

CSIDH: a post-quantum drop-in replacement for (EC)DH

Wouter Castryck¹ Tanja Lange² Chloe Martindale²
Lorenz Panny² Joost Renes³

¹KU Leuven ²TU Eindhoven ³RU Nijmegen

ECC Autumn School, Osaka, 17-18 November 2018

1 / 40

Traditional Diffie-Hellman key exchange

Suppose that $(G, *)$ is a finite group. Examples:

- ▶ $(G, *) = (\mathbb{F}_p - \{0\}, \times)$.

3 / 40



2 / 40

Traditional Diffie-Hellman key exchange

Suppose that $(G, *)$ is a finite group. Examples:

- ▶ $(G, *) = (\mathbb{F}_p - \{0\}, \times)$.
- ▶ $(G, *) = (E(\mathbb{F}_p), +)$, where $+$ is the elliptic curve addition that was defined in Mehdi's lecture.

3 / 40

Traditional Diffie-Hellman key exchange

Suppose that $(G, *)$ is a finite group. Examples:

- ▶ $(G, *) = (\mathbb{F}_p - \{0\}, \times)$.
- ▶ $(G, *) = (E(\mathbb{F}_p), +)$, where $+$ is the elliptic curve addition that was defined in Mehdi's lecture.

For a finite group $(G, *)$ we have a map

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto \underbrace{g * \cdots * g}_{x \text{ times}}. \end{aligned}$$

Traditional Diffie-Hellman key exchange

Suppose that $(G, *)$ is a finite group. Examples:

- ▶ $(G, *) = (\mathbb{F}_p - \{0\}, \times)$.
- ▶ $(G, *) = (E(\mathbb{F}_p), +)$, where $+$ is the elliptic curve addition that was defined in Mehdi's lecture.

For a finite group $(G, *)$ we have a map

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto \underbrace{g * \cdots * g}_{x \text{ times}}. \end{aligned}$$

Examples:

- ▶ $g \in \mathbb{F}_p - \{0\}$, then $(x, g) \mapsto g^x$.

3 / 40

3 / 40

Traditional Diffie-Hellman key exchange

Suppose that $(G, *)$ is a finite group. Examples:

- ▶ $(G, *) = (\mathbb{F}_p - \{0\}, \times)$.
- ▶ $(G, *) = (E(\mathbb{F}_p), +)$, where $+$ is the elliptic curve addition that was defined in Mehdi's lecture.

For a finite group $(G, *)$ we have a map

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto \underbrace{g * \cdots * g}_{x \text{ times}}. \end{aligned}$$

Examples:

- ▶ $g \in \mathbb{F}_p - \{0\}$, then $(x, g) \mapsto g^x$.
- ▶ $P \in E(\mathbb{F}_p)$, then $(x, P) \mapsto xP$.

Traditional Diffie-Hellman key exchange

Suppose that $(G, *)$ is a finite group. Examples:

- ▶ $(G, *) = (\mathbb{F}_p - \{0\}, \times)$.
- ▶ $(G, *) = (E(\mathbb{F}_p), +)$, where $+$ is the elliptic curve addition that was defined in Mehdi's lecture.

For a finite group $(G, *)$ we have a map

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto \underbrace{g * \cdots * g}_{x \text{ times}}. \end{aligned}$$

Examples:

- ▶ $g \in \mathbb{F}_p - \{0\}$, then $(x, g) \mapsto g^x$.
- ▶ $P \in E(\mathbb{F}_p)$, then $(x, P) \mapsto xP$.

For simplicity, for a finite group $(G, *)$ and $x \in \mathbb{Z}$, we'll write g^x for $\underbrace{g * \cdots * g}_{x \text{ times}}$.

3 / 40

3 / 40

Traditional Diffie-Hellman key exchange

For a finite group $(G, *)$, if $g \in G$ and $x \in \mathbb{Z}$, we write $g^x = \underbrace{g * \cdots * g}_{x \text{ times}}$.



Traditional Diffie-Hellman key exchange

For a finite group $(G, *)$, if $g \in G$ and $x \in \mathbb{Z}$, we write $g^x = \underbrace{g * \cdots * g}_{x \text{ times}}$.



$g \in G$



$a \in \mathbb{Z}$

$b \in \mathbb{Z}$

Traditional Diffie-Hellman key exchange

For a finite group $(G, *)$, if $g \in G$ and $x \in \mathbb{Z}$, we write $g^x = \underbrace{g * \cdots * g}_{x \text{ times}}$.



$a \in \mathbb{Z}$

$g \in G$

g^a

\longrightarrow

g^b

\longleftarrow



$b \in \mathbb{Z}$

Traditional Diffie-Hellman key exchange

For a finite group $(G, *)$, if $g \in G$ and $x \in \mathbb{Z}$, we write $g^x = \underbrace{g * \cdots * g}_{x \text{ times}}$.



$a \in \mathbb{Z}$

$(g^b)^a$

$g \in G$

g^a

\longrightarrow

g^b

\longleftarrow

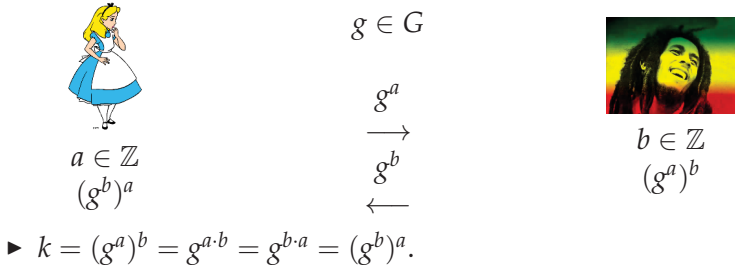


$b \in \mathbb{Z}$

$(g^a)^b$

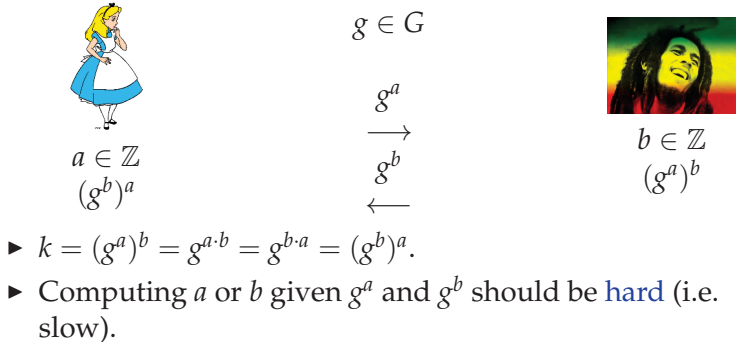
Traditional Diffie-Hellman key exchange

For a finite group $(G, *)$, if $g \in G$ and $x \in \mathbb{Z}$, we write $g^x = \underbrace{g * \dots * g}_{x \text{ times}}$.



Traditional Diffie-Hellman key exchange

For a finite group $(G, *)$, if $g \in G$ and $x \in \mathbb{Z}$, we write $g^x = \underbrace{g * \dots * g}_{x \text{ times}}$.

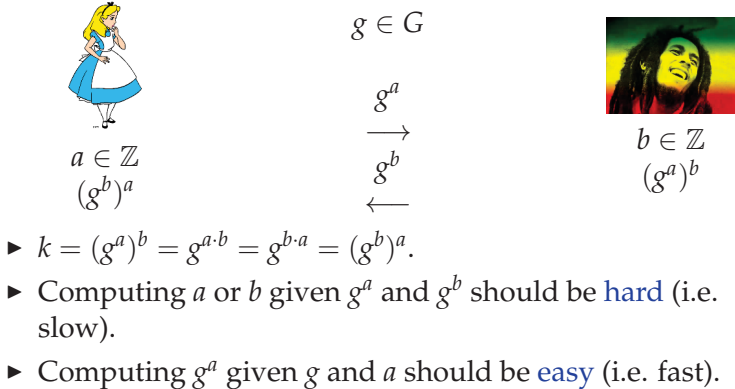


4 / 40

4 / 40

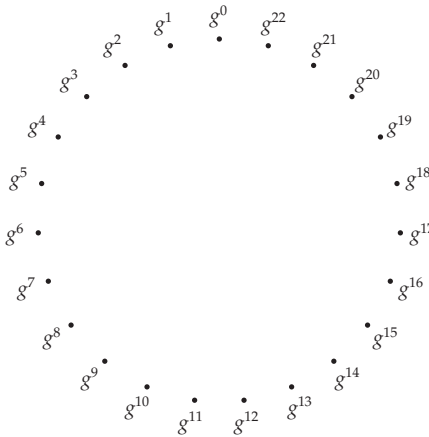
Traditional Diffie-Hellman key exchange

For a finite group $(G, *)$, if $g \in G$ and $x \in \mathbb{Z}$, we write $g^x = \underbrace{g * \dots * g}_{x \text{ times}}$.



Square-and-multiply

Computing g^a : an example. Suppose $|G| = 23$ and that Alice computes g^{13} .

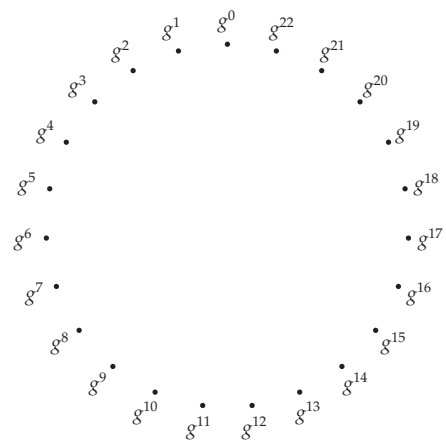


4 / 40

5 / 40

Square-and-multiply

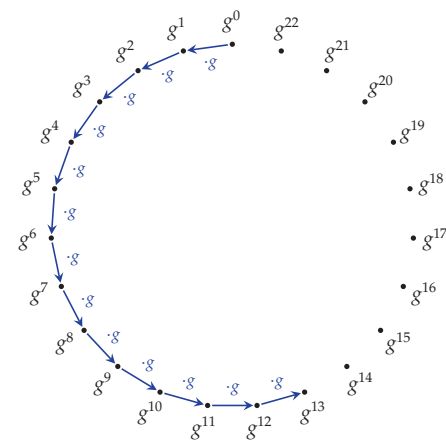
Computing g^a : an example. Suppose $|G| = 23$ and that Alice computes g^{13} .



5 / 40

Square-and-multiply

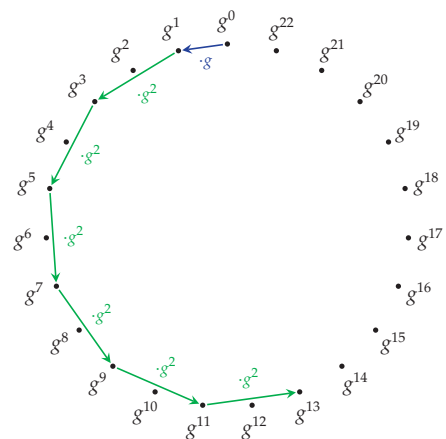
Computing g^a : an example. Suppose $|G| = 23$ and that Alice computes g^{13} .



5 / 40

Square-and-multiply

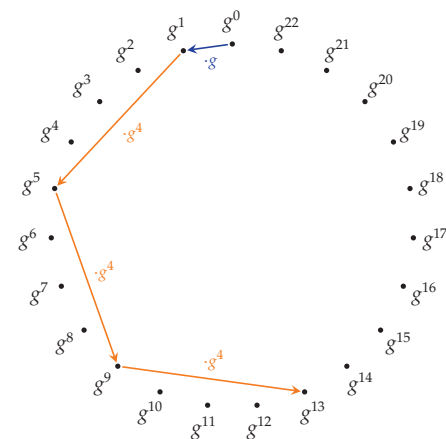
Computing g^a : an example. Suppose $|G| = 23$ and that Alice computes g^{13} .



5 / 40

Square-and-multiply

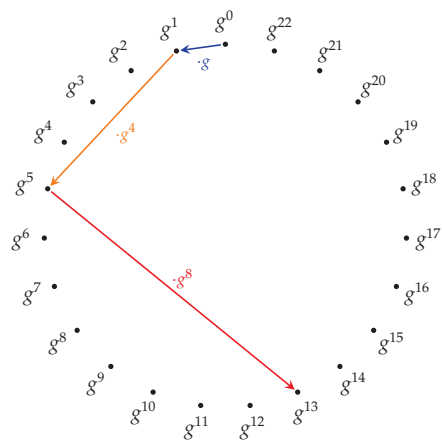
Computing g^a : an example. Suppose $|G| = 23$ and that Alice computes g^{13} .



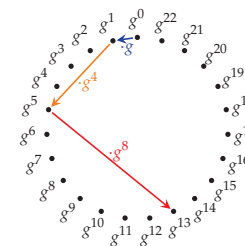
5 / 40

Square-and-multiply

Computing g^a : an example. Suppose $|G| = 23$ and that Alice computes g^{13} .



Square-and-multiply

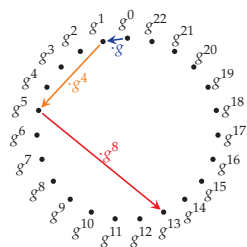


1

5 / 40

6 / 40

Square-and-multiply

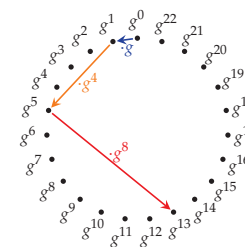


- Alice uses the knowledge that $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ to compute g^{13} .

1

6 / 40

Square-and-multiply

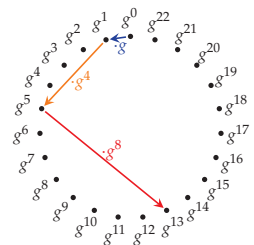


- Alice uses the knowledge that $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ to compute g^{13} .
- An (naïve)¹ attacker has to check g^a for $a = 0, \dots, 13$, so has **no shortcuts**.

¹a smart attacker like Mehdi can often exploit the structure of the specific group to do better than this

6 / 40

Square-and-multiply



- ▶ Alice uses the knowledge that $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ to compute g^{13} .
- ▶ An (naïve) ¹ attacker has to check g^a for $a = 0, \dots, 13$, so has **no shortcuts**.
- ▶ **Exercise:** prove that, for any cyclic group G of size n , if $g \in G$ and $a \in \mathbb{Z}$, Alice can compute g^a in $\leq \log_2(n)$ (multiplication) steps. (In **polynomial time**).

¹a smart attacker like Mehdi can often exploit the structure of the specific group to do better than this (but even Mehdi can't manage polynomial time)

6 / 40

Quantum revolution

Let G be a finite group, let $g \in G$ and let $x \in \mathbb{Z}$. As before, define g^x by

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto g^x := \underbrace{g * \dots * g}_{x \text{ times}}. \end{aligned}$$

Alice can compute g^x in polynomial time.

7 / 40

Quantum revolution

Let G be a finite group, let $g \in G$ and let $x \in \mathbb{Z}$. As before, define g^x by

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto g^x := \underbrace{g * \dots * g}_{x \text{ times}}. \end{aligned}$$

Alice can compute g^x in polynomial time.

Given a quantum computer, Shor's algorithm computes x from g^x ...also in polynomial time.

7 / 40

Quantum revolution

Let G be a finite group, let $g \in G$ and let $x \in \mathbb{Z}$. As before, define g^x by

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (x, g) &\mapsto g^x := \underbrace{g * \dots * g}_{x \text{ times}}. \end{aligned}$$

Alice can compute g^x in polynomial time.

Given a quantum computer, Shor's algorithm computes x from g^x ...also in polynomial time.

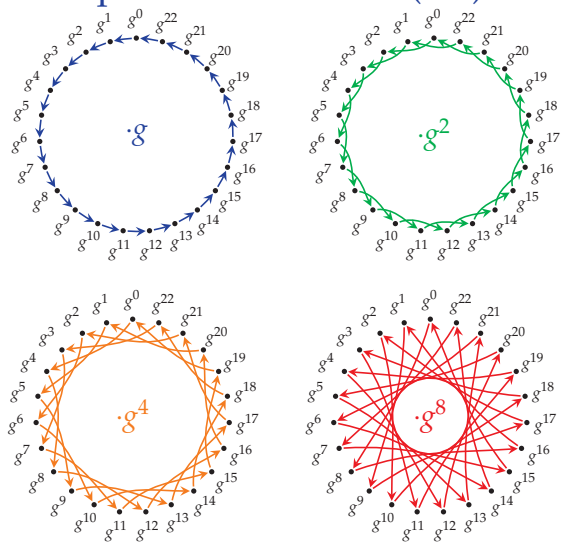
~~ Idea:

Replace the map $\mathbb{Z} \times G \rightarrow G$ by a **group action** of a group H on a **set** S :

$$H \times S \rightarrow S.$$

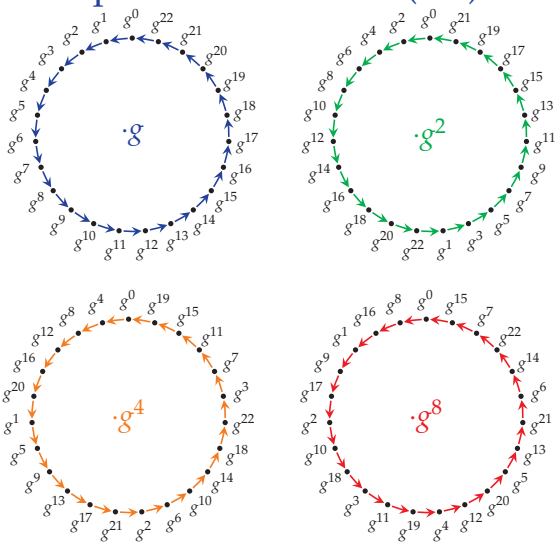
7 / 40

What do we keep from traditional (EC)DH?



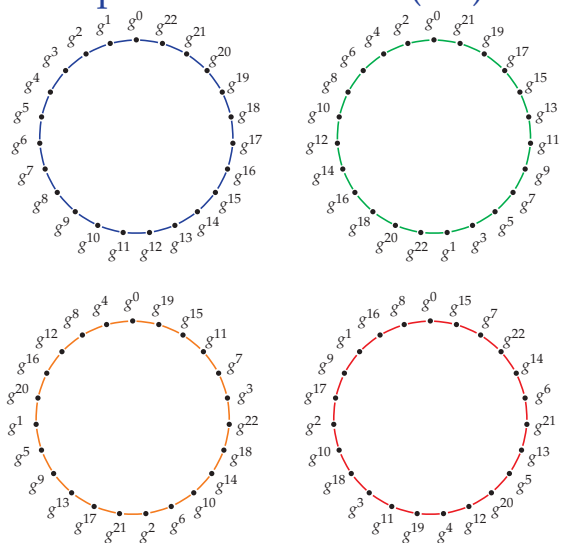
8 / 40

What do we keep from traditional (EC)DH?



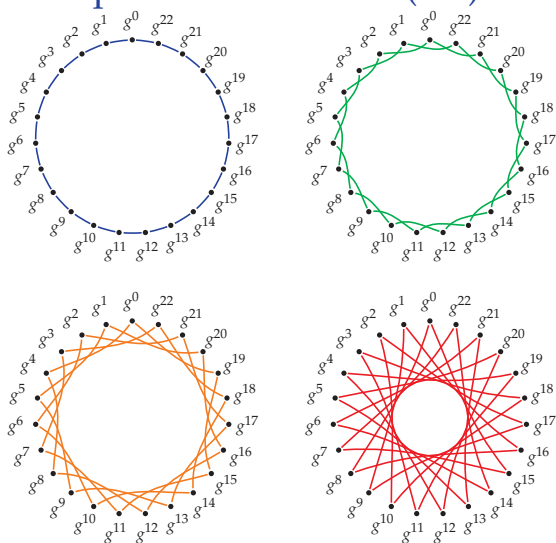
8 / 40

What do we keep from traditional (EC)DH?



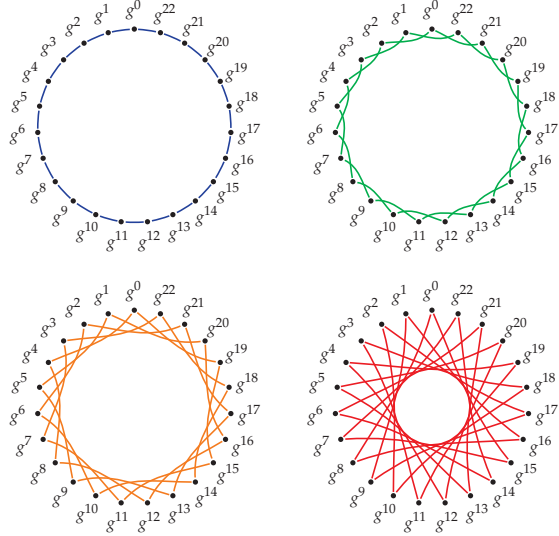
8 / 40

What do we keep from traditional (EC)DH?



8 / 40

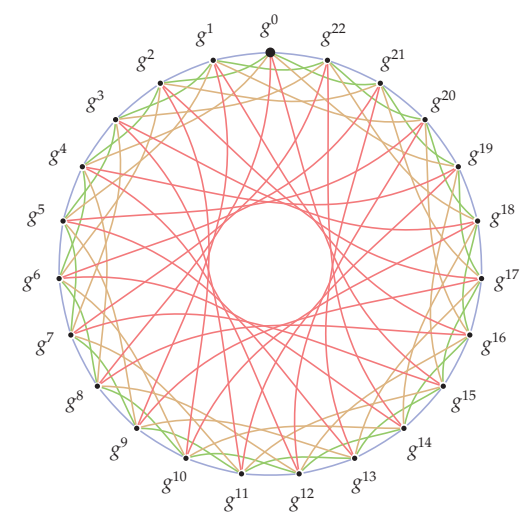
What do we keep from traditional (EC)DH?



Cycles are compatible: [right, then left] = [left, then right], etc.

8 / 40

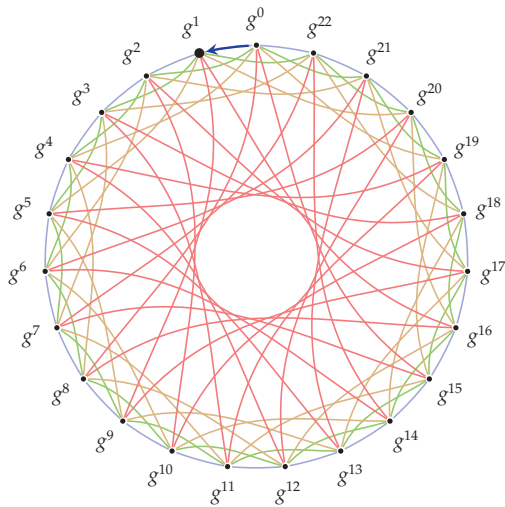
What do we keep from traditional (EC)DH?



Cycles are compatible:
 $g^{13} = g^0$, etc.

9 / 40

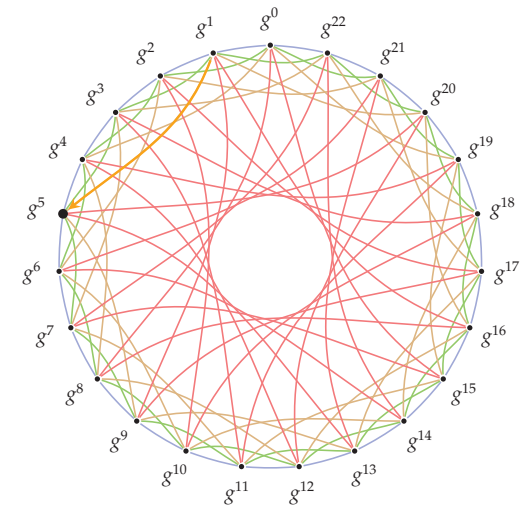
What do we keep from traditional (EC)DH?



Cycles are compatible:
 $g^{13} = g * g^0$, etc.

9 / 40

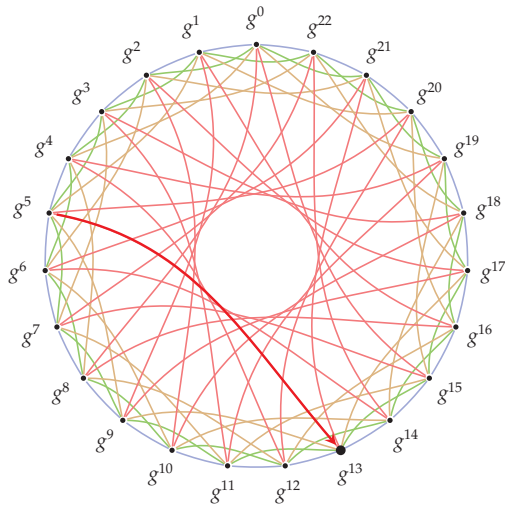
What do we keep from traditional (EC)DH?



Cycles are compatible:
 $g^{13} = g^4 * g * g^0$, etc.

9 / 40

What do we keep from traditional (EC)DH?

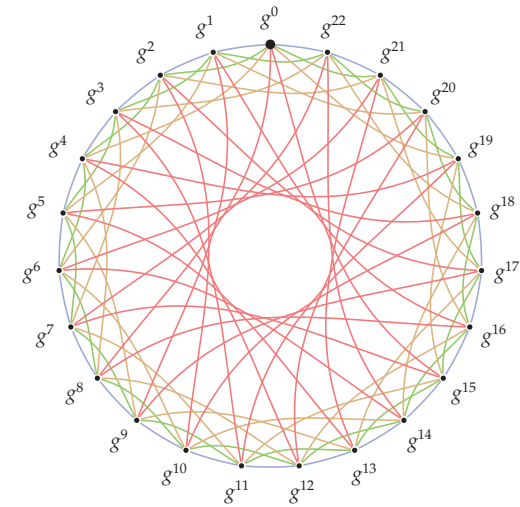


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0, \text{ etc.}$$

9 / 40

What do we keep from traditional (EC)DH?

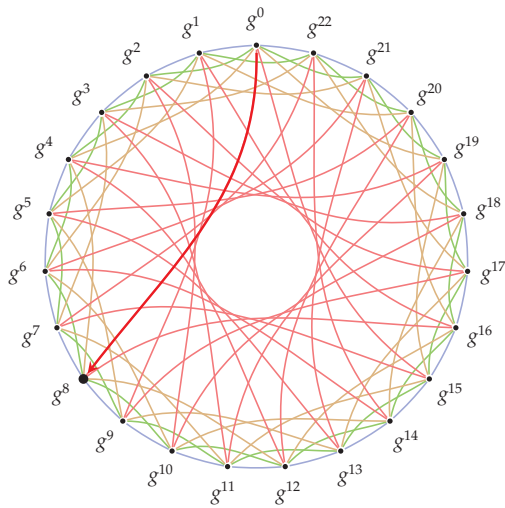


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0 = g^0, \text{ etc.}$$

9 / 40

What do we keep from traditional (EC)DH?

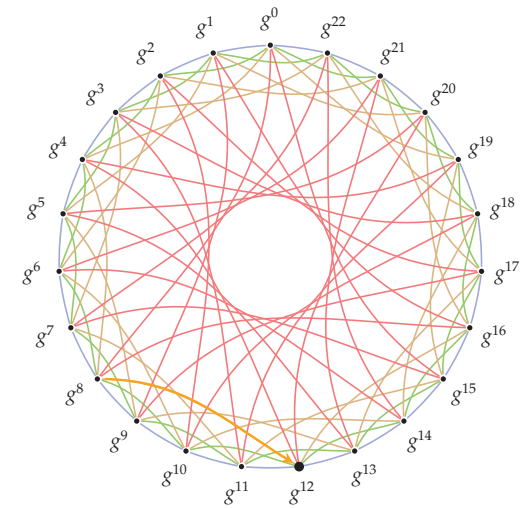


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0 = g^8 * g^0, \text{ etc.}$$

9 / 40

What do we keep from traditional (EC)DH?

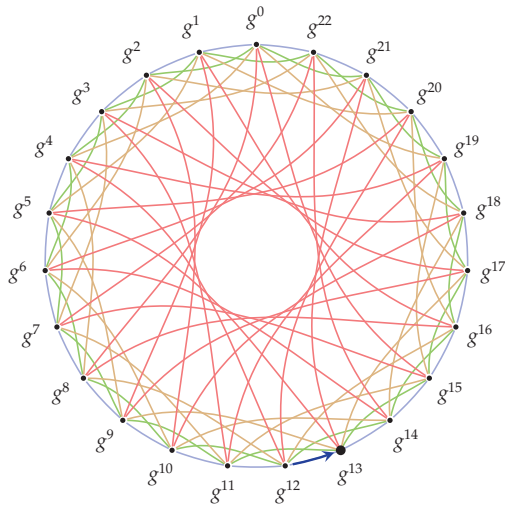


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0 = g^4 * g^8 * g^0, \text{ etc.}$$

9 / 40

What do we keep from traditional (EC)DH?

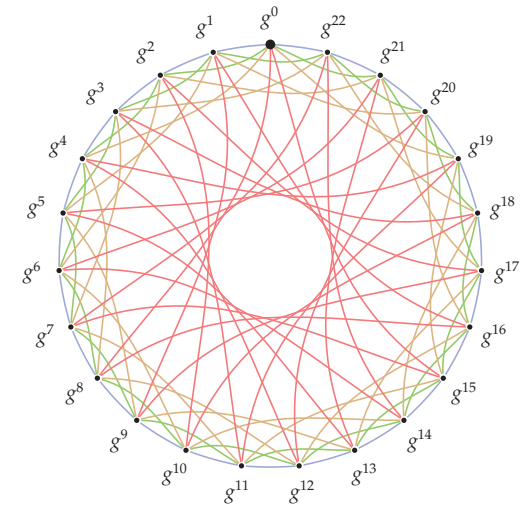


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0, \text{ etc.}$$

9 / 40

What do we keep from traditional (EC)DH?

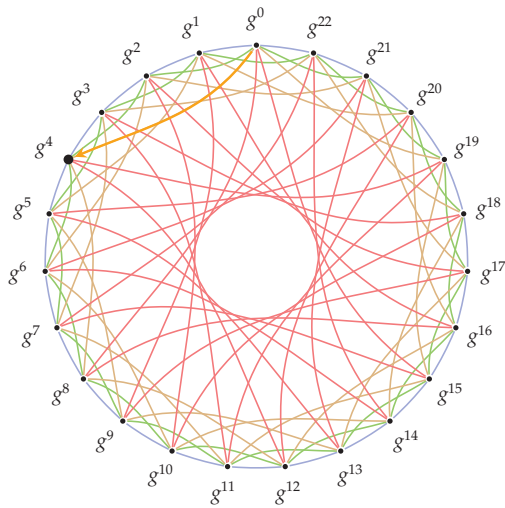


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = g^0, \text{ etc.}$$

9 / 40

What do we keep from traditional (EC)DH?

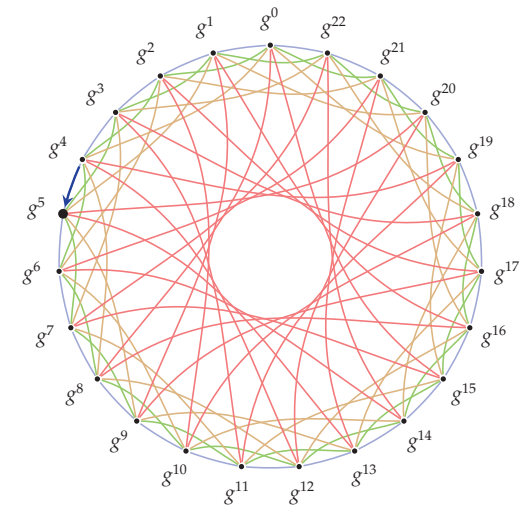


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = g^4 * g^0, \text{ etc.}$$

9 / 40

What do we keep from traditional (EC)DH?

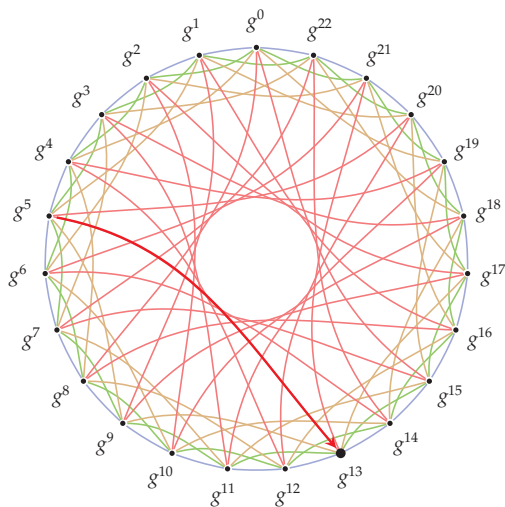


Cycles are compatible:

$$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = g * g^4 * g^0, \text{ etc.}$$

9 / 40

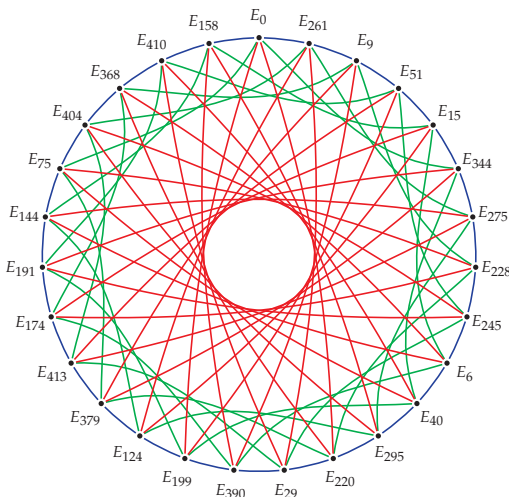
What do we keep from traditional (EC)DH?



Cycles are compatible:
 $g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = g^8 * g * g^4 * g^0$, etc.

9 / 40

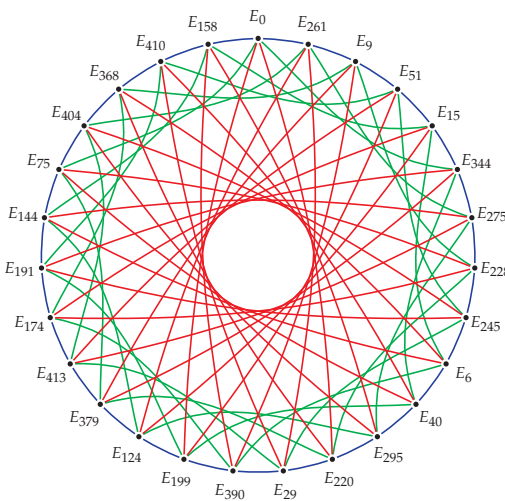
Graphs of elliptic curves



CSIDH: Nodes are now **elliptic curves** and edges are **isogenies**.

10 / 40

Graphs of elliptic curves



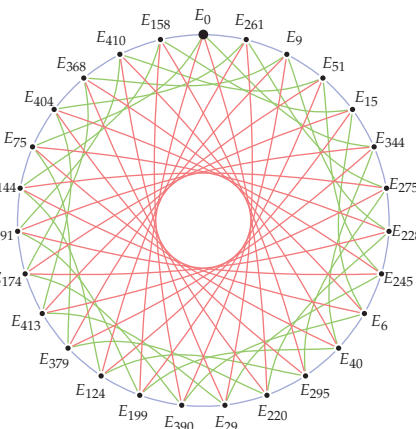
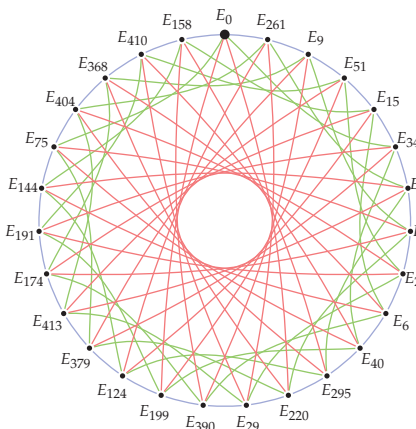
Nodes: Supersingular elliptic curves $E_A: y^2 = x^3 + Ax^2 + x$ over \mathbb{F}_{419} .
 Edges: 3-, 5-, and 7-isogenies (more details to come).

10 / 40

Diffie-Hellman on 'nice' graphs

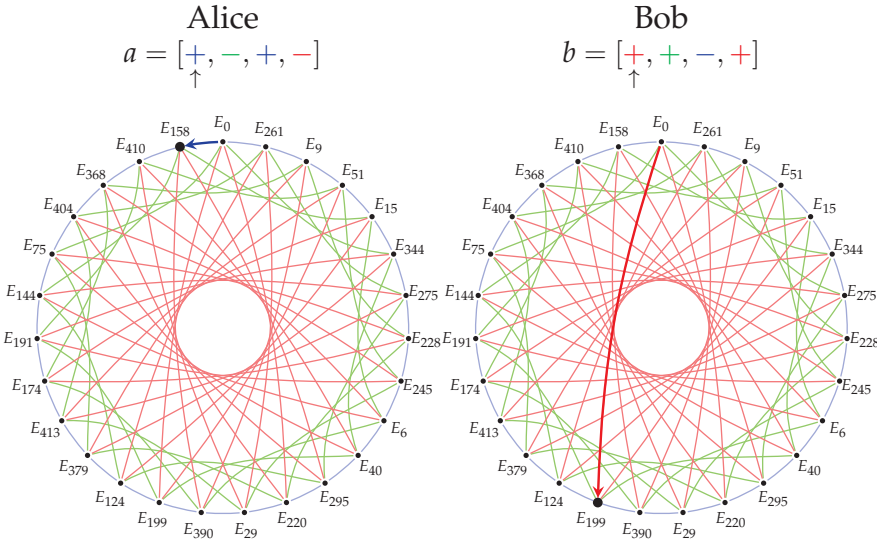
Alice
 $a = [+ , - , + , -]$

Bob
 $b = [+ , + , - , +]$



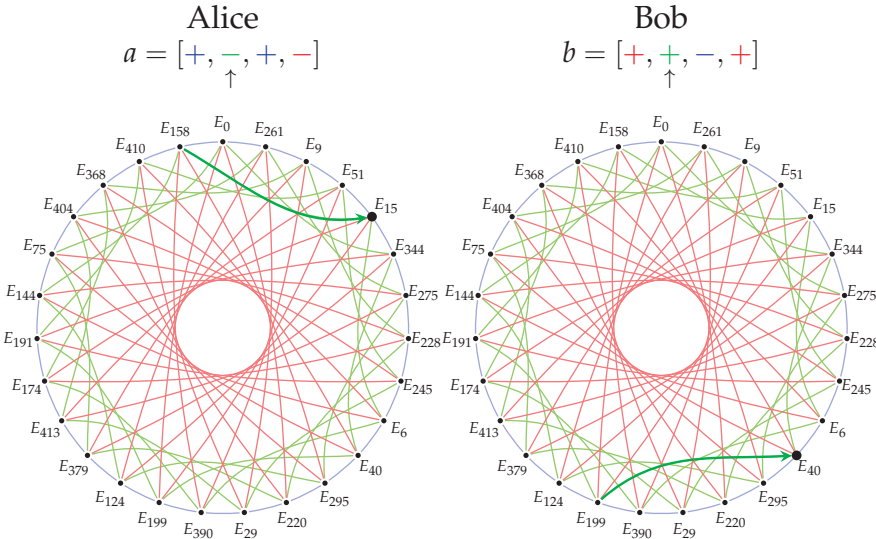
11 / 40

Diffie-Hellman on 'nice' graphs



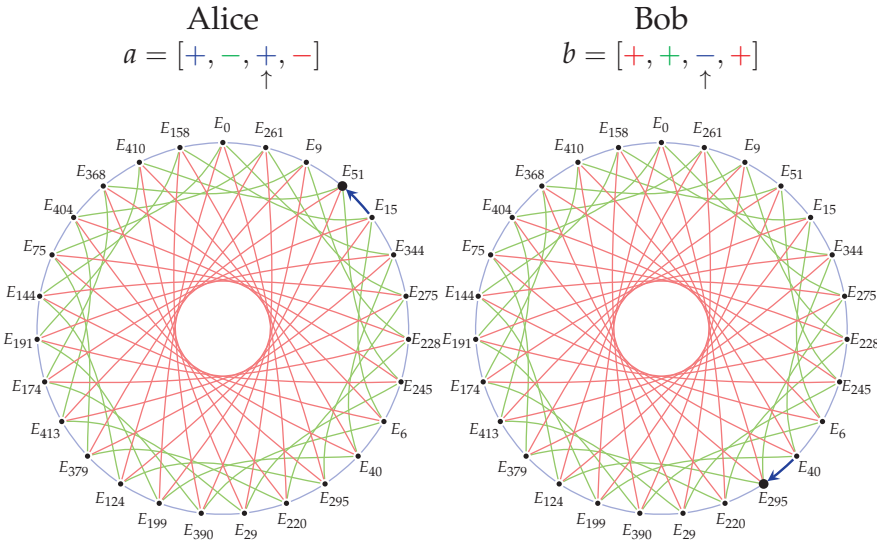
11 / 40

Diffie-Hellman on 'nice' graphs



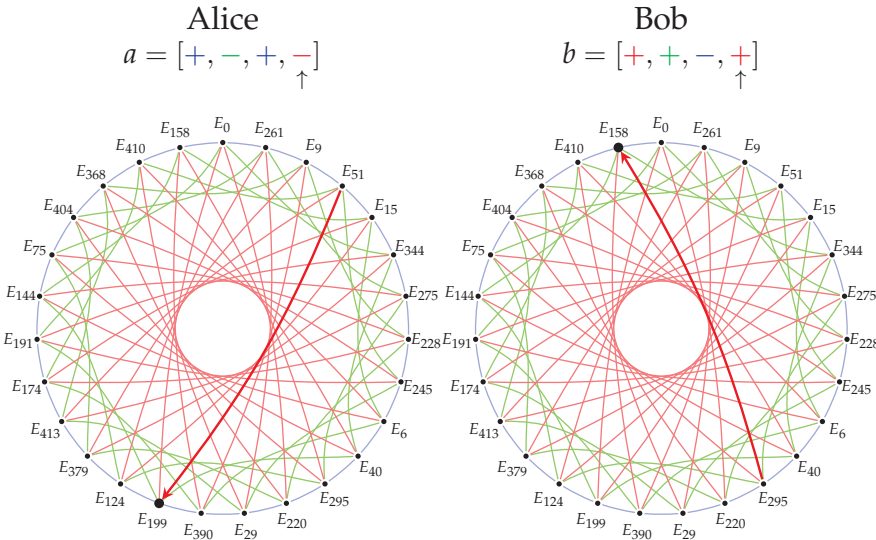
11 / 40

Diffie-Hellman on 'nice' graphs



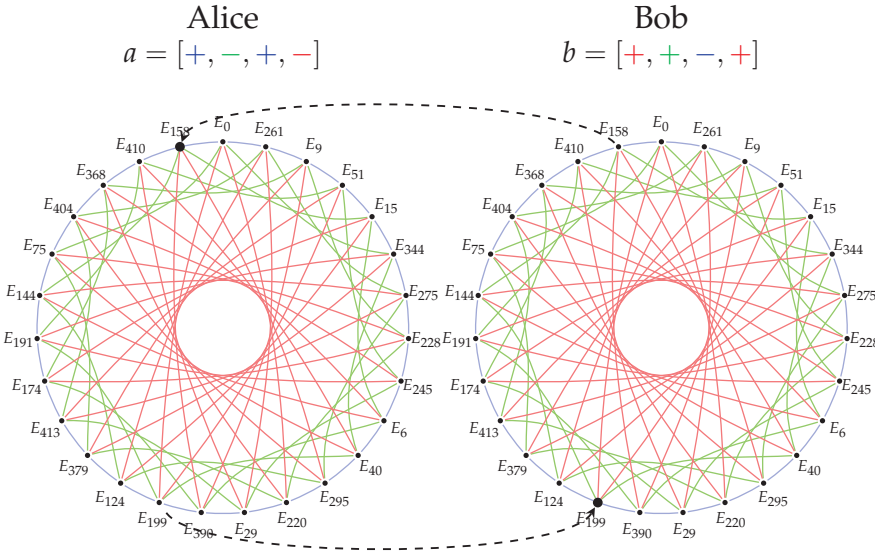
11 / 40

Diffie-Hellman on 'nice' graphs



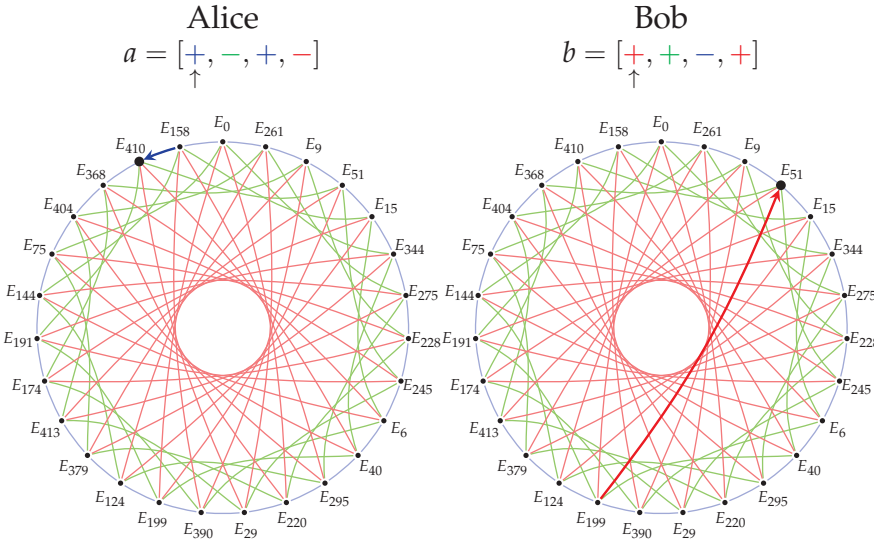
11 / 40

Diffie-Hellman on 'nice' graphs



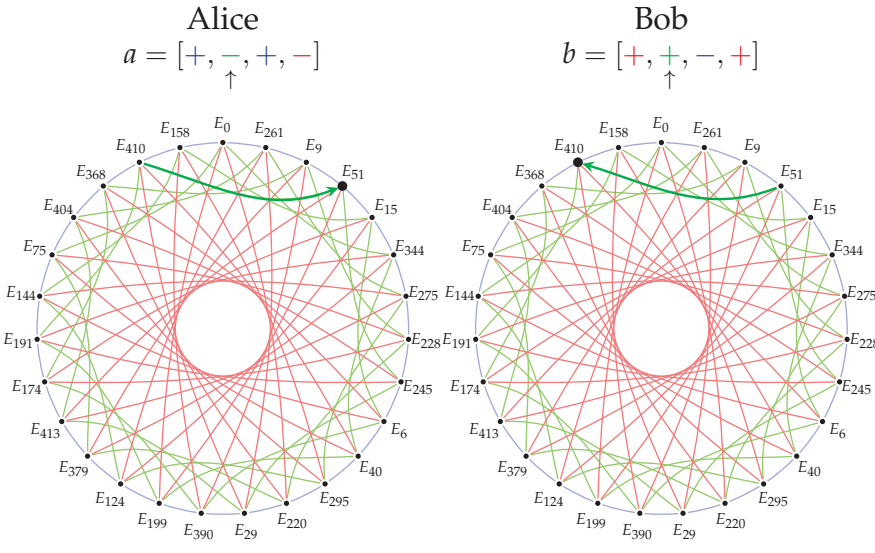
11 / 40

Diffie-Hellman on 'nice' graphs



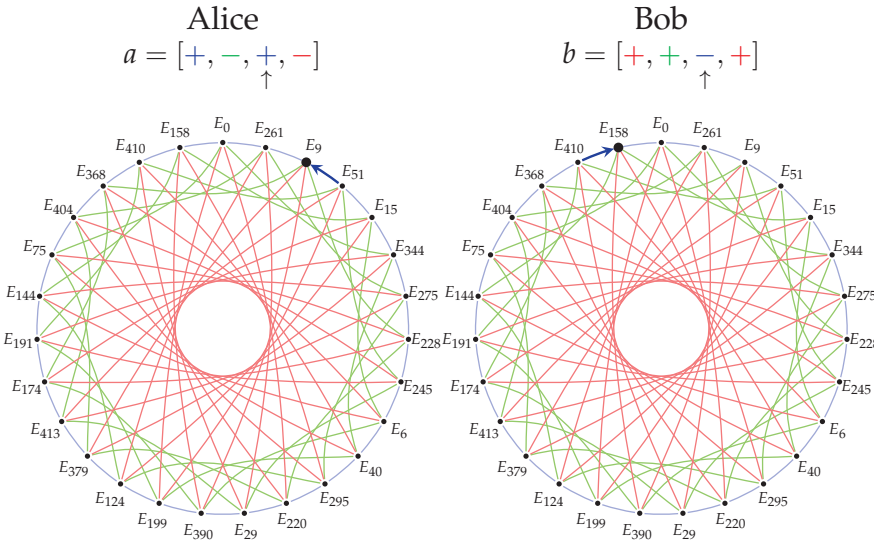
11 / 40

Diffie-Hellman on 'nice' graphs



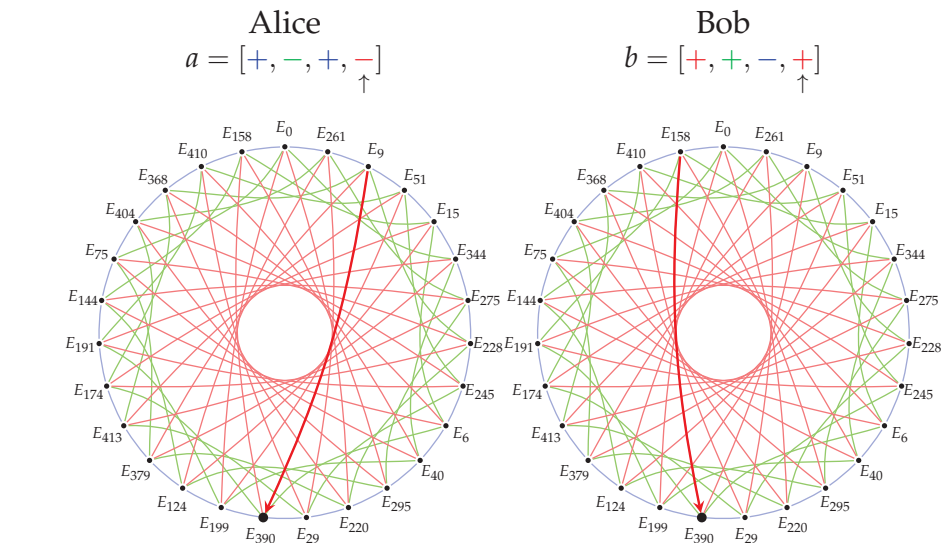
11 / 40

Diffie-Hellman on 'nice' graphs



11 / 40

Diffie-Hellman on 'nice' graphs

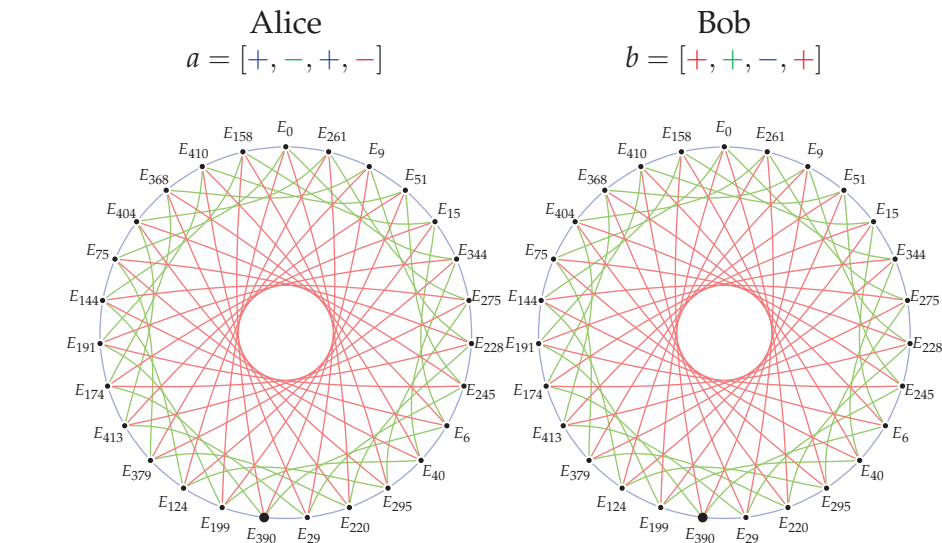


11 / 40

Elliptic curves

Recall from Mehdi's talk:

Diffie-Hellman on 'nice' graphs



11 / 40

Elliptic curves

Recall from Mehdi's talk:

- ▶ Elliptic curves over \mathbb{F}_p can be thought of as curves of the form $E/\mathbb{F}_p : y^2 = f(x)$ with $\deg(f) = 3$ with a 'point at infinity'.

12 / 40

12 / 40

Elliptic curves

Recall from Mehdi's talk:

- ▶ Elliptic curves over \mathbb{F}_p can be thought of as curves of the form $E/\mathbb{F}_p : y^2 = f(x)$ with $\deg(f) = 3$ with a 'point at infinity'.
- ▶ There is a geometric group law called $+$ on the rational points of E .

Elliptic curves

Recall from Mehdi's talk:

- ▶ Elliptic curves over \mathbb{F}_p can be thought of as curves of the form $E/\mathbb{F}_p : y^2 = f(x)$ with $\deg(f) = 3$ with a 'point at infinity'.
- ▶ There is a geometric group law called $+$ on the rational points of E .
- ▶ The point at infinity P_∞ is the identity of the group.

The **group of rational points** on E is

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 : y^2 = f(x)\} \cup \{P_\infty\}.$$

Example

Define $E/\mathbb{F}_5 : y^2 = x^3 + 1$. Then

$$E(\mathbb{F}_5) = \{(0, 1), (0, -1), (2, 3), (2, -3), (-1, 0), P_\infty\}.$$

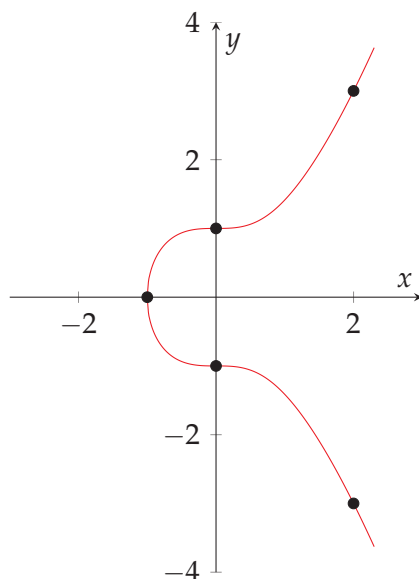
12 / 40

12 / 40

Elliptic curves

- ▶ $E : y^2 = x^3 + 1$.
- ▶ Recall

$$E(\mathbb{F}_5) = \{(2, 3), (0, -1), (-1, 0), (0, 1), (2, -3), P_\infty\}.$$

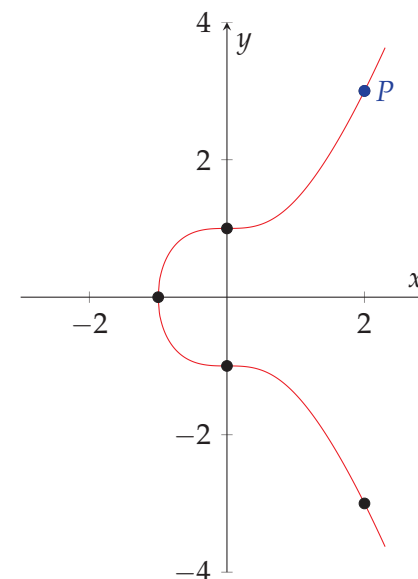


13 / 40

Elliptic curves

- ▶ $E : y^2 = x^3 + 1$.
- ▶ Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), (-1, 0), (0, 1), (2, -3), P_\infty\} \\ &= \{P \end{aligned}$$



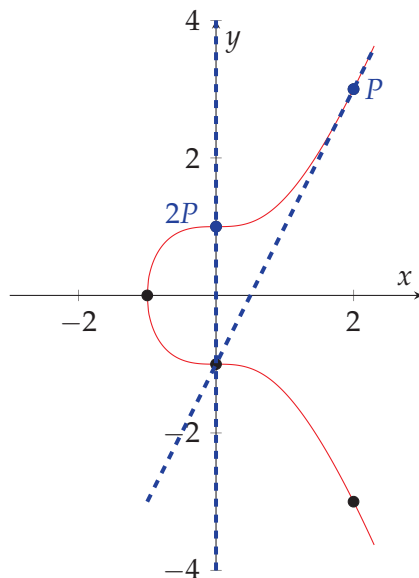
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \end{aligned}$$



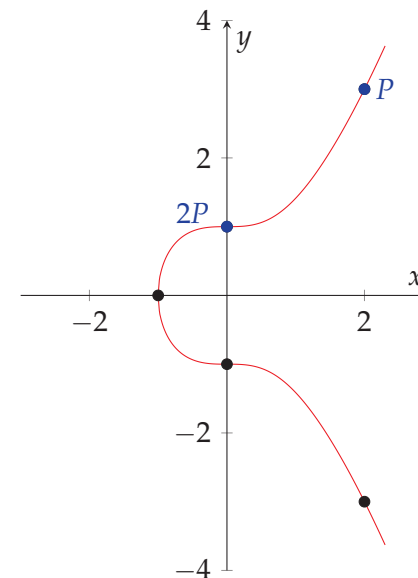
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \end{aligned}$$



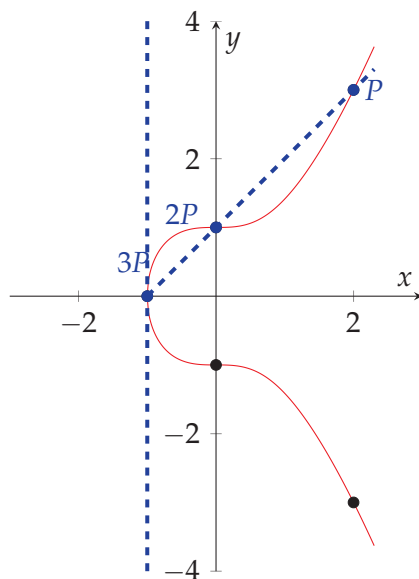
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, \end{aligned}$$



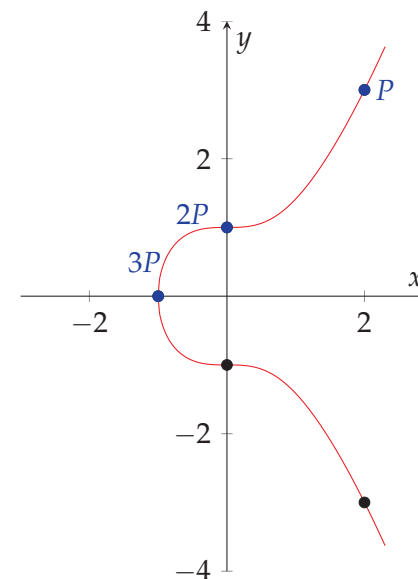
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, \end{aligned}$$



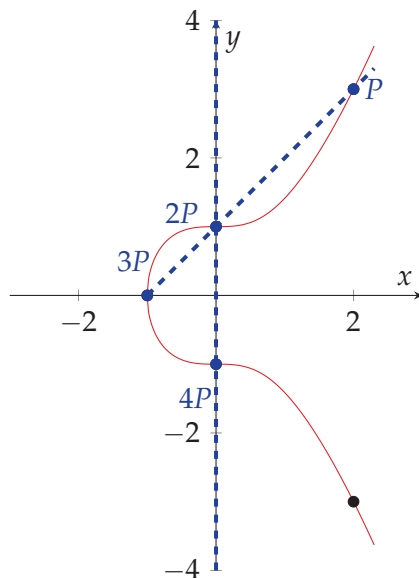
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, 4P, \end{aligned}$$



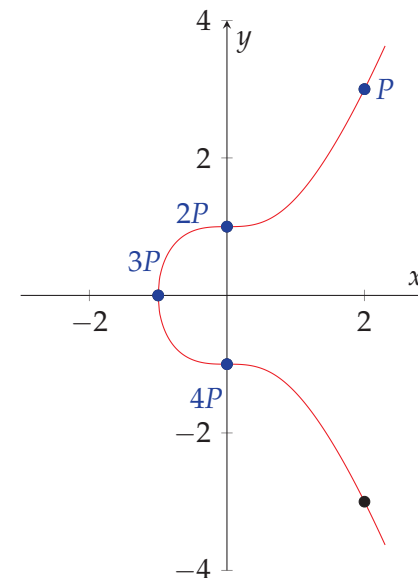
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, 4P, \end{aligned}$$



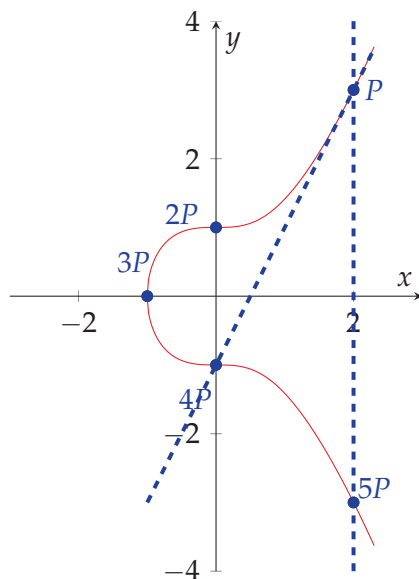
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, 4P, \\ &\quad 5P, \end{aligned}$$



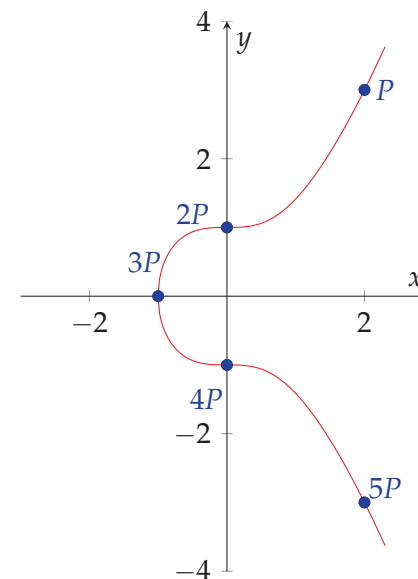
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1.$

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, 4P, \\ &\quad 5P, \end{aligned}$$



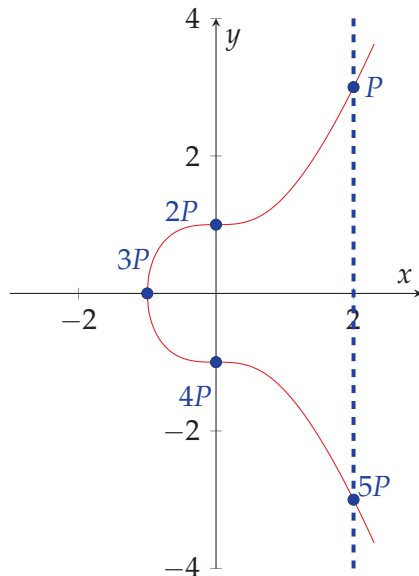
13 / 40

Elliptic curves

► $E : y^2 = x^3 + 1$.

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, 4P, \\ &\quad 5P, 6P\}. \end{aligned}$$



13 / 40

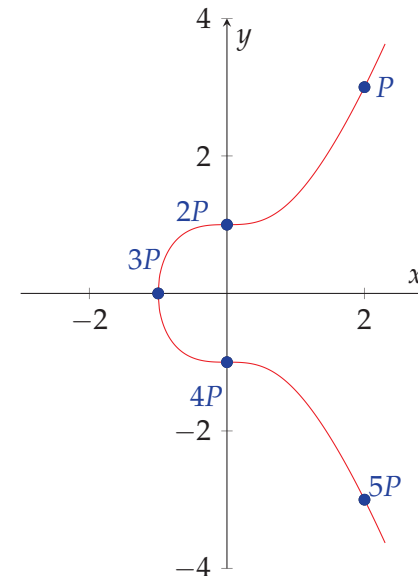
Elliptic curves

► $E : y^2 = x^3 + 1$.

► Recall

$$\begin{aligned} E(\mathbb{F}_5) &= \{(2, 3), (0, -1), \\ &\quad (-1, 0), (0, 1), \\ &\quad (2, -3), P_\infty\}. \\ &= \{P, 2P, \\ &\quad 3P, 4P, \\ &\quad 5P, 6P\}. \end{aligned}$$

► $E(\mathbb{F}_5)$ is **cyclic** –
 $E(\mathbb{F}_5) \cong C_6$.



13 / 40

Elliptic curves

Example

$E/\mathbb{F}_5 : y^2 = x^3 + 1$, then $E(\mathbb{F}_5) \cong C_6$.

Example

$E/\mathbb{F}_5 : y^2 = x^3 + 1$, then $E(\mathbb{F}_5) \cong C_6$.

Definition

An elliptic curve E defined over a finite prime field \mathbb{F}_p with $p \geq 5$ is **supersingular** if $\#E(\mathbb{F}_p) = p + 1$.

14 / 40

14 / 40

Elliptic curves

Example

$E/\mathbb{F}_5 : y^2 = x^3 + 1$, then $E(\mathbb{F}_5) \cong C_6$.

Definition

An elliptic curve E defined over a finite prime field \mathbb{F}_p with $p \geq 5$ is **supersingular** if $\#E(\mathbb{F}_p) = p + 1$.

Theorem

If E/\mathbb{F}_p is supersingular and $p \geq 5$ then

$$E(\mathbb{F}_p) \cong C_{p+1} \quad \text{or} \quad E(\mathbb{F}_p) \cong C_2 \times C_{(p+1)/2}.$$

14 / 40

Elliptic curves

Definition

A point $P \in E(\mathbb{F}_p)$ is called a **n -torsion point** if $nP = P_\infty$. An n -torsion point P is a **point of order n** if there is no positive $m < n$ such that $mP = P_\infty$.

Example

$E/\mathbb{F}_5 : y^2 = x^3 + 1$. Then $E(\mathbb{F}_p) \cong C_6$ and is generated by $P = (2, 3)$.

15 / 40

Elliptic curves

Definition

A point $P \in E(\mathbb{F}_p)$ is called a **n -torsion point** if $nP = P_\infty$.

Definition

A point $P \in E(\mathbb{F}_p)$ is called a **n -torsion point** if $nP = P_\infty$. An n -torsion point P is a **point of order n** if there is no positive $m < n$ such that $mP = P_\infty$.

Example

$E/\mathbb{F}_5 : y^2 = x^3 + 1$. Then $E(\mathbb{F}_p) \cong C_6$ and is generated by $P = (2, 3)$.

- $(2, 3)$ is a 6-torsion point of order 6.

15 / 40

Elliptic curves

15 / 40

Elliptic curves

Definition

A point $P \in E(\mathbb{F}_p)$ is called a *n -torsion point* if $nP = P_\infty$. An n -torsion point P is a *point of order n* if there is no positive $m < n$ such that $mP = P_\infty$.

Example

$E/\mathbb{F}_5 : y^2 = x^3 + 1$. Then $E(\mathbb{F}_p) \cong C_6$ and is generated by $P = (2, 3)$.

- ▶ $(2, 3)$ is a 6-torsion point of order 6.
- ▶ $(-1, 0) = 3(2, 3)$ is a 6-torsion point and a 2-torsion point, and has order 2.

15 / 40

Elliptic curves

Definition

A point $P \in E(\mathbb{F}_p)$ is called a *n -torsion point* if $nP = P_\infty$. An n -torsion point P is a *point of order n* if there is no positive $m < n$ such that $mP = P_\infty$.

Example

E/\mathbb{F}_p supersingular and $p \geq 5$.
Then either

15 / 40

Elliptic curves

Definition

A point $P \in E(\mathbb{F}_p)$ is called a *n -torsion point* if $nP = P_\infty$. An n -torsion point P is a *point of order n* if there is no positive $m < n$ such that $mP = P_\infty$.

Example

E/\mathbb{F}_p supersingular and $p \geq 5$.
Then either

- ▶ $E(\mathbb{F}_p) \cong C_{p+1}$; generated by a point P of order $p + 1$, or

15 / 40

Elliptic curves

Definition

A point $P \in E(\mathbb{F}_p)$ is called a *n -torsion point* if $nP = P_\infty$. An n -torsion point P is a *point of order n* if there is no positive $m < n$ such that $mP = P_\infty$.

Example

E/\mathbb{F}_p supersingular and $p \geq 5$.
Then either

- ▶ $E(\mathbb{F}_p) \cong C_{p+1}$; generated by a point P of order $p + 1$, or
- ▶ $E(\mathbb{F}_p) \cong C_2 \times C_{(p+1)/2}$ and contains a point P of order $(p + 1)/2$.

15 / 40

Elliptic curves

Definition

A point $P \in E(\mathbb{F}_p)$ is called a **n -torsion point** if $nP = P_\infty$. An n -torsion point P is a **point of order n** if there is no positive $m < n$ such that $mP = P_\infty$.

Example

E/\mathbb{F}_p supersingular and $p \geq 5$.

Then either

- ▶ $E(\mathbb{F}_p) \cong C_{p+1}$; generated by a point P of order $p+1$, or
- ▶ $E(\mathbb{F}_p) \cong C_2 \times C_{(p+1)/2}$ and contains a point P of order $(p+1)/2$.

In either case, if $\ell \mid (p+1)$ is an odd prime, then $\frac{p+1}{\ell}P$ is a point of order ℓ .

15 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero morphism $E \rightarrow E'$ that maps the group identity of E to the group identity of E' . It is given by rational maps.

16 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero morphism $E \rightarrow E'$ that maps the group identity of E to the group identity of E' . It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$[2] : \begin{array}{ccc} E_{51} & \rightarrow & E_{51} \\ (x, y) & \mapsto & 2 \cdot (x, y) := (x, y) + (x, y) \end{array}$$

16 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero **morphism** $E \rightarrow E'$ that maps the group identity of E to the group identity of E' . It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$[2] : \begin{array}{ccc} E_{51} & \rightarrow & E_{51} \\ (x, y) & \mapsto & 2 \cdot (x, y) := (x, y) + (x, y) \end{array}$$

- ▶ As $[2]$ is a morphism, it induces a morphism of groups $E(\mathbb{F}_{419}) \rightarrow E(\mathbb{F}_{419})$, i.e. $[2](P + Q) = [2](P) + [2](Q)$.

16 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero morphism $E \rightarrow E'$ that maps the group identity of E to the group identity of E' . It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$[2] : \begin{array}{ccc} E_{51} & \rightarrow & E_{51} \\ (x, y) & \mapsto & 2 \cdot (x, y) := (x, y) + (x, y) \end{array}$$

17 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero morphism $E \rightarrow E'$ that **maps the group identity of E to the group identity of E'** . It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$[2] : \begin{array}{ccc} E_{51} & \rightarrow & E_{51} \\ (x, y) & \mapsto & 2 \cdot (x, y) := (x, y) + (x, y) \end{array}$$

$$\blacktriangleright [2](P_\infty) = P_\infty + P_\infty = P_\infty.$$

17 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero morphism $E \rightarrow E'$ that **maps the group identity of E to the group identity of E'** . It is given by rational maps.

Example

Define $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$[2] : \begin{array}{ccc} E_{51} & \rightarrow & E_{51} \\ (x, y) & \mapsto & 2 \cdot (x, y) := (x, y) + (x, y) \end{array}$$

- $\blacktriangleright [2](P_\infty) = P_\infty + P_\infty = P_\infty$. So $[2]$ maps the group identity of E_{51} to the group identity of E_{51} .

17 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero morphism $E \rightarrow E'$ that maps the group identity of E to the group identity of E' . It is given by **rational maps**.

Example

- \blacktriangleright **Exercise:** show that

$$[2] : \begin{array}{ccc} E_{51} & \rightarrow & E_{51} \\ (x, y) & \mapsto & \left(\frac{\frac{1}{2}x^4 - 18x^3 - 163x^2 - 18x + \frac{1}{2}}{8x(x^2 + 9x + 1)}, \frac{y(x^6 + 18x^5 + 5x^4 - 5x^2 - 18x - 1)}{(8x(x^2 + 9x + 1))^2} \right) \end{array}$$

Hint: Try to compute the rational maps using the group law from Mehdi's talk or see David's talk to learn how to compute the rational maps with Sage.

18 / 40

Elliptic curves and isogenies

Definition

An **isogeny** of elliptic curves over \mathbb{F}_p is a non-zero morphism $E \rightarrow E'$ that maps the group identity of E to the group identity of E' . It is given by rational maps.

Example

Fact: let $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$ and $E_9/\mathbb{F}_{419} : y^2 = x^3 + 9x^2 + x$ be elliptic curves. Then

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

is an isogeny.

19 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

20 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

The **kernel** $\ker(f)$ is the set of points (x, y) that map to the group identity P_∞ :

- If $(x, y) \in \ker(f)$ then $(x, y) = P_\infty$ or $x = -118$.

20 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

The **kernel** $\ker(f)$ is the set of points (x, y) that map to the group identity P_∞ :

- If $(x, y) \in \ker(f)$ then $(x, y) = P_\infty$ or $x = -118$.
- If $(-118, y) \in E_{51}$ then $(x, y) = (-118, \pm 51)$.

20 / 40

Elliptic curves and isogenies

Example

$$\begin{aligned} f : E_{51} &\rightarrow E_9 \\ (x, y) &\mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ &\quad \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right). \end{aligned}$$

The **kernel** $\ker(f)$ is the set of points (x, y) that map to the group identity P_∞ :

- If $(x, y) \in \ker(f)$ then $(x, y) = P_\infty$ or $x = -118$.
- If $(-118, y) \in E_{51}$ then $(x, y) = (-118, \pm 51)$.
- $f(P_\infty) = f((-118, \pm 51)) = P_\infty$.

Fact: an isogeny is uniquely determined by its kernel.

20 / 40

Elliptic curves and isogenies

Example

$$\begin{aligned} f : E_{51} &\rightarrow E_9 \\ (x, y) &\mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ &\quad \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right). \end{aligned}$$

21 / 40

Elliptic curves and isogenies

Example

$$\begin{aligned} f : E_{51} &\rightarrow E_9 \\ (x, y) &\mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ &\quad \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right). \end{aligned}$$

- $\ker(f) = \{(-118, 51), (-118, -51), P_\infty\}$.

21 / 40

Elliptic curves and isogenies

Example

$$\begin{aligned} f : E_{51} &\rightarrow E_9 \\ (x, y) &\mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ &\quad \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right). \end{aligned}$$

- $\ker(f) = \{(-118, 51), (-118, -51), P_\infty\}$.
- $\ker(f)$ is a subgroup of $E_{51}(\overline{\mathbb{F}_{419}})$ (because f induces a morphism of groups).

21 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

- $\ker(f) = \{(-118, 51), (-118, -51), P_\infty\}$.
- $\ker(f)$ is a subgroup of $E_{51}(\overline{\mathbb{F}_{419}})$ (because f induces a morphism of groups).
- $\ker(f)$ is order 3, so must be a cyclic group, hence $(-118, 51) + (-118, 51) + (-118, 51) = P_\infty$.

21 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

22 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

- $\ker(f)$ is a cyclic subgroup of $E_{51}(\mathbb{F}_{419})$, generated by a 3-torsion point $P = (-118, 51)$.

22 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9 \\ (x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \\ \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

- $\ker(f)$ is a cyclic subgroup of $E_{51}(\mathbb{F}_{419})$, generated by a 3-torsion point $P = (-118, 51)$.
- $Q = (210, \sqrt{380}) \in E(\mathbb{F}_{419^2})$ is also a point of order 3.

22 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9$$

$$(x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

- ▶ $\ker(f)$ is a cyclic subgroup of $E_{51}(\mathbb{F}_{419})$, generated by a 3-torsion point $P = (-118, 51)$.
- ▶ $Q = (210, \sqrt{380}) \in E(\mathbb{F}_{419^2})$ is also a point of order 3.
- ▶ Then $f(Q) = (286, 107\sqrt{380})$ is a point of order 3 on E_9 .

22 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9$$

$$(x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

- ▶ $\ker(f)$ is a cyclic subgroup of $E_{51}(\mathbb{F}_{419})$, generated by a 3-torsion point $P = (-118, 51)$.
- ▶ $Q = (210, \sqrt{380}) \in E(\mathbb{F}_{419^2})$ is also a point of order 3.
- ▶ Then $f(Q) = (286, 107\sqrt{380})$ is a point of order 3 on E_9 .
- ▶ There is another 3-isogeny $g : E_9 \rightarrow E_{51}$ with cyclic kernel generated by $f(Q)$.

22 / 40

Elliptic curves and isogenies

Example

$$f : E_{51} \rightarrow E_9$$

$$(x, y) \mapsto \left(\frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right).$$

- ▶ $\ker(f)$ is a cyclic subgroup of $E_{51}(\mathbb{F}_{419})$, generated by a 3-torsion point $P = (-118, 51)$.
- ▶ $Q = (210, \sqrt{380}) \in E(\mathbb{F}_{419^2})$ is also a point of order 3.
- ▶ Then $f(Q) = (286, 107\sqrt{380})$ is a point of order 3 on E_9 .
- ▶ There is another 3-isogeny $g : E_9 \rightarrow E_{51}$ with cyclic kernel generated by $f(Q)$.
- ▶ $g \circ f : E_{51} \rightarrow E_{51}$ is the multiplication-by-3 map.

22 / 40

Elliptic curves and isogenies

Definition

Let $E, E'/\mathbb{F}_p$ be elliptic curves and let ℓ be a prime different from p . An ℓ -isogeny $f : E \rightarrow E'$ is an isogeny with $\#\ker(f) = \ell$.

Definition

Let E/\mathbb{F}_p be an elliptic curve and let $\ell \neq p$ be prime. Let $f : E \rightarrow E'$ be an ℓ -isogeny.

23 / 40

Elliptic curves and isogenies

Definition

Let $E, E'/\mathbb{F}_p$ be elliptic curves and let ℓ be a prime different from p . An ℓ -isogeny $f : E \rightarrow E'$ is an isogeny with $\# \ker(f) = \ell$.

Definition

Let E/\mathbb{F}_p be an elliptic curve and let $\ell \neq p$ be prime. Let $f : E \rightarrow E'$ be an ℓ -isogeny. Then there exists a unique (up to isomorphism) ℓ -isogeny $f^\vee : E' \rightarrow E$ such that $f^\vee \circ f$ is the multiplication-by- ℓ map on E .

23 / 40

Elliptic curves and isogenies

Definition

Let $E, E'/\mathbb{F}_p$ be elliptic curves and let ℓ be a prime different from p . An ℓ -isogeny $f : E \rightarrow E'$ is an isogeny with $\# \ker(f) = \ell$.

Definition

Let E/\mathbb{F}_p be an elliptic curve and let $\ell \neq p$ be prime. Let $f : E \rightarrow E'$ be an ℓ -isogeny. Then there exists a unique (up to isomorphism) ℓ -isogeny $f^\vee : E' \rightarrow E$ such that $f^\vee \circ f$ is the multiplication-by- ℓ map on E . This is called the **dual isogeny**.

Example

$E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$ and $E_9/\mathbb{F}_{419} : y^2 = x^3 + 9x^2 + x$.

23 / 40

Elliptic curves and isogenies

Definition

Let $E, E'/\mathbb{F}_p$ be elliptic curves and let ℓ be a prime different from p . An ℓ -isogeny $f : E \rightarrow E'$ is an isogeny with $\# \ker(f) = \ell$.

Definition

Let E/\mathbb{F}_p be an elliptic curve and let $\ell \neq p$ be prime. Let $f : E \rightarrow E'$ be an ℓ -isogeny. Then there exists a unique (up to isomorphism) ℓ -isogeny $f^\vee : E' \rightarrow E$ such that $f^\vee \circ f$ is the multiplication-by- ℓ map on E . This is called the **dual isogeny**.

Example

$E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$ and $E_9/\mathbb{F}_{419} : y^2 = x^3 + 9x^2 + x$.

The dual of the 3-isogeny $f : E_{51} \rightarrow E_9$ with kernel generated by $(-118, 51)$ is the 3-isogeny $f^\vee : E_9 \rightarrow E_{51}$ with kernel generated by $(286, 107\sqrt{380})$.

23 / 40

Isogeny graphs

Graph of 3-isogenies over \mathbb{F}_{419} .

Example

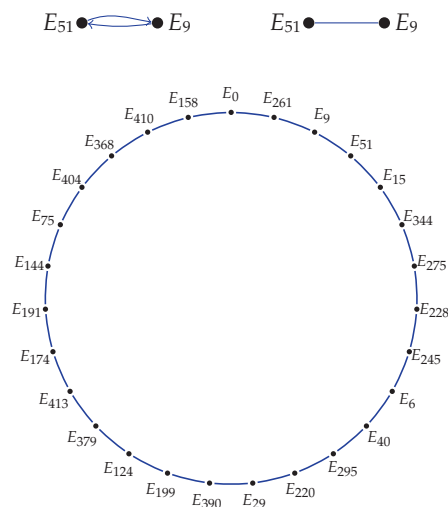


24 / 40

Isogeny graphs

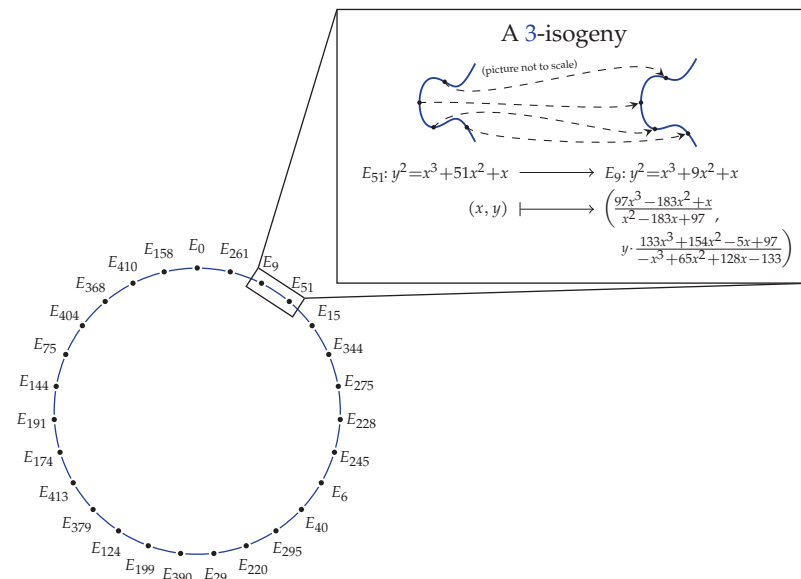
Graph of 3-isogenies over \mathbb{F}_{419} .

Example



24 / 40

Isogeny graphs



25 / 40

Isogeny graphs

Definition

Let p and ℓ be distinct primes. The **isogeny graph** G_ℓ over \mathbb{F}_p has

- Nodes: elliptic curves defined over \mathbb{F}_p with a given number of points (up to \mathbb{F}_p -isomorphism).
- Edges: an edge $E - E'$ represents an ℓ -isogeny $E \rightarrow E'$ defined over \mathbb{F}_p together with its dual isogeny.

Isogeny graphs

Definition

Let p and ℓ be distinct primes. The **isogeny graph** G_ℓ over \mathbb{F}_p has

- Nodes: elliptic curves defined over \mathbb{F}_p with a given number of points (up to \mathbb{F}_p -isomorphism).
- Edges: an edge $E - E'$ represents an ℓ -isogeny $E \rightarrow E'$ defined over \mathbb{F}_p together with its dual isogeny.

- In our example



26 / 40

26 / 40

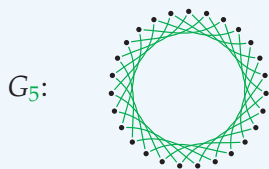
Isogeny graphs

Definition

Let p and ℓ be distinct primes. The **isogeny graph** G_ℓ over \mathbb{F}_p has

- Nodes: elliptic curves defined over \mathbb{F}_p with a given number of points (up to \mathbb{F}_p -isomorphism).
- Edges: an edge $E - E'$ represents an ℓ -isogeny $E \rightarrow E'$ defined over \mathbb{F}_p together with its dual isogeny.

► In our example



26 / 40

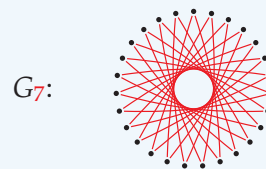
Isogeny graphs

Definition

Let p and ℓ be distinct primes. The **isogeny graph** G_ℓ over \mathbb{F}_p has

- Nodes: elliptic curves defined over \mathbb{F}_p with a given number of points (up to \mathbb{F}_p -isomorphism).
- Edges: an edge $E - E'$ represents an ℓ -isogeny $E \rightarrow E'$ defined over \mathbb{F}_p together with its dual isogeny.

► In our example



26 / 40

Isogeny graphs

Definition

Let p and ℓ be distinct primes. The **isogeny graph** G_ℓ over \mathbb{F}_p has

- Nodes: elliptic curves defined over \mathbb{F}_p with a given number of points (up to \mathbb{F}_p -isomorphism).
- Edges: an edge $E - E'$ represents an ℓ -isogeny $E \rightarrow E'$ defined over \mathbb{F}_p together with its dual isogeny.

► In our example



26 / 40

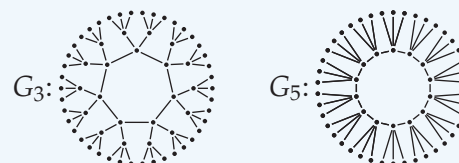
Isogeny graphs

Definition

Let p and ℓ be distinct primes. The **isogeny graph** G_ℓ over \mathbb{F}_p has

- Nodes: elliptic curves defined over \mathbb{F}_p with a given number of points (up to \mathbb{F}_p -isomorphism).
- Edges: an edge $E - E'$ represents an ℓ -isogeny $E \rightarrow E'$ defined over \mathbb{F}_p together with its dual isogeny.

► Generally, the G_ℓ look something like



26 / 40

Endomorphisms

- Our graphs are cycles because all the curves have ‘the same endomorphisms’

Endomorphisms

- Our graphs are cycles because all the curves have ‘the same endomorphisms’

Definition

An **endomorphism** of an elliptic curve E is a morphism $E \rightarrow E$.

27 / 40

27 / 40

Endomorphisms

- Our graphs are cycles because all the curves have ‘the same endomorphisms’

Definition

An **endomorphism** of an elliptic curve E is a morphism $E \rightarrow E$.

Example

- For any $n \in \mathbb{Z}$, the map

$$\begin{aligned} [n] : E &\rightarrow E \\ (x, y) &\mapsto n(x, y). \end{aligned}$$

Endomorphisms

- Our graphs are cycles because all the curves have ‘the same endomorphisms’

Definition

An **endomorphism** of an elliptic curve E is a morphism $E \rightarrow E$.

Example

- For any $n \in \mathbb{Z}$, the map

$$\begin{aligned} [n] : E &\rightarrow E \\ (x, y) &\mapsto n(x, y). \end{aligned}$$

- For E/\mathbb{F}_p , the Frobenius map

$$\begin{aligned} \pi : E &\rightarrow E \\ (x, y) &\mapsto (x^p, y^p). \end{aligned}$$

27 / 40

27 / 40

Endomorphism rings

Let E/\mathbb{F}_p be supersingular.

- ▶ Applying the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ twice results in the multiplication by $-p$ map $[-p]$.

28 / 40

Endomorphism rings

Let E/\mathbb{F}_p be supersingular.

- ▶ Applying the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ twice results in the multiplication by $-p$ map $[-p]$.
- ▶ The set of \mathbb{F}_p -rational endomorphisms of a curve E/\mathbb{F}_p forms a [ring](#) $\text{End}_{\mathbb{F}_p}(E)$.

28 / 40

Endomorphism rings

Let E/\mathbb{F}_p be supersingular.

- ▶ Applying the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ twice results in the multiplication by $-p$ map $[-p]$.
- ▶ The set of \mathbb{F}_p -rational endomorphisms of a curve E/\mathbb{F}_p forms a [ring](#) $\text{End}_{\mathbb{F}_p}(E)$.
- ▶ We can define a ring homomorphism

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-p}] & \rightarrow & \text{End}_{\mathbb{F}_p}(E) \\ n & \mapsto & [n] \\ \sqrt{-p} & \mapsto & \pi. \end{array}$$

28 / 40

Endomorphism rings

Let E/\mathbb{F}_p be supersingular.

- ▶ Applying the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$ twice results in the multiplication by $-p$ map $[-p]$.
- ▶ The set of \mathbb{F}_p -rational endomorphisms of a curve E/\mathbb{F}_p forms a [ring](#) $\text{End}_{\mathbb{F}_p}(E)$.
- ▶ We can define a ring homomorphism

$$\begin{array}{ccc} \mathbb{Z}[\sqrt{-p}] & \rightarrow & \text{End}_{\mathbb{F}_p}(E) \\ n & \mapsto & [n] \\ \sqrt{-p} & \mapsto & \pi. \end{array}$$

- ▶ **Fact:** if $p \equiv 3 \pmod{8}$, $p \geq 5$, and $E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$ is supersingular, then $\text{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$.

28 / 40

Group actions

Remember: we wanted to replace exponentiation

$$\begin{array}{ccc} \mathbb{Z} \times G & \rightarrow & G \\ (x, g) & \mapsto & g^x := \underbrace{g * \cdots * g}_{x \text{ times}}. \end{array}$$

by a **group action** of a group H on a **set** S :

$$H \times S \rightarrow S.$$

29 / 40

Group actions

Definition

An **action** of a group (H, \cdot) on a set S is a map

$$\begin{array}{ccc} H \times S & \rightarrow & S \\ (h, s) & \mapsto & h * s \end{array}$$

such that $\text{id} * s = s$ and $h_1 * (h_2 * s) = (h_1 \cdot h_2) * s$ for all $s \in S$ and all $h_1, h_2 \in H$.

30 / 40

Group actions

Remember: we wanted to replace exponentiation

$$\begin{array}{ccc} \mathbb{Z} \times G & \rightarrow & G \\ (x, g) & \mapsto & g^x := \underbrace{g * \cdots * g}_{x \text{ times}}. \end{array}$$

by a **group action** of a group H on a **set** S :

$$H \times S \rightarrow S.$$

Now we can do it!

29 / 40

Group actions

Definition

An **action** of a group (H, \cdot) on a set S is a map

$$\begin{array}{ccc} H \times S & \rightarrow & S \\ (h, s) & \mapsto & h * s \end{array}$$

such that $\text{id} * s = s$ and $h_1 * (h_2 * s) = (h_1 \cdot h_2) * s$ for all $s \in S$ and all $h_1, h_2 \in H$.

Example

Traditional Diffie-Hellman is an example:

$(H, \cdot) = ((\mathbb{Z}/(p-1)\mathbb{Z})^*, +)$ and $S = (\mathbb{Z}/p\mathbb{Z})^*$. Exponentiation $(h, s) \mapsto s^h$ is a group action.

30 / 40

Group actions

Definition

An **action** of a group (H, \cdot) on a set S is a map

$$\begin{aligned} H \times S &\rightarrow S \\ (h, s) &\mapsto h * s \end{aligned}$$

such that $\text{id} * s = s$ and $h_1 * (h_2 * s) = (h_1 \cdot h_2) * s$ for all $s \in S$ and all $h_1, h_2 \in H$.

For the CSIDH group action

- ▶ the set S is the set of supersingular $E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$ with $p \equiv 3 \pmod{8}$ and $p \geq 5$.
- ▶ the group H is the **class group** of the endomorphism ring $\mathbb{Z}[\sqrt{-p}]$.

30 / 40

Class groups

Let $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Definition

An **ideal** $I \subset \mathcal{O}$ is the set of all \mathcal{O} -linear combinations of a given set of elements of \mathcal{O} .

31 / 40

Class groups

Let $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Definition

An **ideal** $I \subset \mathcal{O}$ is the set of all \mathcal{O} -linear combinations of a given set of elements of \mathcal{O} .

Example

In $\mathbb{Z}[\sqrt{-3}]$ we can consider the ideal

$$\langle 7, 2 + \sqrt{-3} \rangle := \{7a + (2 + \sqrt{-3})b : a, b \in \mathbb{Z}[\sqrt{-3}]\}.$$

31 / 40

Class groups

Let $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Definition

An **ideal** $I \subset \mathcal{O}$ is the set of all \mathcal{O} -linear combinations of a given set of elements of \mathcal{O} .

Example

In $\mathbb{Z}[\sqrt{-3}]$ we can consider the ideal

$$\langle 7, 2 + \sqrt{-3} \rangle := \{7a + (2 + \sqrt{-3})b : a, b \in \mathbb{Z}[\sqrt{-3}]\}.$$

Definition

A **principal ideal** is an ideal of the form $I = \langle \alpha \rangle$.

31 / 40

Class groups

Let $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$.

Definition

An **ideal** $I \subset \mathcal{O}$ is the set of all \mathcal{O} -linear combinations of a given set of elements of \mathcal{O} .

Example

In $\mathbb{Z}[\sqrt{-3}]$ we can consider the ideal

$$\langle 7, 2 + \sqrt{-3} \rangle := \{7a + (2 + \sqrt{-3})b : a, b \in \mathbb{Z}[\sqrt{-3}]\}.$$

Definition

A **principal ideal** is an ideal of the form $I = \langle \alpha \rangle$.

- We can **multiply** ideals I and $J \subset \mathcal{O}$:

$$I \cdot J = \langle \alpha\beta : \alpha \in I, \beta \in J \rangle.$$

31 / 40

Class groups

Definition

Two ideals $I, J \subseteq \mathcal{O}$ are **equivalent** if there exist $\alpha, \beta \in \mathcal{O} \setminus \{0\}$ such that

$$\langle \alpha \rangle \cdot I = \langle \beta \rangle \cdot J.$$

Definition

The **ideal class group** of \mathcal{O} is²

$$\text{Cl}(\mathcal{O}) = \{\text{equivalence classes of nonzero ideals } I \subset \mathcal{O}\}.$$

²modulo details

32 / 40

Class groups

Definition

Two ideals $I, J \subseteq \mathcal{O}$ are **equivalent** if there exist $\alpha, \beta \in \mathcal{O} \setminus \{0\}$ such that

$$\langle \alpha \rangle \cdot I = \langle \beta \rangle \cdot J.$$

²modulo details

32 / 40

Class groups

Definition

Two ideals $I, J \subseteq \mathcal{O}$ are **equivalent** if there exist $\alpha, \beta \in \mathcal{O} \setminus \{0\}$ such that

$$\langle \alpha \rangle \cdot I = \langle \beta \rangle \cdot J.$$

Definition

The **ideal class group** of \mathcal{O} is²

$$\text{Cl}(\mathcal{O}) = \{\text{equivalence classes of nonzero ideals } I \subset \mathcal{O}\}.$$

Miracle fact: the ideal class group is a group!

²modulo details

32 / 40

Class group action

The **class group** of the endomorphism ring $\mathbb{Z}[\sqrt{-p}]$ **acts** on the set S of supersingular elliptic curves $E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$ with $p \equiv 3 \pmod{8}$ and $p \geq 5$.

33 / 40

Class group action

The **class group** of the endomorphism ring $\mathbb{Z}[\sqrt{-p}]$ **acts** on the set S of supersingular elliptic curves $E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$ with $p \equiv 3 \pmod{8}$ and $p \geq 5$. How?

- Recall: An isogeny is **uniquely determined** by its kernel.

33 / 40

Class group action

The **class group** of the endomorphism ring $\mathbb{Z}[\sqrt{-p}]$ **acts** on the set S of supersingular elliptic curves $E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$ with $p \equiv 3 \pmod{8}$ and $p \geq 5$. How?

- Recall: An isogeny is **uniquely determined** by its kernel.
- Let $I \subset \text{End}_{\mathbb{F}_p}(E)$ be an ideal. Then

$$H_I = \cap_{\alpha \in I} \ker(\alpha)$$

is a **subgroup** of $E(\overline{\mathbb{F}_p})$.

33 / 40

Class group action

The **class group** of the endomorphism ring $\mathbb{Z}[\sqrt{-p}]$ **acts** on the set S of supersingular elliptic curves $E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$ with $p \equiv 3 \pmod{8}$ and $p \geq 5$. How?

- Recall: An isogeny is **uniquely determined** by its kernel.
- Let $I \subset \text{End}_{\mathbb{F}_p}(E)$ be an ideal. Then

$$H_I = \cap_{\alpha \in I} \ker(\alpha)$$

is a **subgroup** of $E(\overline{\mathbb{F}_p})$.

- Define $f_I : E \rightarrow E'$ to be the isogeny with kernel H_I .

33 / 40

Class group action

The **class group** of the endomorphism ring $\mathbb{Z}[\sqrt{-p}]$ **acts** on the set S of supersingular elliptic curves $E_A/\mathbb{F}_p : y^2 = x^3 + Ax^2 + x$ with $p \equiv 3 \pmod{8}$ and $p \geq 5$. How?

- Recall: An isogeny is **uniquely determined** by its kernel.
- Let $I \subset \text{End}_{\mathbb{F}_p}(E)$ be an ideal. Then

$$H_I = \cap_{\alpha \in I} \ker(\alpha)$$

is a **subgroup** of $E(\overline{\mathbb{F}_p})$.

- Define $f_I : E \rightarrow E'$ to be the isogeny with kernel H_I .

The CSIDH group action is:

$$\begin{array}{ccc} \text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S & \rightarrow & S \\ (I, E) & \mapsto & f_I(E). \end{array}$$

33 / 40

Class group action

The CSIDH group action is:

$$\begin{array}{ccc} \text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S & \rightarrow & S \\ (I, E) & \mapsto & I * E := f_I(E). \end{array}$$

34 / 40

Class group action

The CSIDH group action is:

$$\begin{array}{ccc} \text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S & \rightarrow & S \\ (I, E) & \mapsto & I * E := f_I(E). \end{array}$$

- The isogeny f_I is an ℓ -isogeny if and only if $I = \langle [\ell], \pi \pm [1] \rangle$.

Class group action

The CSIDH group action is:

$$\begin{array}{ccc} \text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S & \rightarrow & S \\ (I, E) & \mapsto & I * E := f_I(E). \end{array}$$

- The isogeny f_I is an ℓ -isogeny if and only if $I = \langle [\ell], \pi \pm [1] \rangle$.
- A '+' direction isogeny on the ℓ -isogeny graph is the action of $\langle [\ell], \pi - [1] \rangle$.

34 / 40

34 / 40

Class group action

The CSIDH group action is:

$$\begin{aligned} \text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S &\rightarrow S \\ (I, E) &\mapsto I * E := f_I(E). \end{aligned}$$

- The isogeny f_I is an ℓ -isogeny if and only if $I = \langle [\ell], \pi \pm [1] \rangle$.
- A $' + '$ direction isogeny on the ℓ -isogeny graph is the action of $\langle [\ell], \pi - [1] \rangle$.
- A $' - '$ direction isogeny on the ℓ -isogeny graph is the action of $\langle [\ell], \pi + [1] \rangle$.

34 / 40

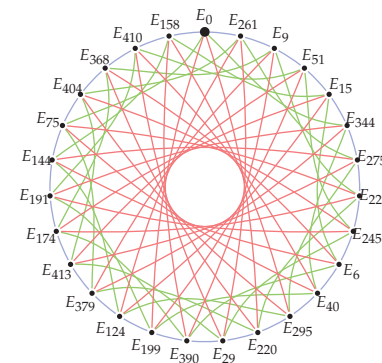
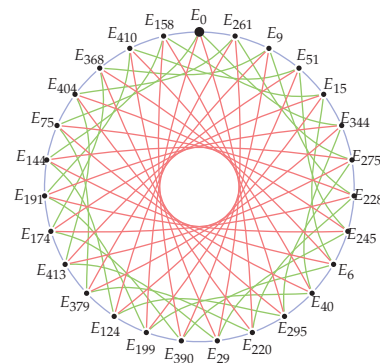
Diffie-Hellman with CSIDH

Alice

$$a = [+ , - , + , -]$$

Bob

$$b = [+ , + , - , +]$$



35 / 40

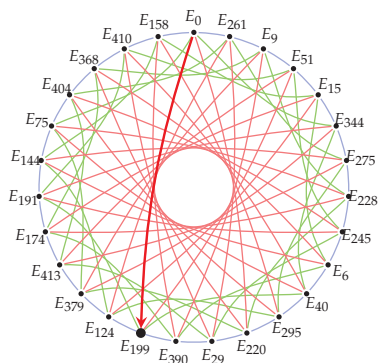
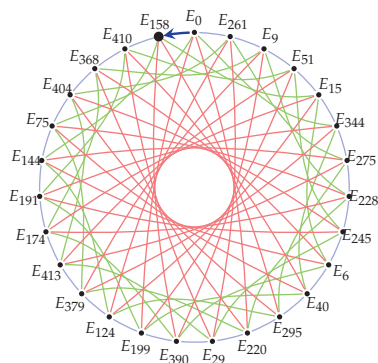
Diffie-Hellman with CSIDH

Alice

$$a = [+ , - , + , -]$$

Bob

$$b = [+ , + , - , +]$$



$$E_{158} = \langle 3, \pi - 1 \rangle * E_0 \quad E_{199} = \langle 7, \pi - 1 \rangle * E_0$$

35 / 40

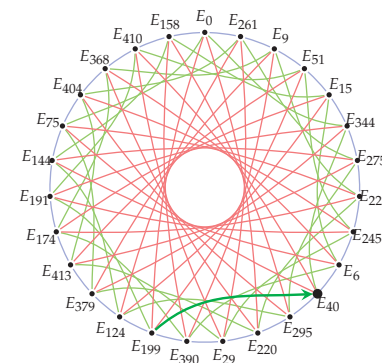
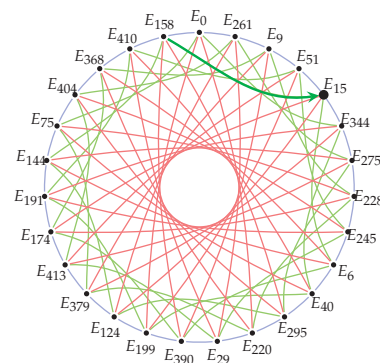
Diffie-Hellman with CSIDH

Alice

$$a = [+ , - , + , -]$$

Bob

$$b = [+ , + , - , +]$$

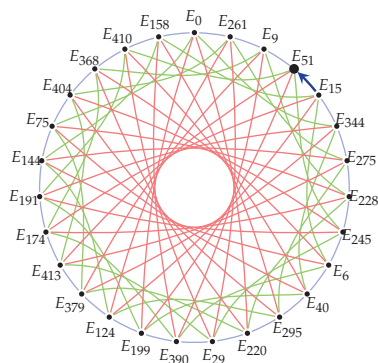


$$E_{15} = \langle 5, \pi + 1 \rangle * E_{158} \quad E_{40} = \langle 5, \pi - 1 \rangle * E_{199}$$

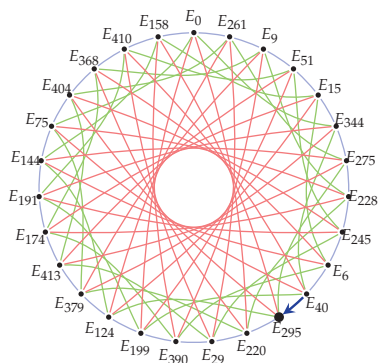
35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+ , - , + , -]$
 \uparrow



Bob
 $b = [+ , + , - , +]$
 \uparrow

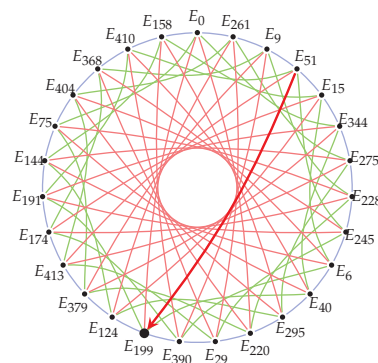


$$E_{15} = \langle 3, \pi - 1 \rangle * E_{51} \quad E_{295} = \langle 3, \pi + 1 \rangle * E_{40}$$

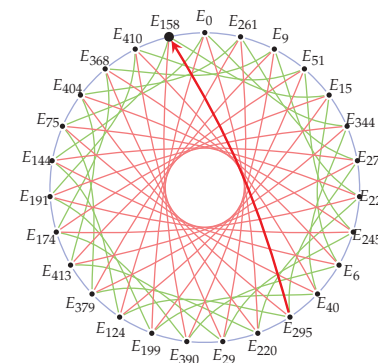
35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+ , - , + , -]$
 \uparrow



Bob
 $b = [+ , + , - , +]$
 \uparrow

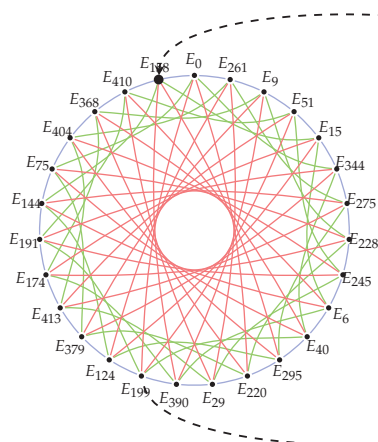


$$E_{199} = \langle 7, \pi + 1 \rangle * E_{51} \quad E_{158} = \langle 7, \pi - 1 \rangle * E_{295}$$

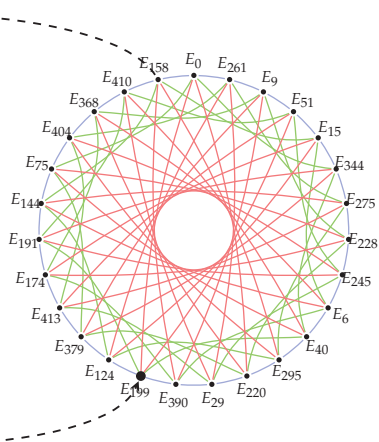
35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+ , - , + , -]$



Bob
 $b = [+ , + , - , +]$

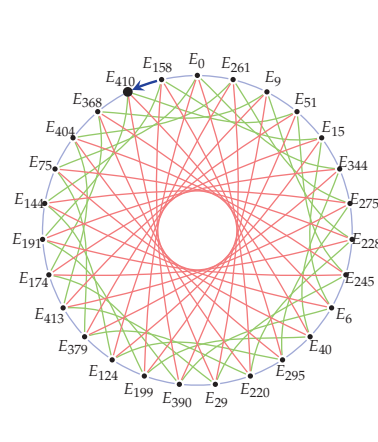


(exchange of public keys)

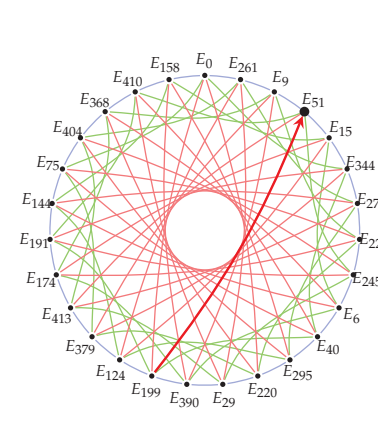
35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+ , - , + , -]$
 \uparrow



Bob
 $b = [+ , + , - , +]$
 \uparrow



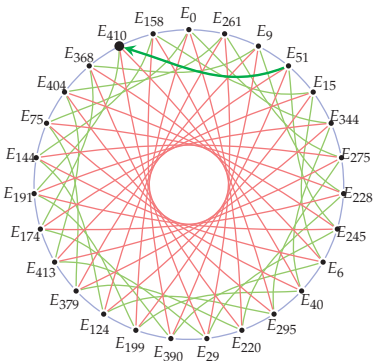
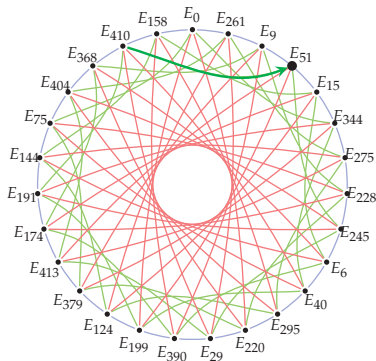
$$E_{410} = \langle 3, \pi - 1 \rangle * E_{158} \quad E_{51} = \langle 7, \pi - 1 \rangle * E_{199}$$

35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+,-,+, -]$
 ↑

Bob
 $b = [+,\color{green}{+},-,\color{red}{+}]$
 ↑



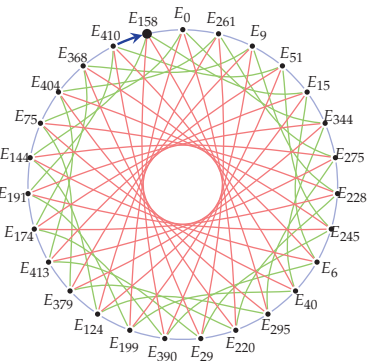
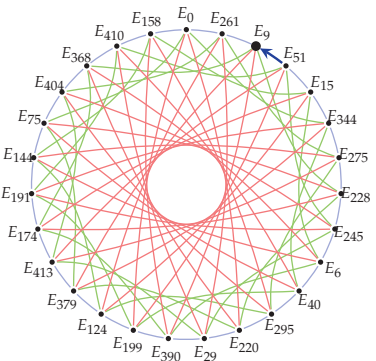
$$E_{51} = \langle 5, \pi + 1 \rangle * E_{410} \quad E_{410} = \langle 5, \pi - 1 \rangle * E_{51}$$

35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+,-,+, -]$
 ↑

Bob
 $b = [+,\color{green}{+},-,\color{red}{+}]$
 ↑



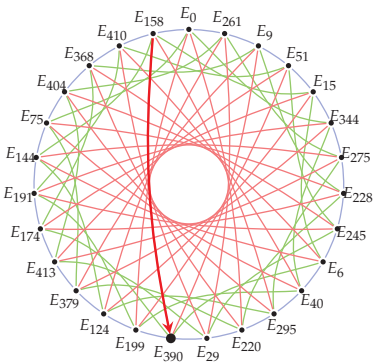
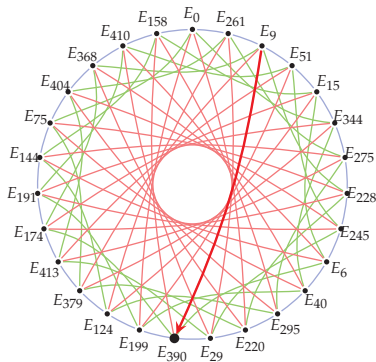
$$E_9 = \langle 3, \pi - 1 \rangle * E_{51} \quad E_{158} = \langle 3, \pi + 1 \rangle * E_{410}$$

35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+,-,+, -]$
 ↑

Bob
 $b = [+,\color{green}{+},-,\color{red}{+}]$
 ↑



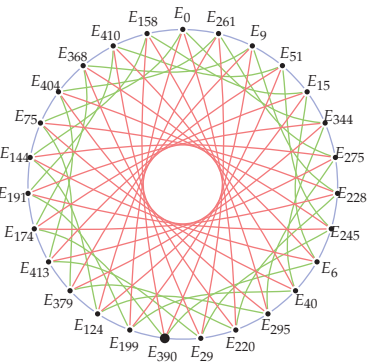
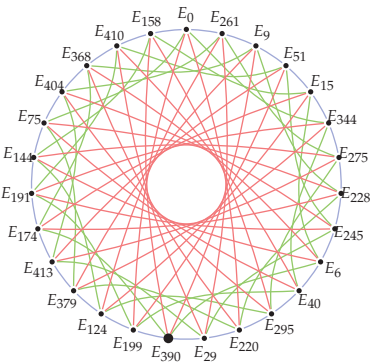
$$E_{390} = \langle 7, \pi + 1 \rangle * E_9 \quad E_{390} = \langle 7, \pi - 1 \rangle * E_{158}$$

35 / 40

Diffie-Hellman with CSIDH

Alice
 $a = [+,-,+, -]$
 ↑

Bob
 $b = [+,\color{green}{+},-,\color{red}{+}]$
 ↑



(shared secret key is E_{390})

35 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .

36 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .
- ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.

36 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .
- ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- ▶ Fix $E_0/\mathbb{F}_p : y^2 = x^3 + x$.

36 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .
- ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- ▶ Fix $E_0/\mathbb{F}_p : y^2 = x^3 + x$.
- ▶ Then E_0 is supersingular.

36 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .
- ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- ▶ Fix $E_0/\mathbb{F}_p : y^2 = x^3 + x$.
- ▶ Then E_0 is supersingular. **Exercise:** show that there is a point of order ℓ_i in $E_0(\mathbb{F}_p)$ for every ℓ_1, \dots, ℓ_n .

36 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .
- ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- ▶ Fix $E_0/\mathbb{F}_p : y^2 = x^3 + x$.
- ▶ Then E_0 is supersingular. **Exercise:** show that there is a point of order ℓ_i in $E_0(\mathbb{F}_p)$ for every ℓ_1, \dots, ℓ_n .
- ▶ All arithmetic for computing ℓ_i -isogenies is now over \mathbb{F}_p . (For more: see David's talk).
- ▶ Every G_{ℓ_i} containing E_0 is a disjoint union of cycles.

36 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .
- ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- ▶ Fix $E_0/\mathbb{F}_p : y^2 = x^3 + x$.
- ▶ Then E_0 is supersingular. **Exercise:** show that there is a point of order ℓ_i in $E_0(\mathbb{F}_p)$ for every ℓ_1, \dots, ℓ_n .
- ▶ All arithmetic for computing ℓ_i -isogenies is now over \mathbb{F}_p . (For more: see David's talk).

36 / 40

Design choices

- ▶ Choose small odd primes ℓ_1, \dots, ℓ_n .
- ▶ Make sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime.
- ▶ Fix $E_0/\mathbb{F}_p : y^2 = x^3 + x$.
- ▶ Then E_0 is supersingular. **Exercise:** show that there is a point of order ℓ_i in $E_0(\mathbb{F}_p)$ for every ℓ_1, \dots, ℓ_n .
- ▶ All arithmetic for computing ℓ_i -isogenies is now over \mathbb{F}_p . (For more: see David's talk).
- ▶ Every G_{ℓ_i} containing E_0 is a disjoint union of cycles.
- ▶ Every node of G_{ℓ_i} is of the form $E_A : y^2 = x^3 + Ax^2 + x -$ can be compressed to just $A \in \mathbb{F}_p$ giving tiny keys.

36 / 40

Why CSIDH?

- ▶ Drop-in post-quantum replacement for (EC)DH

37 / 40

Why CSIDH?

- ▶ Drop-in post-quantum replacement for (EC)DH
- ▶ Non-interactive key exchange (full public-key validation); previously an open problem post-quantumly (for reasonable run-time)

37 / 40

Why CSIDH?

- ▶ Drop-in post-quantum replacement for (EC)DH
- ▶ Non-interactive key exchange (full public-key validation); previously an open problem post-quantumly (for reasonable run-time)
- ▶ Small keys: 64 bytes at conjectured AES-128 security level

37 / 40

Why CSIDH?

- ▶ Drop-in post-quantum replacement for (EC)DH
- ▶ Non-interactive key exchange (full public-key validation); previously an open problem post-quantumly (for reasonable run-time)
- ▶ Small keys: 64 bytes at conjectured AES-128 security level
- ▶ Competitive speed: ~ 85 ms for a full key exchange

37 / 40

Why CSIDH?

- ▶ Drop-in [post-quantum replacement](#) for (EC)DH
- ▶ [Non-interactive key exchange](#) (full [public-key validation](#)); previously an open problem post-quantumly (for reasonable run-time)
- ▶ [Small](#) keys: [64 bytes](#) at conjectured AES-128 security level
- ▶ Competitive [speed](#): ~ 85 ms for a full key exchange
- ▶ [Flexible](#): compatible with 0-RTT protocols such as QUIC; recent preprint uses CSIDH for 'SeaSign' [signatures](#)

37 / 40

Work in progress & future work

- ▶ [Fast, constant-time](#) implementation. For constant-time ideas, see [BLMP].

38 / 40

Work in progress & future work

- ▶ [Fast, constant-time](#) implementation. For constant-time ideas, see [BLMP].
- ▶ More [applications](#).

38 / 40

Work in progress & future work

- ▶ [Fast, constant-time](#) implementation. For constant-time ideas, see [BLMP].
- ▶ More [applications](#).
- ▶ [Your paper here!]

38 / 40



References

Mentioned in this talk:

- Castryck, Lange, Martindale, Panny, Renes:
CSIDH: An Efficient Post-Quantum Commutative Group Action
<https://ia.cr/2018/383> (to appear at ASIACRYPT 2018)
- [BLMP] Bernstein, Lange, Martindale, Panny:
Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies
<https://eprint.iacr.org/2018/1059>
- De Feo, Galbraith:
SeaSign: Compact isogeny signatures from class group actions
<https://ia.cr/2018/824>

Credits should also go to Lorenz Panny - many of the slides from this presentation are from a joint presentation with Lorenz at the Crypto Working Group in Utrecht, the Netherlands. He made all the beautiful pictures! Also credits to Wouter Castryck, whose slides were a source of inspiration for this presentation.

References

Other related work:

- Biasse, Iezzi, Jacobson:
A note on the security of CSIDH
<https://arxiv.org/pdf/1806.03656> (to appear at Indocrypt 2018)
- Bonnetain, Schrottenloher:
*Quantum Security Analysis of CSIDH and Ordinary Isogeny-based Schemes*³
<https://ia.cr/2018/537>
- Childs, Jao, Soukharev:
Constructing elliptic curve isogenies in quantum subexponential time
<https://arxiv.org/abs/1012.4019>
- Delfs, Galbraith:
Computing isogenies between supersingular elliptic curves over \mathbb{F}_p
<https://arxiv.org/abs/1310.7789>
- De Feo, Kieffer, Smith:
Towards practical key exchange from ordinary isogeny graphs
<https://ia.cr/2018/485> (to appear at ASIACRYPT 2018)
- Jao, LeGrow, Leonardi, Ruiz-Lopez:
A polynomial quantum space attack on CRS and CSIDH
(to appear at MathCrypt 2018)
- Meyer, Reith:
A faster way to the CSIDH
<https://ia.cr/2018/782> (to appear at Indocrypt 2018)

Parameters

| CSIDH-log p | intended NIST level | public key size | private key size | time (full exchange) | cycles (full exchange) | stack memory | classical security |
|---------------|---------------------|-----------------|------------------|----------------------|------------------------|--------------|--------------------|
| CSIDH-512 | 1 | 64 b | 32 b | 85 ms | 212e6 | 4368 b | 128 |
| CSIDH-1024 | 3 | 128 b | 64 b | | | | 256 |
| CSIDH-1792 | 5 | 224 b | 112 b | | | | 448 |

³ Concrete numbers in this paper should be treated with caution, see [Section 1.3, BLMP]