RANDOM SAMPLING OF SUPERSINGULAR ELLIPTIC CURVES

(based on a joint work with N. Murru and F. Pintore)

Marzio Mula

University of Trento, Department of Mathematics

April 6, 2022

OVERVIEW

The goals of this talk:

- Defining supersingular elliptic curves.

OVERVIEW

The goals of this talk:

- Defining supersingular elliptic curves.
- Reviewing the classic method to sample supersingular elliptic curves over finite fields of cryptographic size.

OVERVIEW

The goals of this talk:

- Defining supersingular elliptic curves.
- Reviewing the classic method to sample supersingular elliptic curves over finite fields of cryptographic size.
- Explain why the classic method is not suitable for cryptographic applications.

OVERVIEW

The goals of this talk:

- Defining supersingular elliptic curves.
- Reviewing the classic method to sample supersingular elliptic curves over finite fields of cryptographic size.
- Explain why the classic method is not suitable for cryptographic applications.
- Illustrate some alternative methods.

TABLE OF CONTENTS

PRELIMINARIES

ELLIPTIC CURVES

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

ELLIPTIC CURVES

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

$\mathbb{C}$, number fields and finite fields are examples of perfect fields.

ELLIPTIC CURVES

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

$\mathbb{C}$, number fields and finite fields are examples of perfect fields.

An *elliptic curve* over K is a projective curve that can be written, up to birational equivalence, as a cubic in $\mathbb{A}^2(K)$ in *Weierstrass form*

$$Y^2 = X^3 + AX + B \qquad \text{with } A, B \in K$$

having a *base point* at infinity $O = [0 : 1 : 0]$ and such that the *discriminant*

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

is not zero.

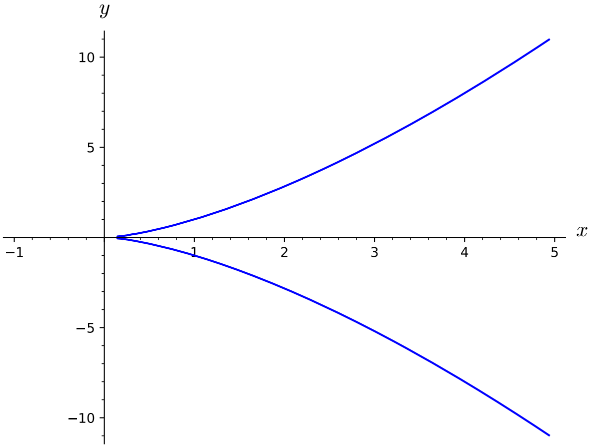
SOME EXAMPLES

$E\colon y^2 = x^3$ over $\mathbb{R}$

$$\Delta(E) = 0$$

$$\Downarrow$$

E is *not* an elliptic curve



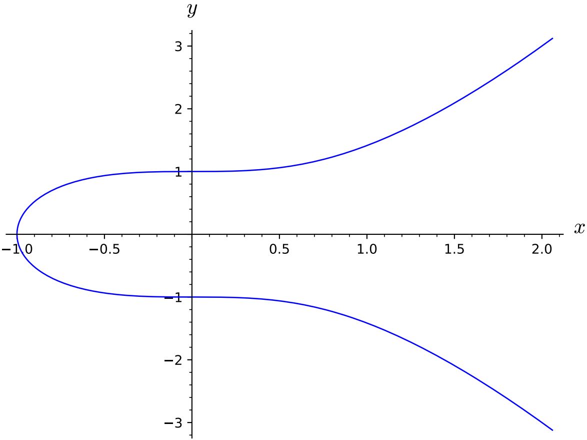
SOME EXAMPLES

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

$\Delta(E) = -432 \neq 0$

$\Downarrow$

E is an elliptic curve



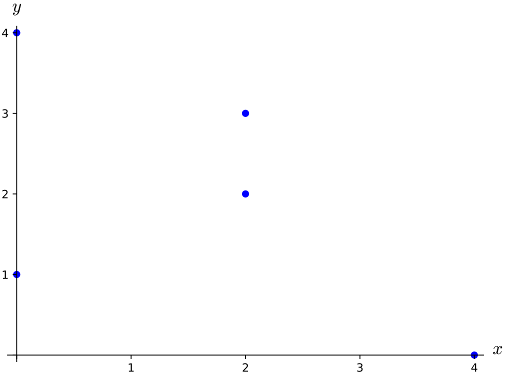
SOME EXAMPLES

$E\colon y^2 = x^3 + 1$ over $\mathbb{F}_5$

$$\Delta(E) = 3 \neq 0$$

$$\Downarrow$$

E is an elliptic curve



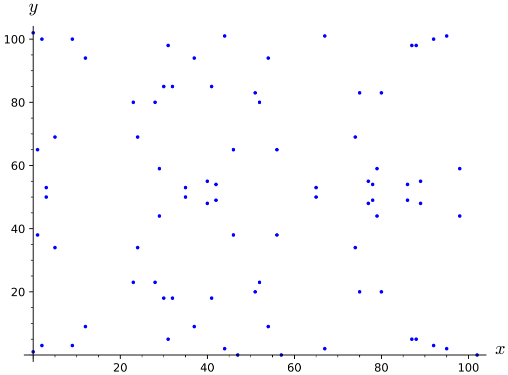
SOME EXAMPLES

$E\colon y^2 = x^3 + 1$ over $\mathbb{F}_{103}$

$\Delta(E) = 83 \neq 0$

$\Downarrow$

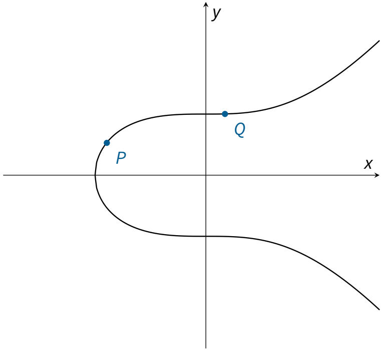
E is an elliptic curve



GROUP LAW

Any two points P, Q (not necessarily distinct) of an elliptic curve E can be added:

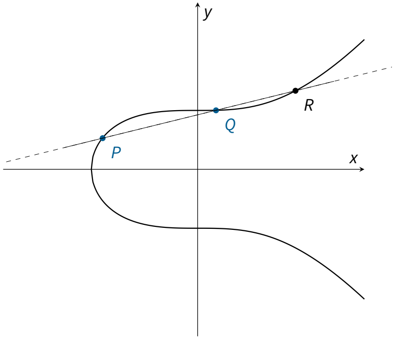
- Let P, Q be two points of E.



GROUP LAW

Any two points P, Q (not necessarily distinct) of an elliptic curve E can be added:

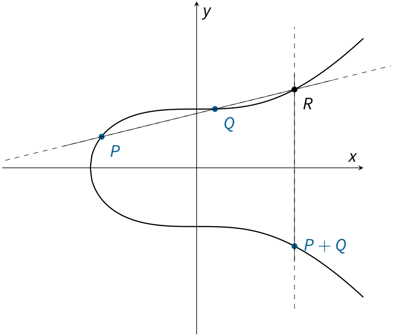
- Let P, Q be two points of E.
- Let R be the third intersection with E of the line through P and Q.



GROUP LAW

Any two points P, Q (not necessarily distinct) of an elliptic curve E can be added:

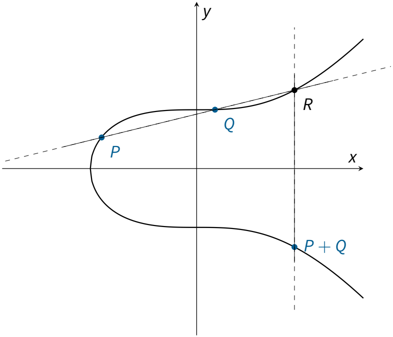
- Let P, Q be two points of E.
- Let R be the third intersection with E of the line through P and Q.
- Define $P + Q$ as the third intersection with E of the line through O and R.



GROUP LAW

Any two points P, Q (not necessarily distinct) of an elliptic curve E can be added:

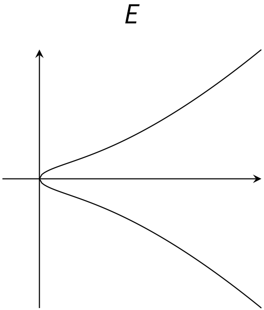
- Let P, Q be two points of E.
- Let R be the third intersection with E of the line through P and Q.
- Define $P + Q$ as the third intersection with E of the line through O and R.

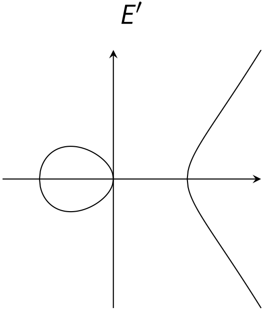


THEOREM

The points of E, together with the sum described above, form an abelian group.

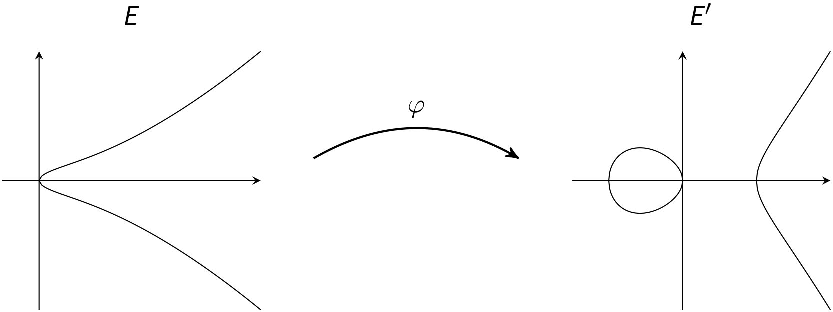
ISOGENIES





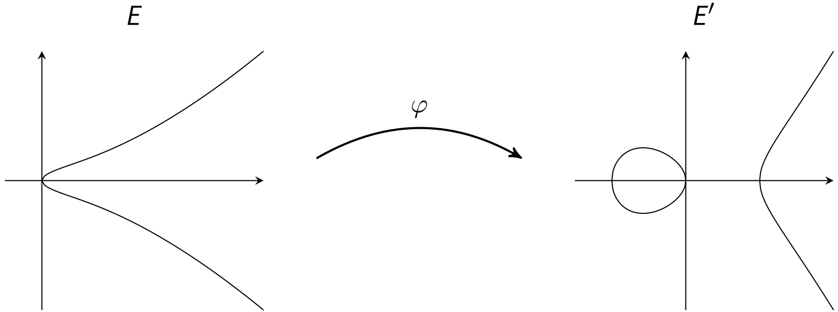
Let E and E' be two elliptic curves over K.

ISOGENIES



Let E and E' be two elliptic curves over K.
An *isogeny* $\varphi\colon E \to E'$ is a rational map sending the base point of E into the base point of E'.

ISOGENIES



Let E and E' be two elliptic curves over K.
An *isogeny* $\varphi\colon E \to E'$ is a rational map sending the base point of E into the base point of E'.

THEOREM

Isogenies are group homomorphisms.

EXAMPLES

- For any positive integer m, define

  $$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}}$$
  $$[-m]P = -[m]P,$$

  and let $[0]P$ be the zero isogeny. Then, the map

  $$\begin{aligned} [m]\colon E &\to E \\ P &\mapsto [m]P \end{aligned}$$

  is an isogeny for any integer m.

EXAMPLES

- For any positive integer m, define

$$[m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}}$$
$$[-m]P = -[m]P,$$

and let $[0]P$ be the zero isogeny. Then, the map

$$\begin{aligned}[m]\colon E &\to E\\ P &\mapsto [m]P\end{aligned}$$

is an isogeny for any integer m.

- If $K = \mathbb{F}_{p^r}$ for some positive integer r, then the map

$$\begin{aligned}\varphi\colon E &\to E^p\\ (x, y) &\mapsto (x^p, y^p)\end{aligned}$$

is an isogeny. In particular, φ^r is called *Frobenius endomorphism*.

ISOGENIES WITH A GIVEN KERNEL

In general, for any <u>finite</u> subgroup G of E, there exists another curve E/G and an isogeny

$$\varphi\colon E \to E/G$$

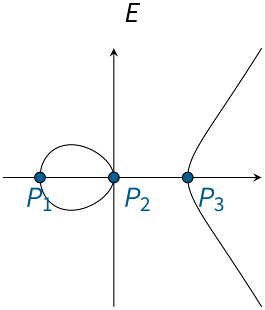
having kernel G.

ISOGENIES WITH A GIVEN KERNEL

In general, for any finite subgroup G of E, there exists another curve E/G and an isogeny

$$\varphi\colon E \to E/G$$

having kernel G.



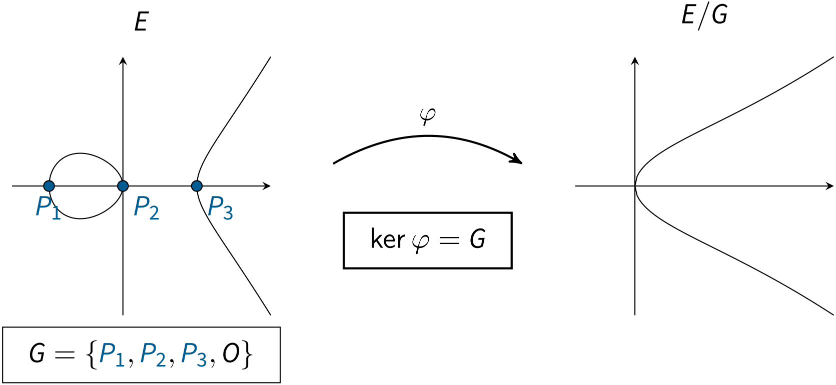
$$\boxed{G = \{P_1, P_2, P_3, O\}}$$

ISOGENIES WITH A GIVEN KERNEL

In general, for any finite subgroup G of E, there exists another curve E/G and an isogeny

$$\varphi\colon E \to E/G$$

having kernel G.



$$\boxed{\ker\varphi = G}$$

$$\boxed{G = \{P_1, P_2, P_3, O\}}$$

ENDOMORPHISMS

Let E be an elliptic curve over K. An *endomorphism* of E is an isogeny $E \to E$.
The set of all the endomorphisms of E is denoted by $\mathrm{End}(E)$.

ENDOMORPHISMS

Let E be an elliptic curve over K. An *endomorphism* of E is an isogeny $E \to E$.

The set of all the endomorphisms of E is denoted by $\mathrm{End}(E)$.

What is the structure of $\mathrm{End}(E)$?

ENDOMORPHISMS

Let E be an elliptic curve over K. An *endomorphism* of E is an isogeny $E \to E$.
The set of all the endomorphisms of E is denoted by $\mathrm{End}(E)$.

What is the structure of $\mathrm{End}(E)$?

THEOREM

$\mathrm{End}(E)$ *is a torsion-free* $\mathbb{Z}$*-module. In particular, the map*

$$\begin{aligned}[\ \ ]\colon \mathbb{Z} &\to \mathrm{End}(E)\\ m &\mapsto [m]\end{aligned}$$

is injective.

Therefore, $\mathrm{End}(E)$ always contains a copy of $\mathbb{Z}$.

COMPLEX MULTIPLICATION

Endomorphisms of the form $[m]$, for $m \in \mathbb{Z}$, are called *trivial*.

Can elliptic curves over K have non-trivial endomorphisms?

If $\mathrm{char}\, K = 0$

For ‘most of’ the elliptic curves,

$$\mathrm{End}(E) \cong \mathbb{Z}.$$

The others are called *CM-curves*, or *curves with complex multiplication*.

COMPLEX MULTIPLICATION

Endomorphisms of the form $[m]$, for $m \in \mathbb{Z}$, are called *trivial*.

Can elliptic curves over K have non-trivial endomorphisms?

If $\mathrm{char}\, K = 0$

For ‘most of’ the elliptic curves,

$$\mathrm{End}(E) \cong \mathbb{Z}.$$

The others are called *CM-curves*, or *curves with complex multiplication*.

If $K = \mathbb{F}_q$

All elliptic curves have non-trivial endomorphisms: one of them is the Frobenius endomorphism

$$(x, y) \mapsto (x^q, y^q).$$

SUPERSINGULAR ELLIPTIC CURVES

More precisely, when $\mathbb{Z} \subsetneq \mathrm{End}(E)$, two cases occur:

- $\mathrm{End}(E)$ is an order in an imaginary quadratic field;

SUPERSINGULAR ELLIPTIC CURVES

More precisely, when $\mathbb{Z} \subsetneq \mathrm{End}(E)$, two cases occur:

- $\mathrm{End}(E)$ is an order in an imaginary quadratic field;
- $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$ (this case occurs only if E is defined over a finite field!)

SUPERSINGULAR ELLIPTIC CURVES

More precisely, when $\mathbb{Z} \subsetneq \mathrm{End}(E)$, two cases occur:

- $\mathrm{End}(E)$ is an order in an imaginary quadratic field;
- $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$ (this case occurs only if E is defined over a finite field!)

An *order* in a finite-dimensional algebra A over $\mathbb{Q}$ is a subring that is also a $\mathbb{Z}$-module of maximal rank.

B is a *quaternion algebra* over $\mathbb{Q}$ if there exist $i, j \in B$ such that $1, i, j, ij$ are a basis for B over $\mathbb{Q}$ and

$$i^2 = a, \qquad j^2 = b, \qquad ji = -ij$$

for some $a, b \in \mathbb{Q}^*$.

SUPERSINGULAR ELLIPTIC CURVES

More precisely, when $\mathbb{Z} \subsetneq \mathrm{End}(E)$, two cases occur:

- $\mathrm{End}(E)$ is an order in an imaginary quadratic field;
- $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$ (this case occurs only if E is defined over a finite field!)

An *order* in a finite-dimensional algebra A over $\mathbb{Q}$ is a subring that is also a $\mathbb{Z}$-module of maximal rank.

B is a *quaternion algebra* over $\mathbb{Q}$ if there exist $i, j \in B$ such that $1, i, j, ij$ are a basis for B over $\mathbb{Q}$ and

$$i^2 = a, \qquad j^2 = b, \qquad ji = -ij$$

for some $a, b \in \mathbb{Q}^*$.

An elliptic curve E over $\mathbb{F}_q$ is *supersingular* if the latter case occurs, i.e. if $\mathrm{End}(E)$ is non-commutative.

MOTIVATION

HARD PROBLEMS FOR SUPERSINGULAR ELLIPTIC CURVES

Let p be a large prime, and suppose that we are given two supersingular elliptic curves E, E'.

HARD PROBLEMS FOR SUPERSINGULAR ELLIPTIC CURVES

Let p be a large prime, and suppose that we are given two supersingular elliptic curves E, E'.
The following problems are considered computationally hard (even for quantum computers!):

- Computing $\mathrm{End}(E)$.

HARD PROBLEMS FOR SUPERSINGULAR ELLIPTIC CURVES

Let p be a large prime, and suppose that we are given two supersingular elliptic curves E, E'.
The following problems are considered computationally hard (even for quantum computers!):

- Computing $\mathrm{End}(E)$.
- Computing an isogeny $\varphi \colon E \to E'$.

HARD PROBLEMS FOR SUPERSINGULAR ELLIPTIC CURVES

Let p be a large prime, and suppose that we are given two supersingular elliptic curves E, E'.
The following problems are considered computationally hard (even for quantum computers!):

- Computing $\mathrm{End}(E)$.
- Computing an isogeny $\varphi\colon E \to E'$.

The latter problem can be exploited in cryptography: an example is the CGL hash function (Charles, Lauter, and Goren 2009).

CGL HASH FUNCTION

THEOREM

Let E be an elliptic curve over K. Then E has exactly 3 subgroups of order 2.

CGL HASH FUNCTION

THEOREM

Let E be an elliptic curve over K. Then E has exactly 3 subgroups of order 2.

Let $m = b_1 b_2 \dots b_n$ be a bit string, and p a large prime.

CGL HASH FUNCTION

THEOREM

Let E be an elliptic curve over K. Then E has exactly 3 subgroups of order 2.

Let $m = b_1b_2 \dots b_n$ be a bit string, and p a large prime.
Setup:

1. Choose a supersingular curve E_0 over $\mathbb{F}_{p^2}$.

CGL HASH FUNCTION

THEOREM

Let E be an elliptic curve over K. Then E has exactly 3 subgroups of order 2.

Let $m = b_1 b_2 \dots b_n$ be a bit string, and p a large prime.

Setup:

1. Choose a supersingular curve E_0 over $\mathbb{F}_{p^2}$.
2. Choose a point $P \neq O$ lying on E_0 and such that $[2]P = 0$.

CGL HASH FUNCTION

THEOREM

Let E be an elliptic curve over K. Then E has exactly 3 subgroups of order 2.

Let $m = b_1 b_2 \ldots b_n$ be a bit string, and p a large prime.

Setup:

1. Choose a supersingular curve E_0 over $\mathbb{F}_{p^2}$.
2. Choose a point $P \neq O$ lying on E_0 and such that $[2]P = 0$.
3. Compute the isogeny $E_0 \to E_1$ with kernel $\{P, O\}$.

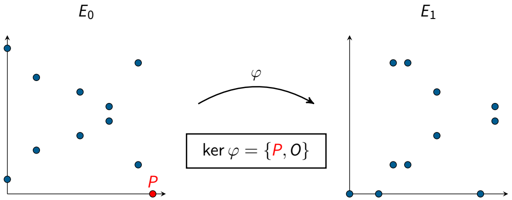
CGL HASH FUNCTION

THEOREM

Let E be an elliptic curve over K. Then E has exactly 3 subgroups of order 2.

Let $m = b_1 b_2 \dots b_n$ be a bit string, and p a large prime.
Setup:

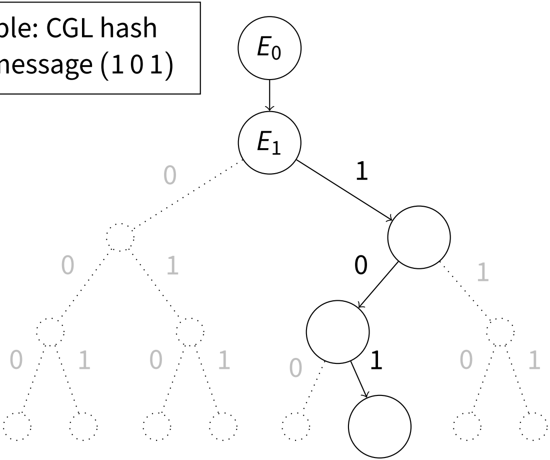
1. Choose a supersingular curve E_0 over $\mathbb{F}_{p^2}$.
2. Choose a point $P \neq O$ lying on E_0 and such that $[2]P = 0$.
3. Compute the isogeny $E_0 \to E_1$ with kernel $\{P, O\}$.



Hash function:

1. Compute the 3 isogenies whose respective kernels are the 3 order-2 subgroups of E_1. One of these isogenies leads back to E_0: we discard it. Label the other two with E_2^0 and E_2^1.

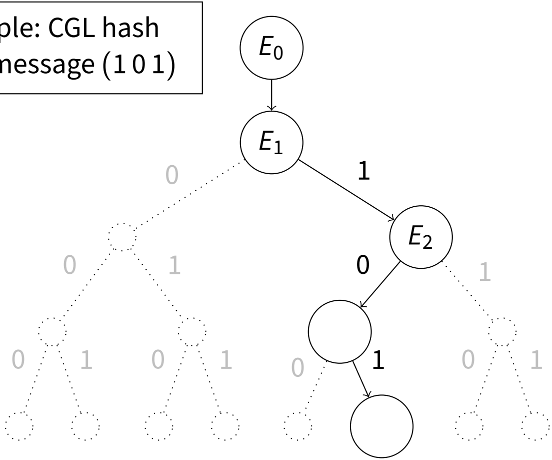
Example: CGL hash of the message (1 0 1)



Hash function:

2. If the first bit of the message is 0, set $E_2 = E_2^0$ and find two vertices E_3^{00} and E_3^{01} like in the previous step. Else, if the first bit of m is 1, set $E_2 = E_2^1$ and find two new vertices E_3^{10} and E_3^{11}.

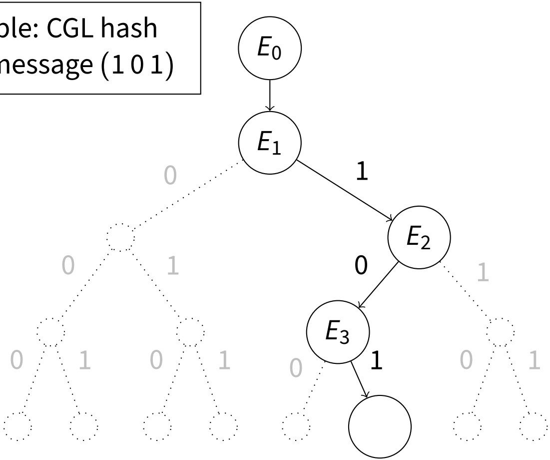
Example: CGL hash of the message (1 0 1)



Hash function:

3. Similarly, choose E_{i+1} depending on the i-th bit of the message.

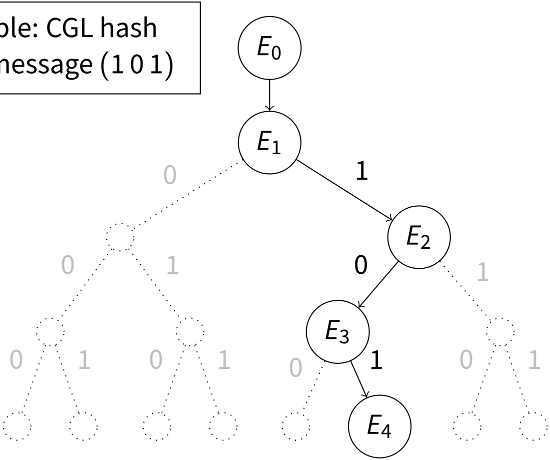
Example: CGL hash
of the message (1 0 1)



Hash function:

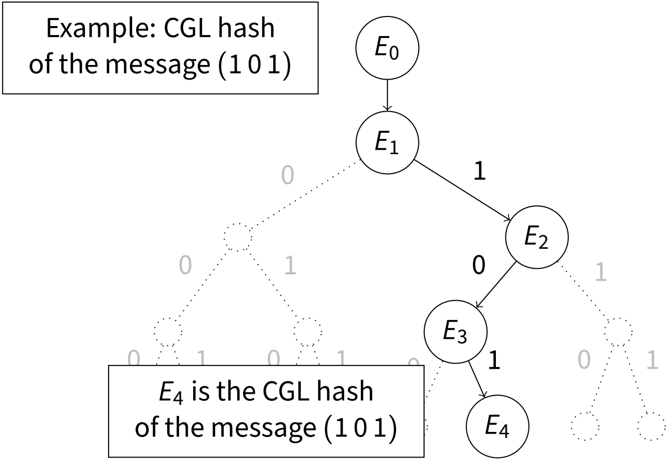
4. Output the hashed message $E_{n+1} = E_{n+1}^{b_1 b_2 \ldots b_n}$, where b_i are the bits of the original message.

Example: CGL hash of the message (1 0 1)



Hash function:

4. Output the hashed message $E_{n+1} = E_{n+1}^{b_1 b_2 \dots b_n}$, where b_i are the bits of the original message.



Example: CGL hash of the message (1 0 1)

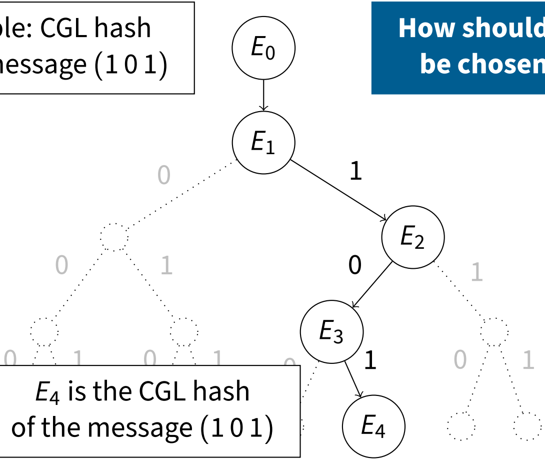
E_4 is the CGL hash of the message (1 0 1)

Hash function:

4. Output the hashed message $E_{n+1} = E_{n+1}^{b_1 b_2 \ldots b_n}$, where b_i are the bits of the original message.

Example: CGL hash of the message (1 0 1)

How should E_0 be chosen?



E_4 is the CGL hash of the message (1 0 1)

CHOICE OF THE STARTING CURVE

To sum up: the CGL hash function consists in a ‘walk’

$$E_0 \to E_1 \to \cdots \to E_{n+1}$$

on a graph whose vertices are supersingular EC, and whose edges are suitably chosen isogenies.

CHOICE OF THE STARTING CURVE

To sum up: the CGL hash function consists in a ‘walk’

$$E_0 \to E_1 \to \cdots \to E_{n+1}$$

on a graph whose vertices are supersingular EC, and whose edges are suitably chosen isogenies.

How should E_0 be chosen?

CHOICE OF THE STARTING CURVE

To sum up: the CGL hash function consists in a ‘walk’

$$E_0 \to E_1 \to \cdots \to E_{n+1}$$

on a graph whose vertices are supersingular EC, and whose edges are suitably chosen isogenies.

How should E_0 be chosen?

THEOREM

$E\colon y^2 = x^3 + 1$ *is supersingular* $\iff$ $p \equiv 2 \mod 3.$

Naive solution: fix $p \equiv 2 \mod 3$ and set $E_0\colon y^2 = x^3 + 1.$

THE WEAKNESS OF $y^2 = x^3 + 1$

However, setting $E_0 : y^2 = x^3 + 1$ as a starting point of the CGL function **compromises the collision-resistance** of the hash because

- $\mathrm{End}(E_0)$ can be efficiently computed.

THE WEAKNESS OF $y^2 = x^3 + 1$

However, setting $E_0 : y^2 = x^3 + 1$ as a starting point of the CGL function **compromises the collision-resistance** of the hash because

- $\mathrm{End}(E_0)$ can be efficiently computed.
- (Wesolowski 2021) Given $\mathrm{End}(E_0)$ and E_{n+1}, one can efficiently compute a (new) message whose hash is E_{n+1}. A collision!

RANDOM WALKS FROM $y^2 = x^3 + 1$

A naive workaround: starting from $E\colon y^2 = x^3 + 1$, do a ‘random walk’ $E \to \cdots \to E'$ and set $\boldsymbol{E_0 = E'}$:

$$\overbrace{E \to \cdots \to\ }^{\text{random walk}} \underbrace{E' \to E_1 \to \cdots \to E_{n+1}}_{\text{CGL hash function}}.$$

RANDOM WALKS FROM $y^2 = x^3 + 1$

A naive workaround: starting from $E\colon y^2 = x^3 + 1$, do a ‘random walk’ $E \to \cdots \to E'$ and set $\boldsymbol{E_0 = E'}$:

$$\overbrace{E \to \cdots \to E'}^{\text{random walk}} \!\!\!\!\underbrace{ \to E_1 \to \cdots \to E_{n+1}}_{\text{CGL hash function}}.$$

Good news

(Pizer 1998) A uniformly random E_0 can be found after a few steps.

RANDOM WALKS FROM $y^2 = x^3 + 1$

A naive workaround: starting from $E\colon y^2 = x^3 + 1$, do a ‘random walk’ $E \to \cdots \to E'$ and set $\boldsymbol{E_0 = E'}$:

$$\overbrace{E \to \cdots \to E'}^{\text{random walk}} \to E_1 \to \cdots \to E_{n+1}.$$

$$\underbrace{E' \to E_1 \to \cdots \to E_{n+1}}_{\text{CGL hash function}}$$

Good news

(Pizer 1998) A uniformly random E_0 can be found after a few steps.

Bad news

(Wesolowski 2021) Knowing both $\mathrm{End}(E)$ and the random walk $E \to E'$, one can efficiently compute $\mathrm{End}(E_0)$.

RANDOM WALKS FROM $y^2 = x^3 + 1$

A naive workaround: starting from $E\colon y^2 = x^3 + 1$, do a 'random walk' $E \to \cdots \to E'$ and set $\boldsymbol{E_0 = E'}$:

$$\overbrace{E \to \cdots \to \rlap{$\underbrace{\phantom{E' \to E_1 \to \cdots \to E_{n+1}}}_{\text{CGL hash function}}$}E'}^{\text{random walk}} \to E_1 \to \cdots \to E_{n+1}\,.$$

Good news

(Pizer 1998) A uniformly random E_0 can be found after a few steps.

Bad news

(Wesolowski 2021) Knowing both $\mathrm{End}(E)$ and the random walk $E \to E'$, one can efficiently compute $\mathrm{End}(E_0)$.
Knowing $\mathrm{End}(E_0)$ and E_{n+1}, one can efficiently find a collision.

THE cSRS PROBLEM

In conclusion: we are not able to find a suitable starting EC for the CGL function!

THE cSRS PROBLEM

In conclusion: we are not able to find a suitable starting EC for the CGL function!

Cryptographic Supersingular Random Sampling (cSRS) problem

Find an algorithm Alg that, on input a large prime p, samples a uniformly random supersingular elliptic curve E over $\mathbb{F}_p$ (or $\mathbb{F}_{p^2}$).

THE cSRS PROBLEM

In conclusion: we are not able to find a suitable starting EC for the CGL function!

Cryptographic Supersingular Random Sampling (cSRS) problem

Find an algorithm Alg that, on input a large prime p, samples a uniformly random supersingular elliptic curve E over $\mathbb{F}_p$ (or $\mathbb{F}_{p^2}$).

Computing $\mathrm{End}(E)$ from the equation of E $\underline{\text{and the transcript of } \mathrm{Alg}}$ must be hard.

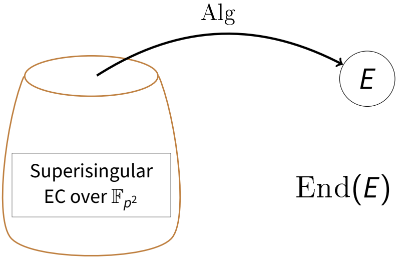
THE cSRS PROBLEM

In conclusion: we are not able to find a suitable starting EC for the CGL function!

Cryptographic Supersingular Random Sampling (cSRS) problem

Find an algorithm Alg that, on input a large prime p, samples a uniformly random supersingular elliptic curve E over $\mathbb{F}_p$ (or $\mathbb{F}_{p^2}$).

Computing $\mathrm{End}(E)$ from the equation of E $\underline{\text{and the transcript of } \mathrm{Alg}}$ must be hard.



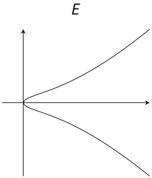
$\mathrm{End}(E) = ?$

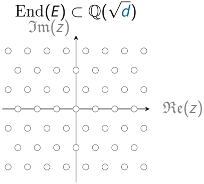
Known approaches

CM REDUCTION

THEOREM (DEURING 1941)

Fix a prime $p \geq 5$. Let E be an elliptic curve over a number field K, with $\mathrm{End}(E)$ isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$...

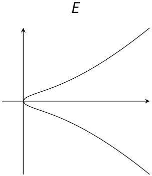




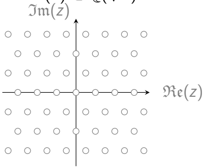
CM REDUCTION

THEOREM (DEURING 1941)

…Let $\mathfrak{P}$ be a prime of K over p, and suppose that E has a good reduction (i.e. the $\mathfrak{P}$-adic valuation of $\Delta(E)$ equals 0) modulo $\mathfrak{P}$, which we denote by $\tilde{E}$…



$\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{d})$

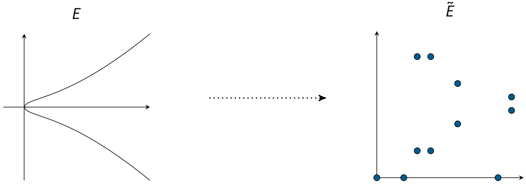


CM REDUCTION

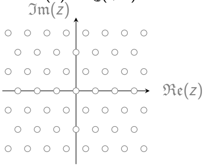
THEOREM (DEURING 1941)

...Then

$\tilde{E}$ is supersingular $\Leftrightarrow$ d is not a quadratic residue modulo p.



$\mathrm{End}(E) \subset \mathbb{Q}(\sqrt{d})$



$$\subseteq \qquad \mathrm{End}(\tilde{E})$$

DEURING'S THEOREM AND CSRS PROBLEM

Deuring's theorem provides an efficient criterion for determining whether the reduction modulo p of a CM curve is supersingular or not.

DEURING'S THEOREM AND CSRS PROBLEM

Deuring's theorem provides an efficient criterion for determining whether the reduction modulo p of a CM curve is supersingular or not.

Strategy to compute a supersingular EC over $\mathbb{F}_p$:

Compute a CM curve over a number field, and check if its reduction modulo *p* is supersingular.

j-INVARIANTS

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over K. The *j-invariant* of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)} = 6912\frac{A^3}{4A^3 + 27B^2}.$$

j-INVARIANTS

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over K. The *j-invariant* of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)} = 6912\frac{A^3}{4A^3 + 27B^2}.$$

THEOREM

- *Two elliptic curves over K are isomorphic if and only if they have the same j-invariant.*
- *Let $j_0 \in \overline{K}$. There exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.*

j-INVARIANTS

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over K. The *j-invariant* of E is

$$j(E) = -1728\frac{(4A)^3}{\Delta(E)} = 6912\frac{A^3}{4A^3 + 27B^2}.$$

THEOREM

- *Two elliptic curves over K are isomorphic if and only if they have the same j-invariant.*
- *Let $j_0 \in \overline{K}$. There exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.*

EXAMPLE

The curve $y^2 = x^3 + 1$ has j-invariant 0.

FINDING CM j-INVARIANTS

THEOREM

Let E be an elliptic curve over a number field K, and let $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic order.
Then, $\mathrm{End}(E) \cong \mathcal{O}$ if and only if $j(E)$ is a root of the **Hilbert class polynomial $P_{\mathcal{O}}$.**

FINDING CM j-INVARIANTS

THEOREM

Let E be an elliptic curve over a number field K, and let $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic order.
Then, $\mathbf{End}(\boldsymbol{E}) \cong \boldsymbol{\mathcal{O}}$ if and only if $j(E)$ is a root of the **Hilbert class polynomial $P_{\mathcal{O}}$.**

We can skip the definition of $P_{\mathcal{O}}$ here... but we remark its surprising features:

- $P_{\mathcal{O}}$ has integer coefficients.

FINDING CM j-INVARIANTS

THEOREM

Let E be an elliptic curve over a number field K, and let $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic order.
Then, $\mathrm{End}(E) \cong \mathcal{O}$ if and only if $j(E)$ is a root of the ***Hilbert class polynomial $P_{\mathcal{O}}$.***

We can skip the definition of $P_{\mathcal{O}}$ here... but we remark its surprising features:

- $P_{\mathcal{O}}$ has integer coefficients.
- $P_{\mathcal{O}}$ can be explicitly computed if the discriminant of $\mathcal{O}$ is small.

FINDING CM j-INVARIANTS

THEOREM

Let E be an elliptic curve over a number field K, and let $\mathcal{O} \subset \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic order.
Then, $\mathbf{End}(\boldsymbol{E}) \cong \boldsymbol{\mathcal{O}}$ if and only if $j(E)$ is a root of the **Hilbert class polynomial $\boldsymbol{P_{\mathcal{O}}}$.**

We can skip the definition of $P_{\mathcal{O}}$ here... but we remark its surprising features:

- $P_{\mathcal{O}}$ has integer coefficients.
- $P_{\mathcal{O}}$ can be explicitly computed if the discriminant of $\mathcal{O}$ is small.

Thus, supersingular j-invariants modulo p can be found as roots of $P_{\mathcal{O}}$ modulo p, for a suitably chosen $\mathcal{O}$. This is the core of **Bröker's algorithm**.

BRÖKER'S ALGORITHM

The following algorithm (Bröker 2009) finds a supersingular EC over $\mathbb{F}_p$ in $\tilde{O}(\log p)$ time:

Algorithm 1: Bröker's algorithm

```
Input: A prime $p \geq 5$.
Output: A supersingular $j$-invariant $j \in \mathbb{F}_p$.
Set $q = 3$;
while $\left(\frac{-q}{p}\right) = 1$ do
    Assign $q$ to the next prime equivalent to 3 modulo 4;
end
Compute the Hilbert class polynomial $P_{\mathcal{O}}$ relative to the quadratic
  order $\mathcal{O}$ of discriminant $-q$;
Find a root $\alpha \in \mathbb{F}_p$ of $P_{\mathcal{O}}$ modulo $p$;
Set $j = \alpha$.
```

BRÖKER'S METHOD: A SOLUTION FOR THE CSRS PROBLEM?

Let E be the superisingular EC over $\mathbb{F}_p$ output by Bröker's algorithm.

Is $\mathrm{End}(E)$ hard to compute?

BRÖKER'S METHOD: A SOLUTION FOR THE CSRS PROBLEM?

Let E be the superisingular EC over $\mathbb{F}_p$ output by Bröker's algorithm.

Is $\mathrm{End}(E)$ hard to compute?

Unfortunately (Love and Boneh 2020), the answer is negative!

(Underlying reason: $\mathrm{End}(E)$ contains an order of small discriminant.)

EXHAUSTIVE SEARCH

It is natural to ask if the most obvious approach might solve the cSRS problem:

Sample a random $j \in \overline{\mathbb{F}_p}$, and check if it is supersingular.

EXHAUSTIVE SEARCH

It is natural to ask if the most obvious approach might solve the cSRS problem:

Sample a random $j \in \overline{\mathbb{F}_p}$, and check if it is supersingular.

However...

THEOREM

Fix a prime p. There exist $O(p)$ supersingular j-invariants, and they all lie in $\mathbb{F}_{p^2}$.
The supersingular j-invariants over $\mathbb{F}_p$ are $O(\sqrt{p})$.

Consequence: if p is large, it is extremely unlikely that a random element of $\mathbb{F}_{p^2}$ (or $\mathbb{F}_p$) is a supersingular j-invariant.

HASSE INVARIANT

Consider a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Define the *Hasse invariant* of E:

$$A_p = \text{coefficient of } x^{p-1} \text{ in } (x^3 + Ax + B)^{(p-1)/2}.$$

HASSE INVARIANT

Consider a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Define the *Hasse invariant* of E:

$$A_p = \text{coefficient of } x^{p-1} \text{ in } (x^3 + Ax + B)^{(p-1)/2}.$$

THEOREM

Let E be an elliptic curve over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. Then E is supersingular if and only if $A_p = 0$.

HASSE INVARIANT

Consider a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$. Define the *Hasse invariant* of E:

$$A_p = \text{coefficient of } x^{p-1} \text{ in } (x^3 + Ax + B)^{(p-1)/2}.$$

THEOREM

Let E be an elliptic curve over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. Then E is supersingular if and only if $A_p = 0$.

A_p can be seen as a polynomial in the variables A and B, whose roots are exactly the parameters of all supersingular elliptic curves over $\overline{\mathbb{F}_p}$.

IS THE HASSE INVARIANT USEFUL?

Problem

The degree of A_p is exponential in the size of p.

IS THE HASSE INVARIANT USEFUL?

Problem

The degree of A_p is exponential in the size of p.

Possible research directions

We can find arbitrarilty many roots of A_p using Bröker's method + random walks.
We also know something more about the coefficients A_p...

Alternative directions

OTHER MODELS OF ELLIPTIC CURVES

Elliptic curves have various representations other than the Weierstrass model $y^2 = x^3 + Ax + B$.

Model	Affine equation	j-invariant	Equivalent Weierstrass model
Legendre	$y^2 = x(x-1)(x-\lambda)$	$2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$	$\begin{cases} A = \frac{-\lambda^2+\lambda-1}{3} \\ B = \frac{-2\lambda^3+3\lambda^2+3\lambda-2}{27} \end{cases}$
Montgomery	$B'y^2 = x^3 + A'x^2 + x$	$\frac{256(A'^2-3)^3}{A'^2-4}$	$\begin{cases} A = B'^2\left(1-\frac{A'^2}{3}\right), \\ B = \frac{B'^3A'}{3}\left(\frac{2A'^2}{9}-1\right) \end{cases}$
Jacobi	$y^2 = \epsilon x^4 - 2\delta x^2 + 1$	$64\frac{(\delta^2+3\epsilon)^3}{\epsilon(\delta^2-\epsilon)^2}$	$\begin{cases} A = -4\epsilon - \frac{4}{3}\delta^2, \\ B = -\frac{16}{27}\delta(\delta^2-9\epsilon). \end{cases}$

GENERALISED HASSE INVARIANT

The Hasse invariant can be actually defined for any of the above models.

GENERALISED HASSE INVARIANT

The Hasse invariant can be actually defined for any of the above models.

Namely, consider a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve $E\colon y^2 = f(x)$ over $\mathbb{F}_q$ as in one of the above models. Define the *Hasse invariant* of E:

$$A_p = \text{coefficient of } x^{p-1} \text{ in } (f(X))^{(p-1)/2}.$$

GENERALISED HASSE INVARIANT

The Hasse invariant can be actually defined for any of the above models.

Namely, consider a finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve $E\colon y^2 = f(x)$ over $\mathbb{F}_q$ as in one of the above models. Define the *Hasse invariant* of E:

$$A_p = \text{coefficient of } x^{p-1} \text{ in } (f(X))^{(p-1)/2}.$$

THEOREM

Let E be an elliptic curve over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$. Then E is supersingular if and only if $A_p = 0$.

COMPUTING A_p

For each model of elliptic curve, we explicitly constructed A_p.

To ease notation, set $m = (p-1)/2$.

Model	A_p
Weierstrass	$\sum_{i=\lceil \frac{p-1}{4} \rceil}^{\lfloor \frac{p-1}{3} \rfloor} \binom{m}{i} \binom{m-i}{2m-3i} A^{2m-3i} B^{2i-m}$
Legendre	$(-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i$
Montgomery	$\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{i} \binom{m-i}{m-2i} A^{m-2i}$
Jacobi	$\sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{i} \binom{m-i}{m-2i} \epsilon^i (-2\delta)^{m-2i}$

DIVISION POLYNOMIALS

One can define a family of polynomials

$$\psi_m \in \mathbb{Z}[A, B, x, y],$$

called *divison polynomials* and indexed by $m = 2, 3, 4, \ldots,$ with the following property:

DIVISION POLYNOMIALS

One can define a family of polynomials

$$\psi_m \in \mathbb{Z}[A, B, x, y],$$

called *divison polynomials* and indexed by $m = 2, 3, 4, \ldots$, with the following property:

$$\psi_m(A, B, x_0, y_0) = 0$$
$$\Updownarrow$$
$$[m](x_0, y_0) = O \quad \text{on the curve} \quad E\colon y^2 = x^3 + Ax + B.$$

p-TORSION POINTS

THEOREM (DOLISKANI 2018)

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{F}_{p^2}$, and assume $j(E) \notin \{0, 1728\}$.
Then E is supersingular if and only if $\psi_p^2(A, B, x_0, y_0) - 1 = 0$ for each $(x_0, y_0) \in E$.

We generalised the above result to the cases $j = 0, 1728$.

p-TORSION POINTS

THEOREM (DOLISKANI 2018)

Let $E\colon\ y^2 = x^3 + Ax + B$ *be an elliptic curve over* $\mathbb{F}_{p^2}$*, and assume* $j(E) \notin \{0, 1728\}$*.*
Then E *is supersingular if and only if* $\psi_p^2(A, B, x_0, y_0) - 1 = 0$ *for each* $(x_0, y_0) \in E$*.*

We generalised the above result to the cases $j = 0, 1728$.

REMARK

The variable y *can be eliminated from* $\psi_p^2(A, B, x, y) - 1 = 0$*, since we are working modulo the curve equation.*

COMPUTING $\psi_p^2(A, B, x, y) - 1$

Strategy to sample supersingular elliptic curves:

- compute $\psi_p^2 - 1$ as a polynomial in $\mathbb{F}_p[A, B, x]$;

COMPUTING $\psi_p^2(A, B, x, y) - 1$

Strategy to sample supersingular elliptic curves:

- compute $\psi_p^2 - 1$ as a polynomial in $\mathbb{F}_p[A, B, x]$;
- find values of A and B that annihilate $\psi_p^2 - 1$: these are parameters of a supersingular elliptic curve.

COMPUTING $\psi_p^2(A, B, x, y) - 1$

Strategy to sample supersingular elliptic curves:

- compute $\psi_p^2 - 1$ as a polynomial in $\mathbb{F}_p[A, B, x]$;
- find values of A and B that annihilate $\psi_p^2 - 1$: these are parameters of a supersingular elliptic curve.

Further assumptions to diminish the computational cost:

- restrict the root finding to $A, B \in \mathbb{F}_p$;
- assume $B = -1 - A$.

COMPUTING $\psi_p^2(A, B, x, y) - 1$

Strategy to sample supersingular elliptic curves:

- compute $\psi_p^2 - 1$ as a polynomial in $\mathbb{F}_p[A, B, x]$;
- find values of A and B that annihilate $\psi_p^2 - 1$: these are parameters of a supersingular elliptic curve.

Further assumptions to diminish the computational cost:

- restrict the root finding to $A, B \in \mathbb{F}_p$;
- assume $B = -1 - A$.

Still not enough!

SMALL-TORSION POINTS

Supersingular EC can be characterized in terms of small-degree division polynomial, if p has a special form.

THEOREM

Let $p = \prod_{i=1}^{r} \ell_i^{e_i} - 1$ *be a prime such that*

$$\prod_{i=1}^{r} \ell_i > 2\sqrt{p},$$

and let $E\colon\ y^2 = x^3 + Ax + B$ *be an elliptic curve over* $\mathbb{F}_p$*.*
Then E *is supersingular if and only if the division polynomial* $\psi_{\ell_i}(A, B, x, y)$ *has a root* $(x_i, y_i) \in E(\mathbb{F}_p)$ *for each* $i \in \{1, \ldots, r\}$*.*

A SYSTEM OF 'SMALL' DIVISION POLYNOMIALS

Consequence: any solution of the system of equations

$$\begin{cases} \psi_{\ell_i}(A, B, x_i, y_i) = 0 & \text{for each } i \in \{1, \dots r\} \\ y_i^2 - x_i^3 - Ax_i - B = 0 & \text{for each } i \in \{1, \dots r\} \\ x_i^p - x_i = 0 & \text{for each } i \in \{1, \dots r\} \\ y_i^p - y_i = 0 & \text{for each } i \in \{1, \dots r\} \\ A^p - A = 0 & \\ B^p - B = 0 & \end{cases}$$

yields the coefficients of a supersingular elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$, together with the coordinates of $\mathbb{F}_p$-rational ℓ_i-torsion points (x_i, y_i) for $i \in \{1, \dots, r\}$.

A SYSTEM OF 'SMALL' DIVISION POLYNOMIALS

Consequence: any solution of the system of equations

$$\begin{cases} \psi_{\ell_i}(A, B, x_i, y_i) = 0 & \text{for each } i \in \{1, \dots r\} \\ y_i^2 - x_i^3 - Ax_i - B = 0 & \text{for each } i \in \{1, \dots r\} \\ x_i^p - x_i = 0 & \text{for each } i \in \{1, \dots r\} \\ y_i^p - y_i = 0 & \text{for each } i \in \{1, \dots r\} \\ A^p - A = 0 \\ B^p - B = 0 \end{cases}$$

yields the coefficients of a supersingular elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_p$, together with the coordinates of $\mathbb{F}_p$-rational ℓ_i-torsion points (x_i, y_i) for $i \in \{1, \dots, r\}$.

This method seems promising...

ESSENTIAL BIBLIOGRAPHY

Bröker, R. (2009). “Constructing supersingular elliptic curves”. In: *Journal of Combinatorics and Number Theory* 1(3), pp. 269–273.

Charles, D. X., K. E. Lauter, and E. Z. Goren (2009). “Cryptographic Hash Functions from Expander Graphs”. In: *Journal of Cryptology* 22 (1), pp. 93–113.

Deuring, M. (1941). “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper”. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14.1, pp. 197–272.

Doliskani, J. (2018). “On Division Polynomial PIT and Supersingularity”. In: *Computing Research Repository (CoRR)*.

Love, J. and D. Boneh (2020). “Supersingular Curves With Small Non-integer Endomorphisms”. In: *Fourteenth Algorithmic Number Theory Symposium*, pp. 7–22.

Pizer, A. K. (1998). “Ramanujan graphs”. In: *Computational perspectives on number theory (Chicago, IL, 1995)*. Amer. Math. Soc., 159–178.

Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*. Vol. 151. Graduate Texts in Mathematics. Springer.

Wesolowski, B. (2021). “The supersingular isogeny path and endomorphism ring problems are equivalent”. In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, pp. 1100–1111.

Thank you for your attention!