $\#E_1(k) = \#E_2(k)$.





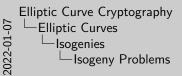
» Isogeny Problems

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:



```
s Isogeny Problems
It is easy to find out if two curves are isogenous
Tho curves E<sub>1</sub>, E<sub>2</sub> over a finite field k, are isogenous
over k if and only if # E<sub>1</sub>(k) = # E<sub>2</sub>(k).
Finding the isogeny is domatically harder.
```

nclusion

Resources

» 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^\prime , find an isogeny between them.

Elliptic Curve Cryptography
Co-10-27
Co-27

» Isogeny Problems
It is easy to find out if two curves are longenous

**Isomerous E., E.; over a finite field h an longenous
own it find only if it field in it field has longenous
own it find only if it field in it field.

**Finding the longeny is demarkately harder

**Isomerous intermediated importaging longeny problem is
**Finding Content to superingingle linguity corned E. E.*

**Finding Content to superingingle linguity or problem is
**Finding Content to superingingle linguity or problem is
**Finding Content to superingingle linguity.
**Indiana Content to superinging linguity.
**Indiana Content to superinging linguity.
**Indiana Conte

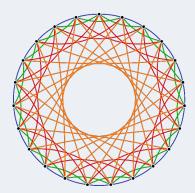


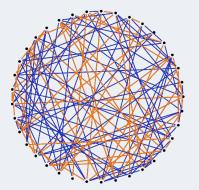
Conclusion

Resources

» Isogeny Graphs

Look something like this! We focus on the second





Elliptic Curve Cryptography

Elliptic Curves

Isogenies

Isogeny Graphs



1. CSIDH is pronounced Seaside

istory Back

onclusion

Resource
0
00000

» Isogeny Graphs

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

» Isogeny Graphs $\mbox{Let } p,\ell \mbox{ be a primes, } K \mbox{ a field of characteristic } p.$

ckground

nclusion

Resource

» 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 bu a primes, K a field of characteristic p.

1300 in the charac

ackground

nclusion

Resources
0
00000
0

» 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.

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

ackground

nclusion

Resources
0
00000
0

» 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.

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

clusion

Resources

» 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}_{n^2}

» Isogeny Graphs

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

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

We can represent vertices as elements of F_c:

nclusion

Resource

» 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

Elliptic Curve Cryptography

Elliptic Curves

Isogenies

Isogeny Graphs

» 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 ℓ • Edges: Separable isogenies from $E \to E'$ 4- Both up to isomorphisms (i.e. vertices are

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

nclusion

Resor

» 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}_{n^2}
 - * Graph is directed
 - * Graph has good mixing properties

Elliptic Curve Cryptography

Elliptic Curves

Isogenies

Isogeny Graphs

» Isogeny Graphs

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

The ℓ-supersingular isogeny graph has as:

• Vertices: Supersingular Elliptic curves over F

• Edges: Separable isogenies from E → E'

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

We can represent vertices as elements of \mathbb{F}_p : Graph is directed Graph has good mixing properties

clusion

Resource

» 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}_{n^2}
 - * Graph is directed
 - * Graph has good mixing properties
 - * Can walk in the graph with Velu's method

Elliptic Curve Cryptography
Co-10-2000

Elliptic Curves

Isogenies

Isogeny Graphs

» 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 ℓ • Edges: Separable isogenies from $E \to E'$ 4- Both up to isomorphisms (i.e. vertices are

We can represent vertices as elements of F_p
 Graph is directed.

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.

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}_{n^2}
 - * Graph is directed
 - * Graph has good mixing properties
 - * Can walk in the graph with Velu's method
 - * Most vertices have degree $\ell+1$

Elliptic Curve Cryptography 2022-01-07 Elliptic Curves Isogenies -Isogeny Graphs

» Isogeny Graphs

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

The /-supersingular isogeny graph has as: Vertices: Supersingular Elliptic curves over J Edges: Separable isogenies from $E \rightarrow E'$ 4- Both up to isomorphisms (i.e. vertices are

We can represent vertices as elements of F.,

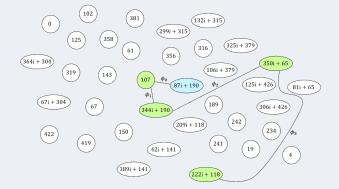
Can walk in the graph with Velu's method Most vertices have degree $\ell+1$

Resour

0000000000 0000000 000000000

SIDH $(p = 2^4 3^3 - 1)$

Alice's pk



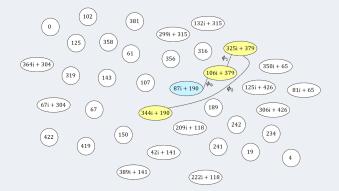
```
Elliptic Curve Cryptography \begin{tabular}{ll} \begin{tabular}{ll} Elliptic Curves \\ \hline \begin{tabular}{ll} -Elliptic Curves \\ \hline \begin{tabular}{ll} -Isogenies \\ \hline \begin{tabular}{ll} -SIDH \end{tabular} (p=2^43^3-1) \\ \end{tabular}
```



Resource

SIDH $(p = 2^4 3^3 - 1)$

Bob's pk



Elliptic Curve Cryptography $\begin{tabular}{l} \begin{tabular}{l} \b$



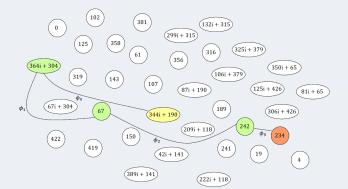
Elliptic Curves

onclusion

Resource

SIDH $(p = 2^4 3^3 - 1)$

Alice's pk



Elliptic Curve Cryptography $\begin{tabular}{l} \begin{tabular}{l} \b$



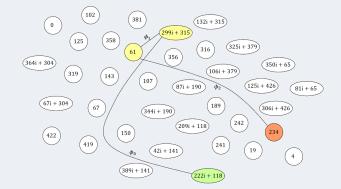
Conclusion

Resourc

000

SIDH $(p = 2^4 3^3 - 1)$

Alice's pk

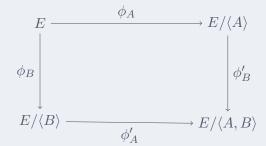


```
Elliptic Curve Cryptography \begin{tabular}{ll} \begin{tabular}{ll} Elliptic Curves \\ \hline \begin{tabular}{ll} -Elliptic Curves \\ \hline \begin{tabular}{ll} -Isogenies \\ \hline \begin{tabular}{ll} -SIDH \end{tabular} (p=2^43^3-1) \\ \end{tabular}
```

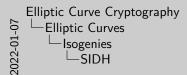




Picture to keep in mind:



Details will follow





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

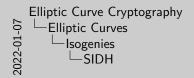
History Ba

Conclusion
o

Resource0 00000

» SIDH

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



» $\ \, {\bf SIDH}$ Parties select $p=2^{t_A}3^{t_B}-1$ prime,

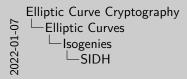


onclusion

Resource

» SIDH

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



» SIDH Parties select $p=2^{c.3}3^{ca}-1$ prime, a supersingular starting curve E/\mathbb{F}_p ,

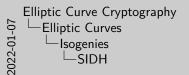
onclusion

Resources

» 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 $p = \mathcal{L}^{A_3 Y_0} = 1$ prime, a supersingular starting curve $E/\mathbb{F}_{\mathcal{F}^s}$, four points P_A , P_B , Q_A , Q_B s.t. $(P_A, Q_A) = E/\mathbb{F}^{a_1} [N_B, Q_B) = E/\mathbb{F}^{a_1} [N_B, Q_B) = E/\mathbb{F}^{a_1} [N_B, Q_B) = E/\mathbb{F}^{a_1} [N_B + \mathbb{F}^{a_2} [N_B + \mathbb{F}^{a_3} [N_B + \mathbb{F}^{a_4} [N_B + \mathbb{F}^{a_4}$

Elliptic Curves

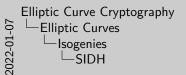
nclusion

Resource: 0 000000

» 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 $p = 2^{-\alpha}3^{\alpha}n - 1$ prime, a supersingular starting curve $E/F_{\mathcal{F}_{\beta}}$, for points P_{δ} , P_{δ} , Q_{δ} , Q_{δ

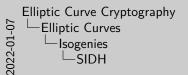
onclusion

Resource:
0 00000

» 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 $p = 2^n 3^n - 1$ prime, a supersingular starting curve E/\mathbb{F}_{p^n} , four points P_A , P_B , Q_B , Q_B a.t. $(P_A, Q_A) = E2^n 3$, $(P_B, Q_B) = E[3^n]$.

Alice, Bob sample $n_A \leftarrow 4\mathbb{Z}_{2^n A}$, $n_B \leftarrow 4\mathbb{Z}_{2^n B}$, and compute $S_Y = P_Y + |n_1/2| + 2$.

Alice computes the 2^{c_A} isogeny $\phi_A : E \rightarrow E/\langle S_A \rangle = E_A$ Bob computes the 3^{c_B} isogeny $\phi_B : E \rightarrow E/\langle S_B \rangle = E_B$

» 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 $\operatorname{pk}_X = (E_X, P_X' = \phi_X(P_X), Q_X' = \phi_X(Q_X))$

» SIDH

The public keys are

Parties select $p = 2^n 3^m - 1$ prime, a supersingular starting curve $E[\mathbb{F}_p]$, four points P_h, P_h, Q_h, Q_h at $\{P_h, Q_h\} = E[\mathbb{F}^n]$. $\{P_h, Q_h\} = E[\mathbb{F}^n]$. $\{P_h, Q_h\} = E[\mathbb{F}^n]$. Alloes, Bob sample $h_h + 4 \mathbb{E}_{Z^h} h_h = 0$. $\mathbb{E}[\mathbb{F}^n]$. All compute $S_X = P_X + [\mathbb{F}_X]Q_X$. Alloe computes the 2^n 4 isogeney $\phi_A : E = E/(S_h) = E_A$.

Bob computes the 3^{e_R} isogeny $\phi_R: E \to E/(S_R) = E_R$

 $pk_X = (E_X, P_X' = \phi_X(P_X), Q_X' = \phi_X(Q_X))$

» 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 $\operatorname{pk}_X = (E_X, P_X' = \phi_X(P_X), Q_X' = \phi_X(Q_X))$
- * Alice computes $S_A' = P_B' + [n_A]Q_B'$, and an isogeny $\phi_A' : E_B \to E/\langle S_A' \rangle = E_{AB}$

Elliptic Curve Cryptography
Co-10Co-2000

Elliptic Curves

Isogenies

SIDH

» SIDH

Parties select $p = 2^n 2^n 2^n - 1$ prime, a supersingular starting caree $E(\mathbb{F}_g)$, for some $S_1, P_{22}, Q_1, Q_2 = \mathbb{E}[\mathbb{F}^n]$, $(P_2, Q_1) = \mathbb{E}[\mathbb{F}^n]$, $(P_3, Q_2) = \mathbb{E}[\mathbb{F}^n]$, $(P_3, Q_2) = \mathbb{E}[\mathbb{F}^n]$. Alone, Book suppose $A_1 = \mathbb{E}[\mathbb{F}^n]$, $(P_3, P_3) = \mathbb{E}[\mathbb{F}^n]$, A local companion the 2^n - A local companion A is A. The partie laws p is A local A is A local A in A

Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogen-

SIDH

Parties select $p = 2^{e_A}3^{e_B} - 1$ prime, a supersingular starting curve E/\mathbb{F}_{n^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 $pk_X = (E_X, P'_Y = \phi_X(P_X), Q'_Y = \phi_X(Q_X))$
- * Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogeny $\phi'_{\Delta}: E_B \to E/\langle S'_{\Delta} \rangle = E_{AB}$
- * Bob computes $S'_{B} = P'_{A} + [n_{B}]Q'_{A}$, and an isogeny $\phi_B': E_A \to E/\langle S_B' \rangle = E_{BA}$

Elliptic Curve Cryptography 2022-01-07 Elliptic Curves Isogenies -SIDH

» SIDH

Parties select $p = 2^{c_A}3^{c_B} - 1$ prime, a supersingular starting curve E/F.s. four points Ps. Pn. Os. On s.t.

Alice. Bob sample n , ←s Z_{m +} , n_m ←s Z_{m m}, and compute $S_Y = P_Y + [n_Y]Q_Y$ Alice computes the 2^{ϵ_A} isogeny $\phi_A: E \to E/\langle S_A \rangle = E_A$ Bob computes the 3^{c_B} isogeny $\phi_B: E \to E/\langle S_B \rangle = E_B$

The public keys are $pk_X = (E_X, P_X' = \phi_X(P_X), Q_X' = \phi_X(Q_X))$ Alice computes $S'_A = P'_B + [n_A]Q'_B$, and an isogen-

Bob computes $S'_B = P'_A + |n_B|Q'_A$, and an isogeny

» 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 $\operatorname{pk}_X = (E_X, P_Y' = \phi_X(P_X), Q_Y' = \phi_X(Q_X))$
- * 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 $j(E_{AB}) = j(E_{BA})$

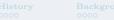
» SIDH

Parties select $p = 2^{c_A}3^{c_B} - 1$ prime, a supersingular starting curve $E[F_{p_F}, \text{four points } F_A, P_B, Q_A, Q_B \text{ s.t. } (P_A, Q_A) = E[Z^a], (P_B, Q_B) = E[S^a].$ Alica, Bob sample $n_A \leftarrow 3 Z_{p_A}, n_B \leftarrow 3 Z_{p_B}$, and compute

Alice, Bob sample $n_A \leftarrow 4\mathbb{Z}_{Z'A}$, $n_B \leftarrow 4\mathbb{Z}_{Z'B}$, and compute $S_X = P_X + [n_X]Q_X$ Alice computes the Z'^A isogeny $\phi_A : E \rightarrow E/(S_A) = E_A$ Bob computes the Z'^A isogeny $\phi_B : E \rightarrow E/(S_B) = E_B$ The public lays are

pkx = $(E_X, P_X' = \phi_X(P_X), Q_X' = \phi_X(Q_X))$ Alice computes $S_A' = P_B' + [n_A]Q_B'$, and an isogen

Alice computes $S_A' = P_B' + [n_A]Q_B'$, and an isogeny $\phi_A' : E_B \rightarrow E/\langle S_A' \rangle = E_{AB}$ Bob computes $S_B' = P_A' + [n_B]Q_A'$, and an isogeny



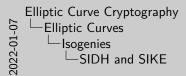
kground Elliptic Curves

Conclusion 0

Resources

» SIDH and SIKE

* SIDH is vulnerable to active attacks





Conclusion

Resources 0 00000 0

» 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

onclusion

Resources
0
00000

» 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

Elliptic Curve Cryptography

Elliptic Curves

Isogenies

SIDH and SIKE

» SIDH and SIKE

Very short keys

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

Currently a bit on the slow side

onclusion

Resources
0
00000

» 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

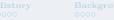
Elliptic Curve Cryptography
Co-10-2000
Elliptic Curves
Isogenies
SIDH and SIKE

» 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

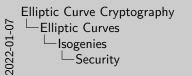


Conclusion
o

Resource

» Security

Best attack is on CSSI problem.



» Security
Best attack is on CSSI problem.

kground Elliptic Curves

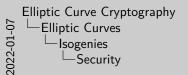
onclusion

Resources

» 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} .

0000000000000000000



» Security

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

tic Curves

0000000000000000000

nclusion

Resources
0
000000

» 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

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

But attack is on CSSI problem. Suppose we want to find an ℓ^* -inggrey between $E_0 \rightarrow E_1$, both supersingular and over $F_{\ell'}$ test s = a/2 and $E_1 = E_1 = \frac{1}{2} \left[H + E_2 \left(E_1^{(k)} \mid H \text{ cyclic.}|H| - \ell^k\right)\right]$ $S = -((0) \times S_0 \downarrow \cup \cup \{(1) \times S_0 \downarrow)$ $g : S \rightarrow F_0 = (0, H) \rightarrow f(E_1)$

0000000000000000000

» 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

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

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

» Security

Best attack is on CSI problem. Suppose we want to find an ℓ -longing between $E_{\ell} - E_{\ell}$, both supersingular and over $F_{\ell'}$ Let $k \approx n/2$ and $S_{i,k} = \left\{ H \leq E_{i,k}[e^k] \mid H \text{ cyclic.}[H] - \ell^k \right\}$ $S = \{(0) \times S_{i,k}\} \sqcup \{(1) \times S_{i,k}\}$

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

Elliptic Curves

0000000000000000000

nclusion

Resources

» 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

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

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:

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

Elliptic Curve Cryptography
Color Elliptic Curves
Isogenies
Security

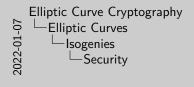
9 Security
But attack is on CSSI problem. Suppose we want to find an C-singuply belowes $E_0 - E_1$, both supersingular and over \mathbb{F}_p .

Let $\mathbb{R} = \mathbb{F}_p$ and $S_0 = \{H \in E(\mathbb{R}^d) \mid H \text{ eyele}, [H] = t^k\}$ $S = -\{(0) \times S_0 \rfloor \sqcup \mathsf{L}(\{1\} \times S_0 \})$ $g : S = S_p \cdot (0, H) - \mathsf{L}(H)^*$ A collision $g(H) = -(d, H)^*$ subset of SST. To enable

Pollard-Rho style methods, let $h : \mathbb{F}_{\omega} \to S$ be a hash function

» Security

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

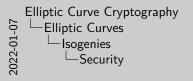


» Security $h \ \text{maps a set} \approx p/12 \ \text{to} \ S \ \text{which has size} \approx p^{1/4} \ \text{so introduces a}$ lot of collisions.

000000000000000000

» 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.

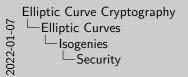


» Security $h \ \text{maps a set} \approx p/12 \ \text{to} \ S \ \text{which has size} \approx p^{1/4} \ \text{so introduces a}$ lot of collisions. To find a 'golden' one we use the van Oorschot



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 Wisner (x0W) algorithm. When using m processors and w memory cells, time complexity is

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



otic Curves

Conclusion

Resource 0 00000 0

0000

Conclusion

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

Elliptic Curve Cryptography
Conclusion
Conclusion
Conclusion

» Conclusion

Elliptic curves are pretty damn cool
 We only scratched the surfacel



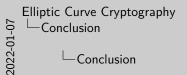
otic Curves

Conclusion

Resources

» 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 surfacel
 ECDH base of most of the web's key exchanges



c Curves

onclusion

Resources

» 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

Elliptic Curve Cryptography
Conclusion
Conclusion

» Conclusion

Elliptic curves are pretty damn cool
 We only scratched the surfacel

ECDH base of most of the web's key exchanges
 BLS Pairing based signatures both efficient and secure

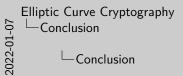


onclusion

Resource 0 00000 0

» 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 surfacel

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

ic Curves 000000 00 nclusion

Resources

» Resources

- 0 J.H. Silverman, J.T. Tate, Rational Points on Elliptic Curves
- 1 .H. Silverman, The Arithmetic of Elliptic Curves¹
- 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

Elliptic Curve Cryptography
Co-10-27
Resources
Resources

» Resources

0 J.H. Silverman, J.T. Tate, Rational Points on Elliptic Curves

J.H. Silverman, J.T. Tate, Rational Points on El
 H. Silverman, The Arithmetic of Elliptic Curves
 D.A. Cox. Primes of the form x² + nx²

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

bible

¹The bible

kground Ellipt

 $egin{array}{c} \mathbf{Conclusio} \\ \circ \end{array}$

ısion

» 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]

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]

Fields discussed in [7, III.1.14, VII]

*Weierstrass form in [1, III.2]

*Definition of elliptic curve [1, III.2, III.3] or [0, 2.2]

*Elliptic curves diagram from [lacr] and curves from [1, Fig 3.1, 3.2]

**Descriptions - Immediate formula from [1, III.3]

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]

Elliptic Curve Cryptography 2022-01-07 Resources -Detailed References -Detailed References & Credits

» Detailed References & Credits

Group Law diagram [0, Fig 1.16] Formulae [1, III.2.3] Scalar multiplication notation [1, III.2]

Multiplication isoseny [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] ground Elliptic Curves 00000000000 0000000 000

onclusion

Resource

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]

Elliptic Curve Cryptography
Resources
Detailed References
Detailed References & Credits

Detailed References & Credits

- Representation example opposed in [6, 3.1]

- Representation example opposed in [6, 3.1]

- Representation for the property of the property o

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]

tic Curves

onclusion

Resoure

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]

Elliptic Curve Cryptography
Resources
Detailed References
Detailed References & Credits

» 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 Horn. [1, III.4.8]
 Isogeny composition, degree and multiplicativity [1, III.4]
 Dual lisogeny [1, III.6]
 Frobinius isogeny and separability [3, 2.1.2]

Dual Isogeny [1, III.6]
Frobinius isogeny and separability [3, 2.1.2]
Kernels and Vela [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]

- * 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]

Elliptic Curve Cryptography 2022-01-07 Resources -Detailed References -Detailed References & Credits

» Detailed References & Credits

Isogenous with same number of points [1, Ex. 5.4] Graphs from L. Panny's [lekenpraatje] Vertices as elements of Fig 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]

c Curves

Conclusion

 $\begin{matrix} \text{Resources} \\ \circ \\ \circ \circ \circ \circ \circ \circ \\ \bullet \end{matrix}$

» 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]

Elliptic Curve Cryptography
Resources
Further Reading
Further Reading

» Further Reading

Attacks on SIDH [tonsion] [GPST]
 Mathematics of Isogony Based Crystography [deFeo17]
 VOW attack actimation [VOW98] [ACV-18] [CLN+19]
[IWS20]
 Verifiable Dalay Functions from Isogonies and Pairings
[dFMPS10]
 Delfs-Cafearith attack [Do16] [SCS21]