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

Wouter Castryck[1] Tanja Lange[2] Chloe Martindale[2]
Lorenz Panny[2] Joost Renes[3]

[1]KU Leuven [2]TU Eindhoven [3]RU Nijmegen

ECC Autumn School, Osaka, 17-18 November 2018


[ˈsiːˌsaɪd]

Traditional Diffie-Hellman key exchange

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

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

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.

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

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

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

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

Examples:

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

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

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

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

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

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 $\underbrace{g * \cdots * g}_{x \text{ times}}$.

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 $g^x = \underbrace{g * \cdots * g}_{x \text{ times}}$.

$a \in \mathbb{Z}$

$g \in G$

$b \in \mathbb{Z}$

Traditional Diffie-Hellman key exchange

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

$a \in \mathbb{Z}$

$g \in G$

$\xrightarrow{g^a}$

$\xleftarrow{g^b}$

$b \in \mathbb{Z}$

Traditional Diffie-Hellman key exchange

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

$a \in \mathbb{Z}$

$(g^b)^a$

$g \in G$

$\xrightarrow{g^a}$

$\xleftarrow{g^b}$

$b \in \mathbb{Z}$

$(g^a)^b$

Traditional Diffie-Hellman key exchange

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

$g \in G$

$a \in \mathbb{Z}$

$(g^b)^a$

$\xrightarrow{g^a}$

$\xleftarrow{g^b}$

$b \in \mathbb{Z}$

$(g^a)^b$

- $k = (g^a)^b = g^{a \cdot b} = g^{b \cdot a} = (g^b)^a$.

Traditional Diffie-Hellman key exchange

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

$g \in G$

$a \in \mathbb{Z}$

$(g^b)^a$

$\xrightarrow{g^a}$

$\xleftarrow{g^b}$

$b \in \mathbb{Z}$

$(g^a)^b$

- $k = (g^a)^b = g^{a \cdot b} = g^{b \cdot a} = (g^b)^a$.
- Computing a or b given g^a and g^b should be hard (i.e. slow).

Traditional Diffie-Hellman key exchange

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

$a \in \mathbb{Z}$
$(g^b)^a$

$g \in G$

$\xrightarrow{g^a}$

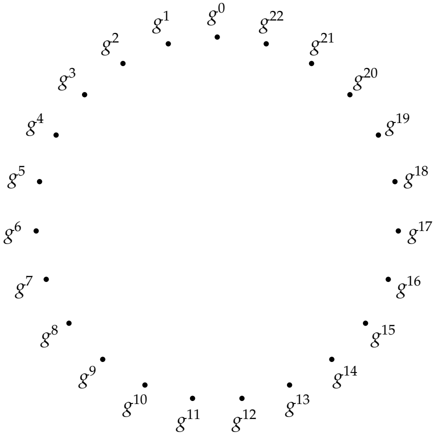
$\xleftarrow{g^b}$

$b \in \mathbb{Z}$
$(g^a)^b$

- $k = (g^a)^b = g^{a \cdot b} = g^{b \cdot a} = (g^b)^a$.
- Computing a or b given g^a and g^b should be hard (i.e. slow).
- Computing g^a given g and a should be easy (i.e. fast).

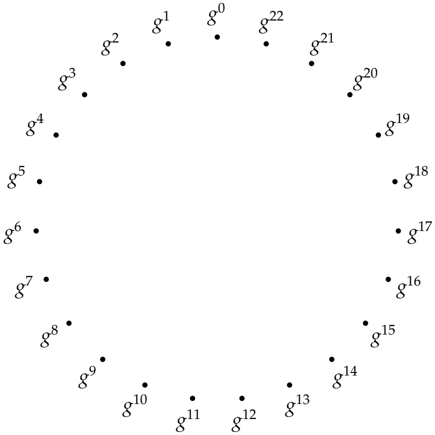
Square-and-multiply

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



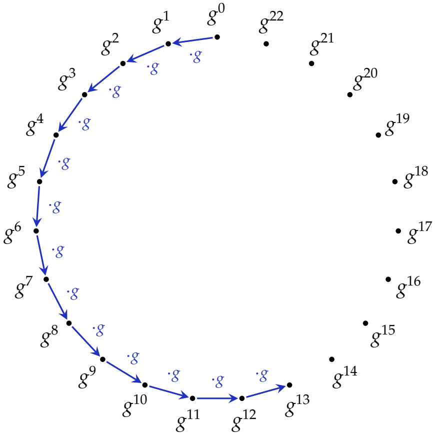
Square-and-multiply

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



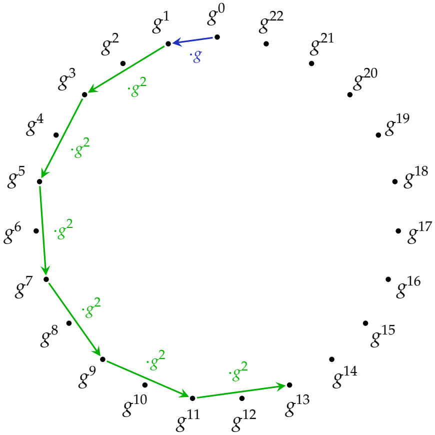
Square-and-multiply

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



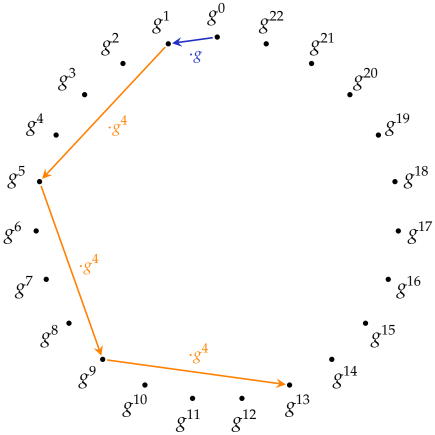
Square-and-multiply

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



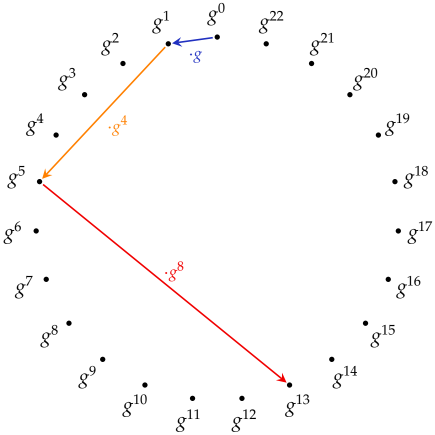
Square-and-multiply

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

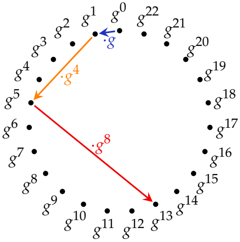


Square-and-multiply

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

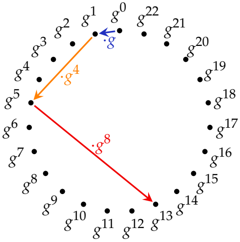


Square-and-multiply



1

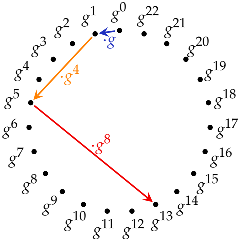
Square-and-multiply



- 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

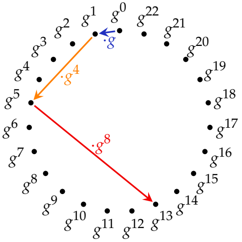
Square-and-multiply



- 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 $a = 0, \ldots, 13$, so has no shortcuts.

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

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 $a = 0, \ldots, 13$, 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).

[1] a 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)

Quantum revolution

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

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

Alice can compute g^x in polynomial time.

Quantum revolution

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

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

Alice can compute g^x in polynomial time.

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

Quantum revolution

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

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

Alice can compute g^x in polynomial time.

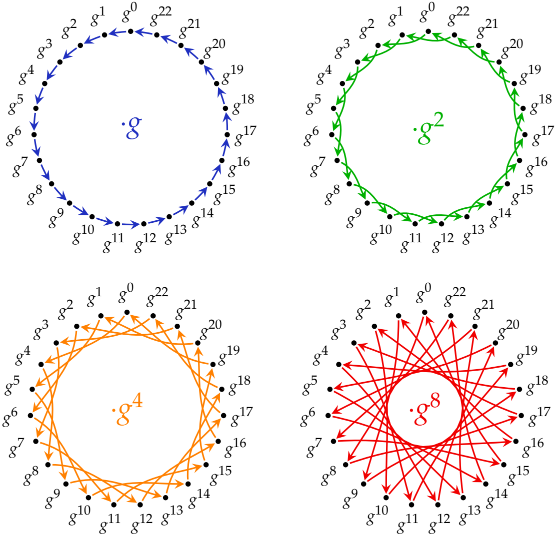
Given a quantum computer, Shor's algorithm computes x from g^x ...also in polynomial time.

$\rightsquigarrow$ Idea:

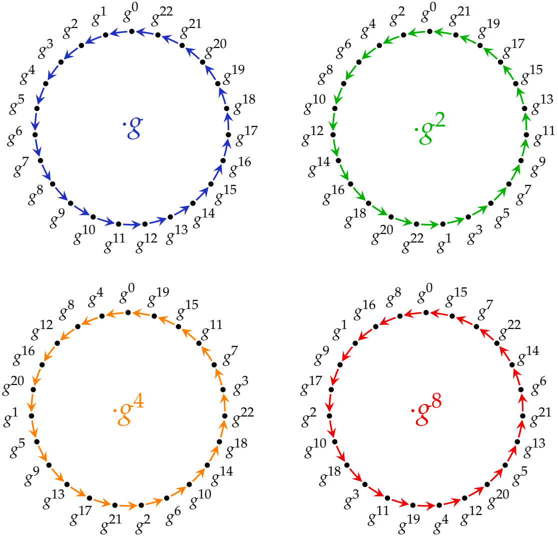
Replace the map $\mathbb{Z} \times G \to G$ by a group action of a group H on a set S:

$$H \times S \to S.$$

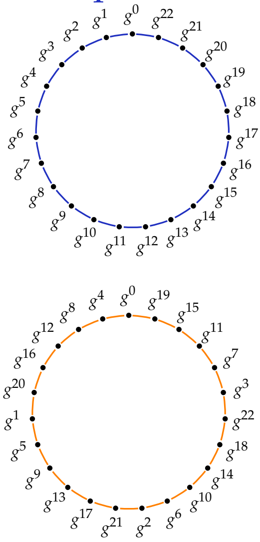
What do we keep from traditional (EC)DH?



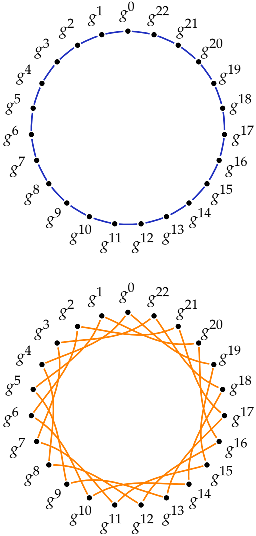
What do we keep from traditional (EC)DH?



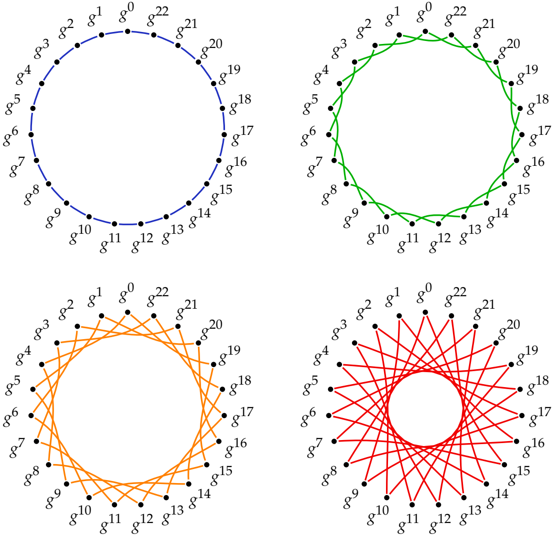
What do we keep from traditional (EC)DH?



What do we keep from traditional (EC)DH?

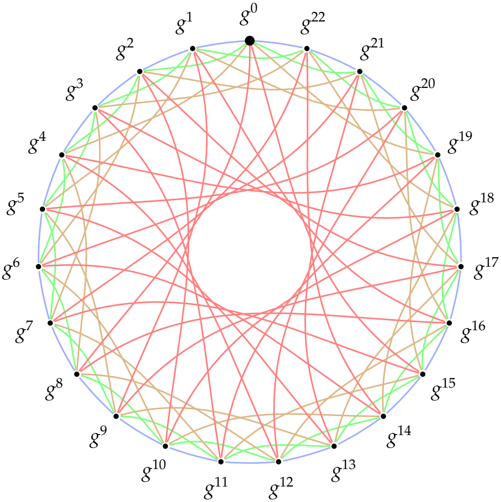


What do we keep from traditional (EC)DH?



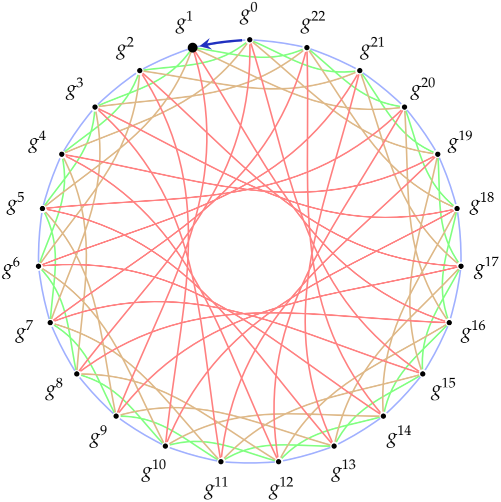
Cycles are compatible: [right, then left] = [left, then right], etc.

What do we keep from traditional (EC)DH?



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

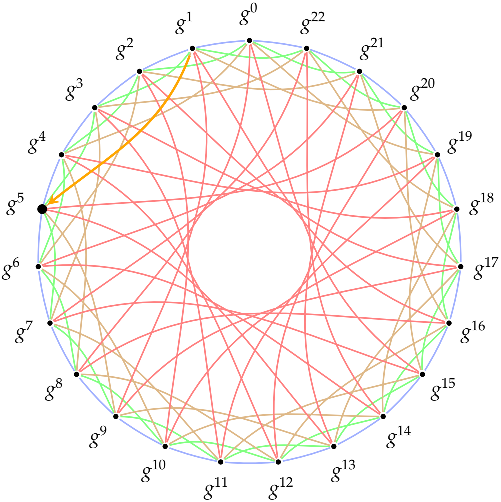
What do we keep from traditional (EC)DH?



Cycles are compatible:

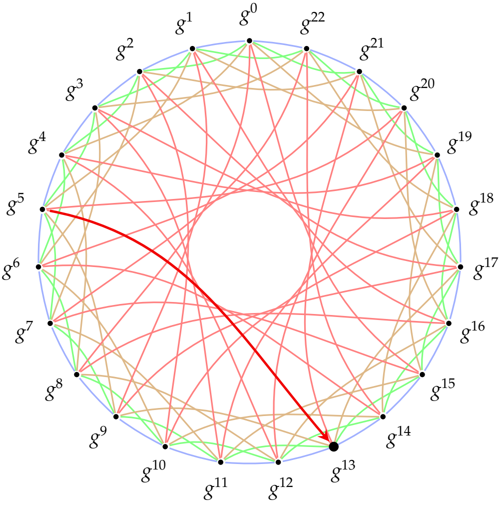
$g^{13} = \quad g * g^0$, etc.

What do we keep from traditional (EC)DH?



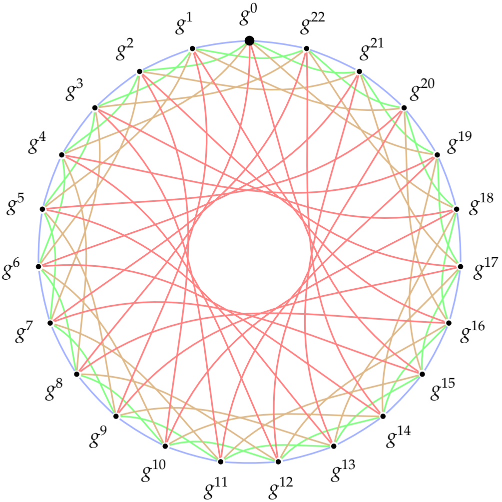
Cycles are compatible:
$g^{13} = \quad g^4 * g * g^0$, etc.

What do we keep from traditional (EC)DH?



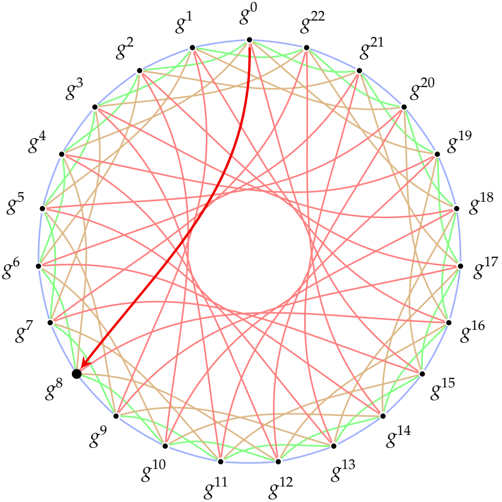
Cycles are compatible:
$g^{13} = g^8 * g^4 * g * g^0$, etc.

What do we keep from traditional (EC)DH?



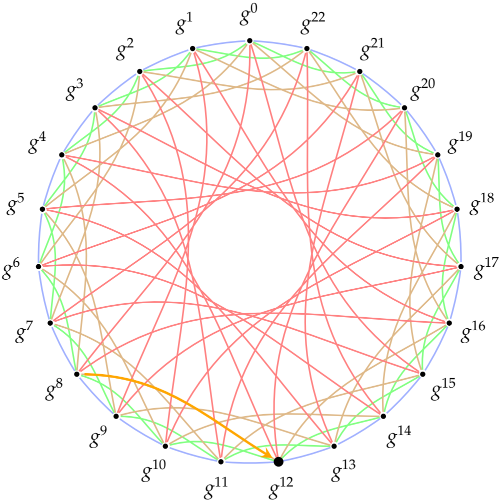
Cycles are compatible:
$g^{13} = g^8 * g^4 * g * g^0 =$ g^0 , etc.

What do we keep from traditional (EC)DH?



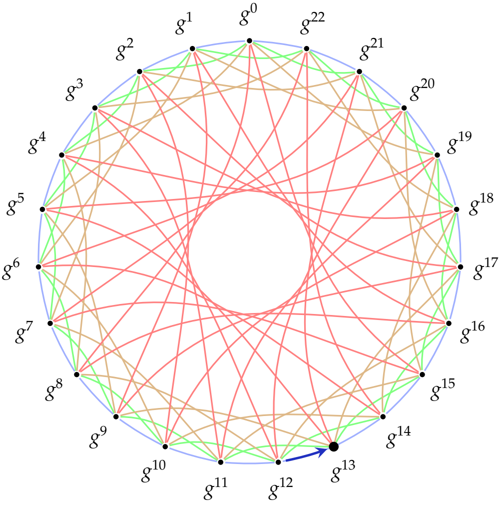
Cycles are compatible:
$g^{13} = g^8 * g^4 * g * g^0 = \quad g^8 * g^0$, etc.

What do we keep from traditional (EC)DH?



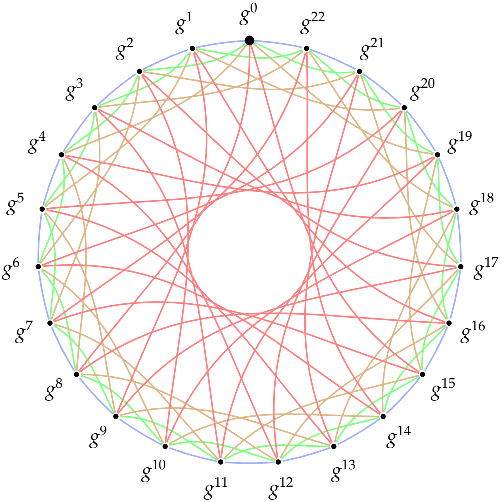
Cycles are compatible:
$g^{13} = g^8 * g^4 * g * g^0 = \quad g^4 * g^8 * g^0$, etc.

What do we keep from traditional (EC)DH?



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

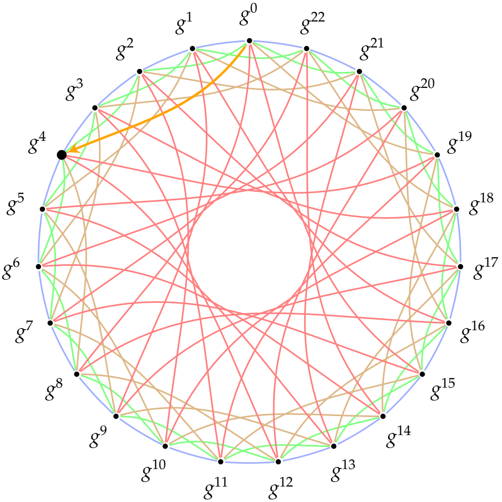
What do we keep from traditional (EC)DH?



Cycles are compatible:

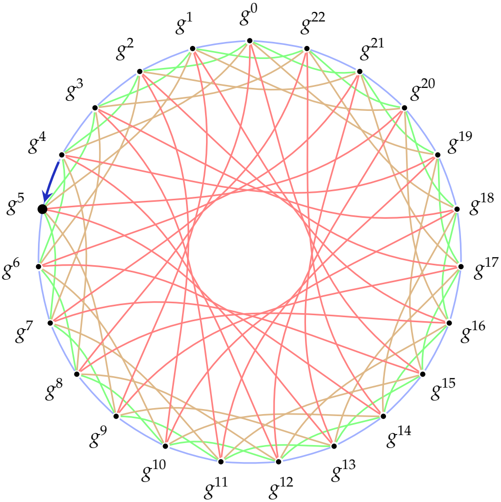
$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = \qquad g^0$, etc.

What do we keep from traditional (EC)DH?



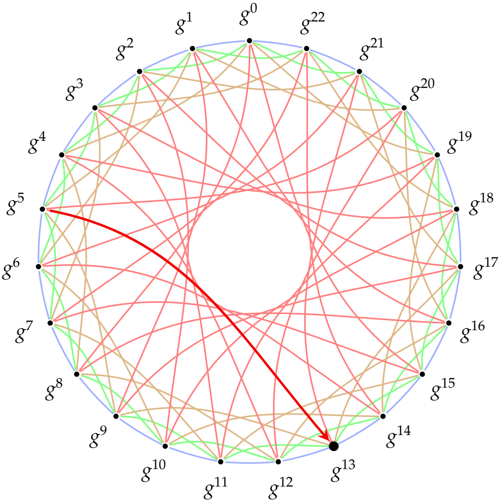
Cycles are compatible:
$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = \quad g^4 * g^0$, etc.

What do we keep from traditional (EC)DH?



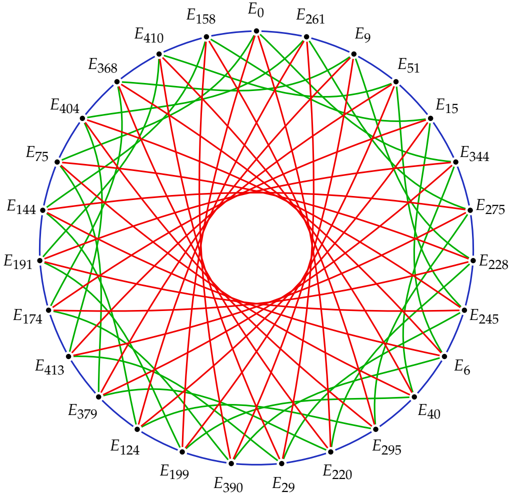
Cycles are compatible:
$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = \quad g * g^4 * g^0$, etc.

What do we keep from traditional (EC)DH?



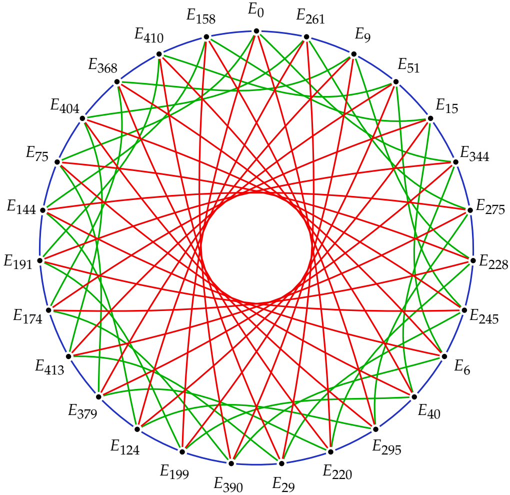
Cycles are compatible:
$g^{13} = g^8 * g^4 * g * g^0 = g * g^4 * g^8 * g^0 = g^8 * g * g^4 * g^0$, etc.

Graphs of elliptic curves



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

Graphs of elliptic curves

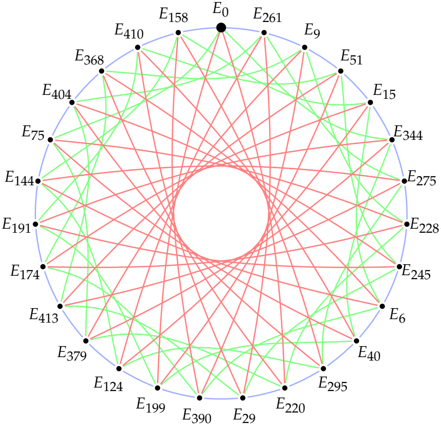


Nodes: Supersingular elliptic curves $E_A : y^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_{419}$.
Edges: 3-, 5-, and 7-isogenies (more details to come).

Diffie-Hellman on 'nice' graphs

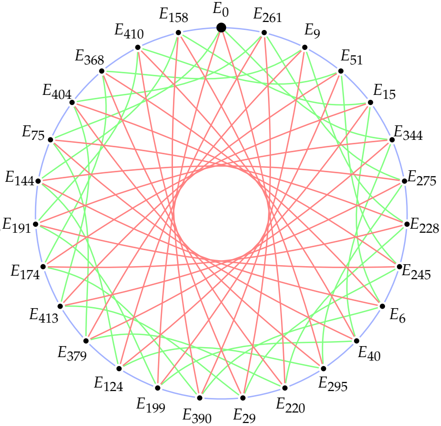
Alice

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



Bob

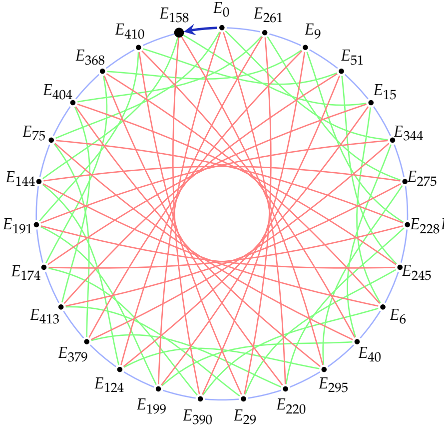
$b = [+, +, -, +]$



Diffie-Hellman on 'nice' graphs

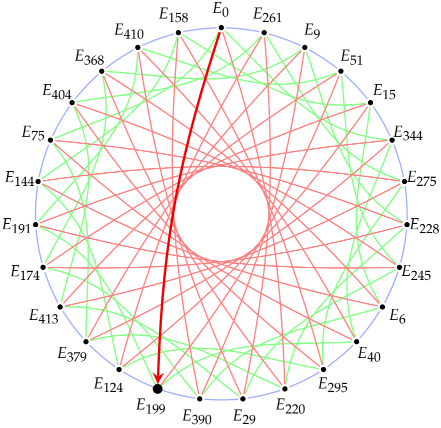
Alice

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



Bob

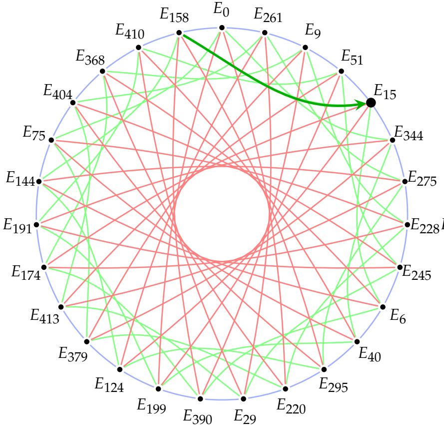
$b = [+, +, -, +]$
$\uparrow$



Diffie-Hellman on 'nice' graphs

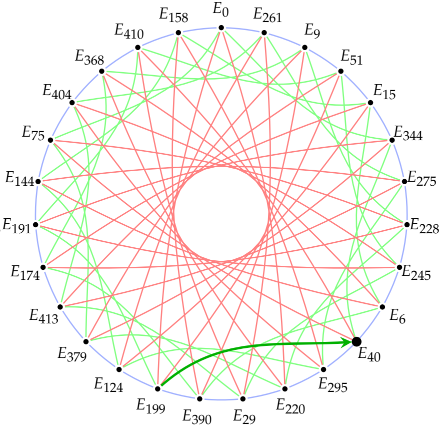
Alice

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



Bob

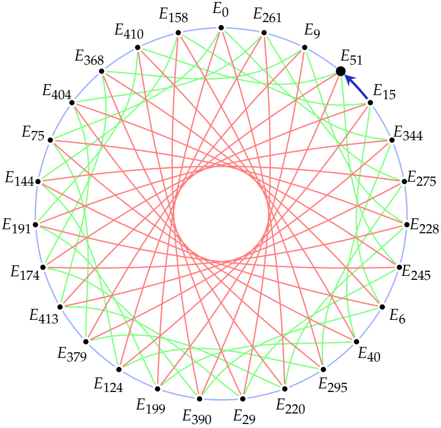
$b = [+, +, -, +]$
$\uparrow$



Diffie-Hellman on ‘nice’ graphs

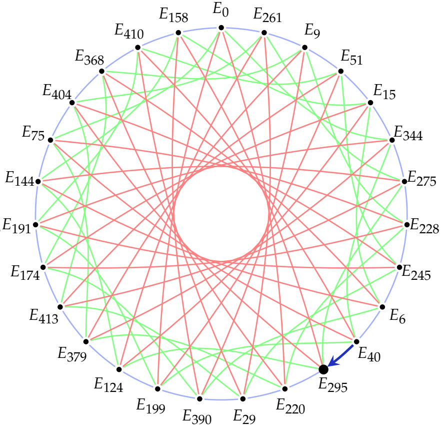
Alice

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



Bob

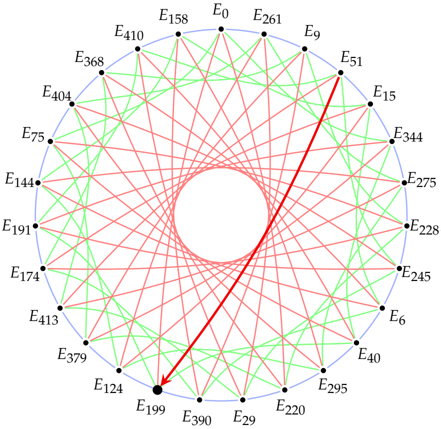
$b = [+, +, -, +]$
$\uparrow$



Diffie-Hellman on ‘nice’ graphs

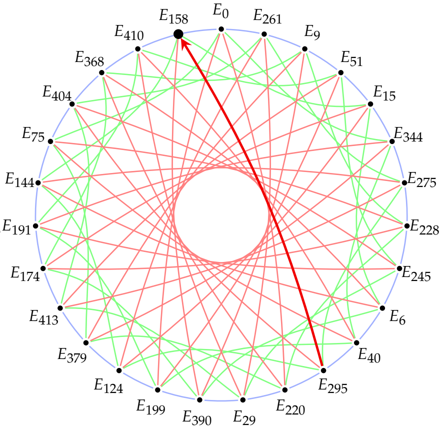
Alice

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



Bob

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



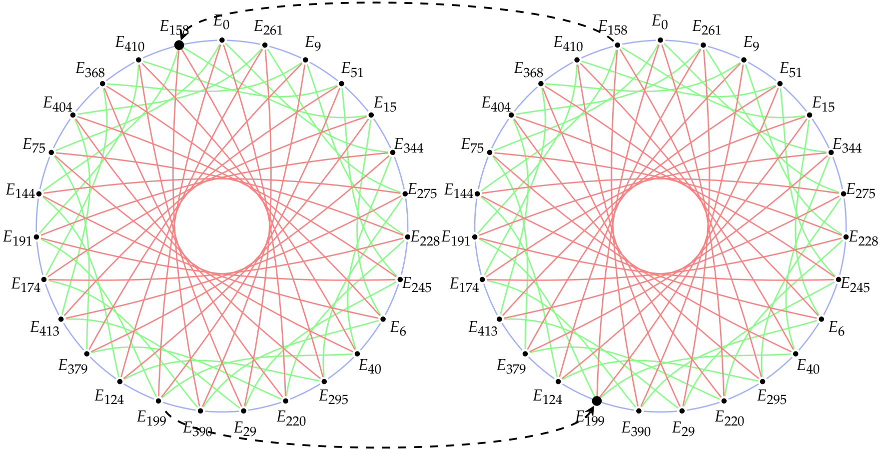
Diffie-Hellman on ‘nice’ graphs

Alice

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

Bob

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

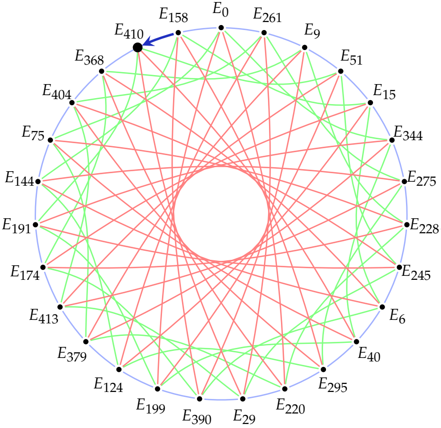


Diffie-Hellman on 'nice' graphs

Alice

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

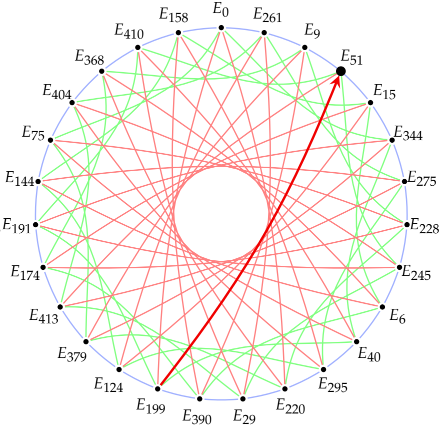
$\uparrow$



Bob

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

$\uparrow$



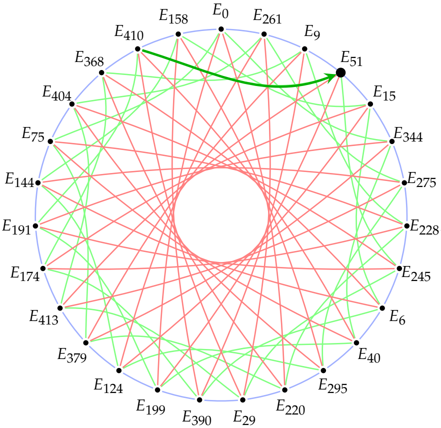
Diffie-Hellman on 'nice' graphs

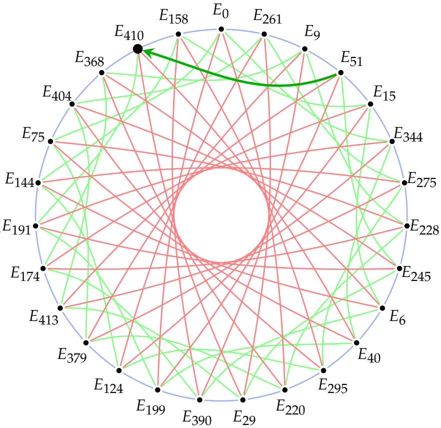
Alice

$$a = [+, \underset{\uparrow}{-}, +, -]$$

Bob

$$b = [+, \underset{\uparrow}{+}, -, +]$$

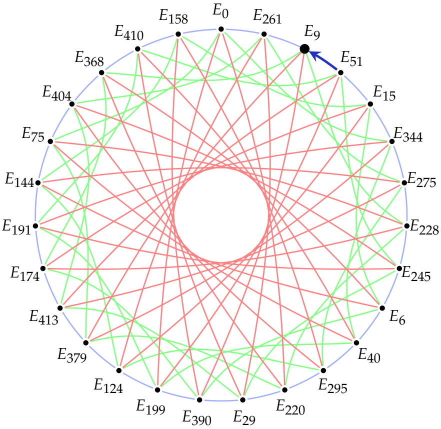




Diffie-Hellman on 'nice' graphs

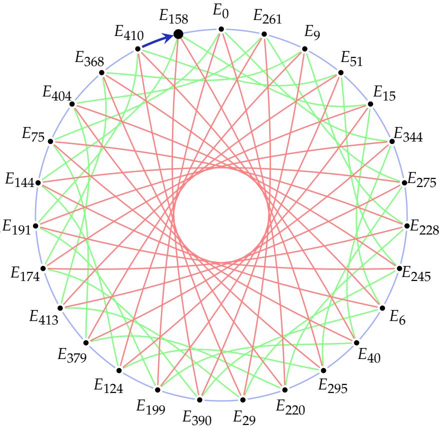
Alice

$a = [{\color{blue}+}, {\color{green}-}, {\color{blue}+}, {\color{red}-}]$
$\quad\quad\quad\quad\quad\quad\uparrow$



Bob

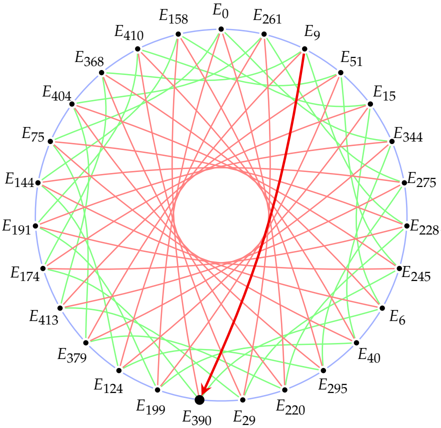
$b = [{\color{red}+}, {\color{green}+}, {\color{blue}-}, {\color{red}+}]$
$\quad\quad\quad\quad\quad\quad\uparrow$



Diffie-Hellman on 'nice' graphs

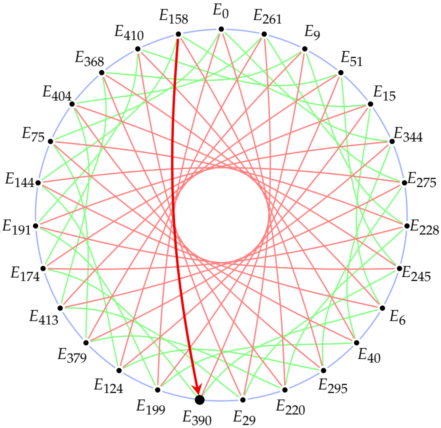
Alice

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



Bob

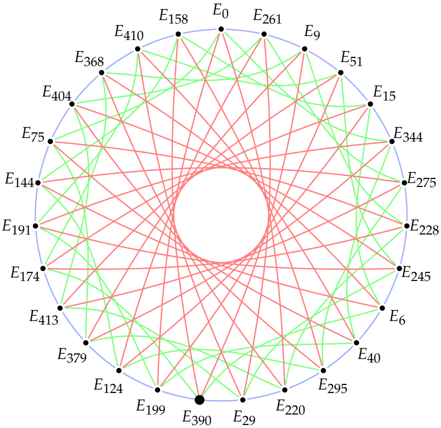
$b = [+, +, -, +]$
$\uparrow$



Diffie-Hellman on 'nice' graphs

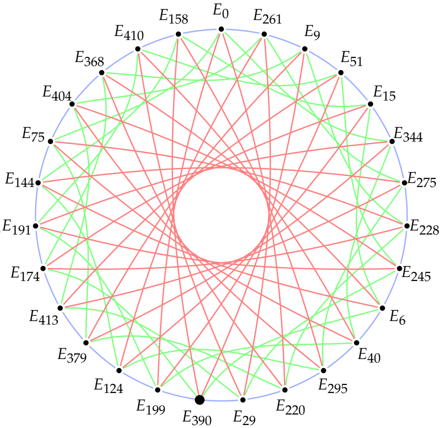
Alice

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



Bob

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



Elliptic curves

Recall from Mehdi's talk:

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'.

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

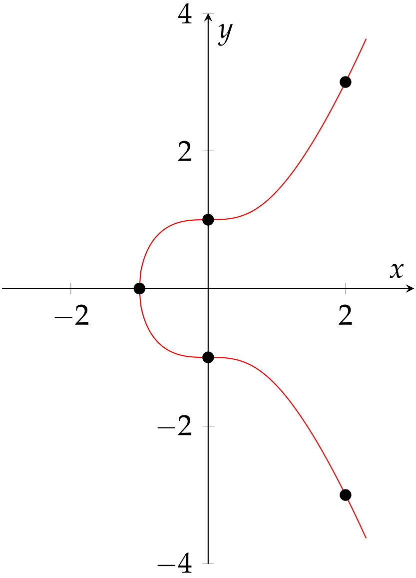
Define $E/\mathbb{F}_5 : y^2 = x^3 + 1$. Then

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

Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

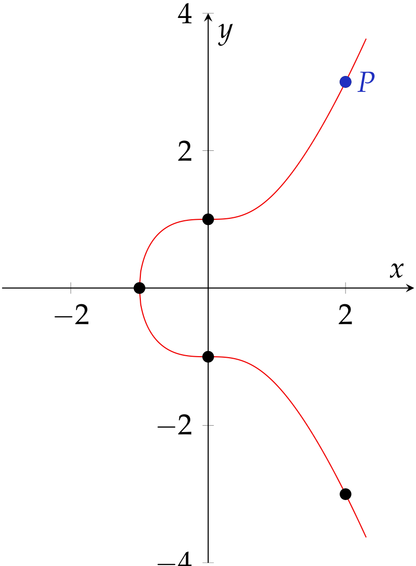
$$E(\mathbb{F}_5) = \{(2,3), (0,-1), (-1,0), (0,1), (2,-3), P_\infty\}.$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

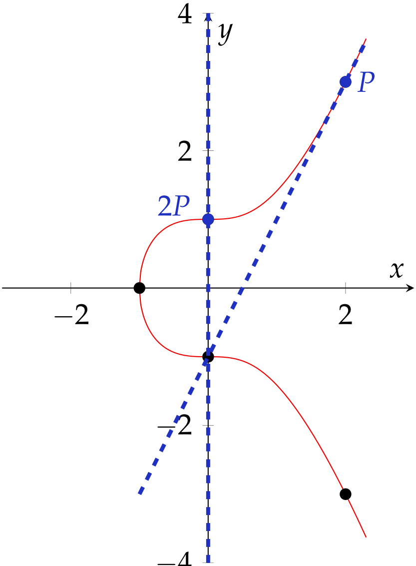
$$\begin{aligned} E(\mathbb{F}_5) = \{&(2,3), (0,-1), \\ &(-1,0), (0,1), \\ &(2,-3), P_\infty\}. \\ = \{&P \end{aligned}$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

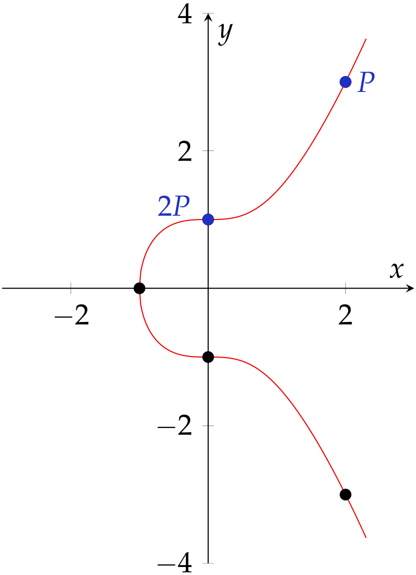
$$\begin{aligned} E(\mathbb{F}_5) &= \{(2,3),(0,-1),\\ &\qquad (-1,0),(0,1),\\ &\qquad (2,-3),P_\infty\}.\\ &= \{P, 2P, \end{aligned}$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

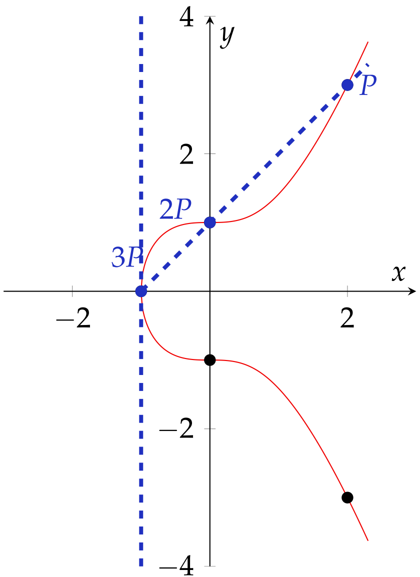
$$\begin{aligned} E(\mathbb{F}_5) = \{&(2,3), (0,-1), \\ &(-1,0), (0,1), \\ &(2,-3), P_\infty\}. \\ = \{&P, 2P, \end{aligned}$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

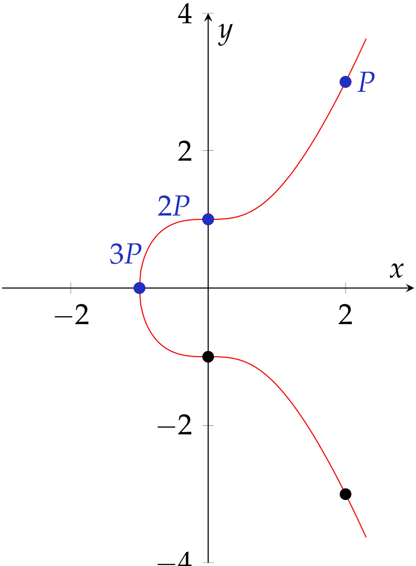
$$\begin{aligned} E(\mathbb{F}_5) &= \{(2,3), (0,-1), \\ &\qquad (-1,0), (0,1), \\ &\qquad (2,-3), P_\infty\}. \\ &= \{P, 2P, \\ &\qquad 3P, \end{aligned}$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

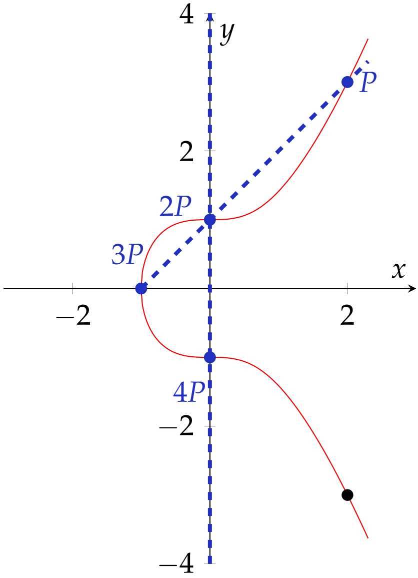
$$
\begin{aligned}
E(\mathbb{F}_5) = \{&(2,3), (0,-1),\\
&(-1,0), (0,1),\\
&(2,-3), P_\infty\}.\\
= \{&P, 2P,\\
&3P,
\end{aligned}
$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

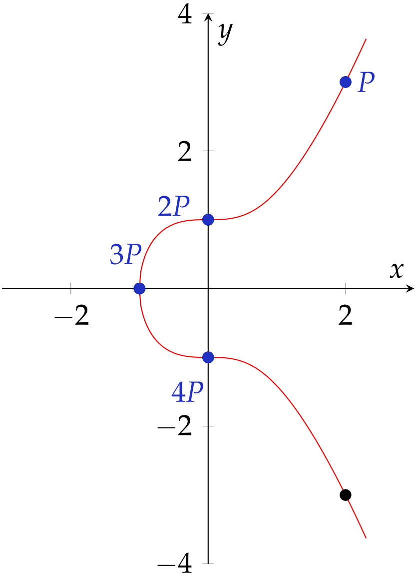
$$
\begin{aligned}
E(\mathbb{F}_5) = \{&(2,3), (0,-1),\\
&(-1,0), (0,1),\\
&(2,-3), P_\infty\}.\\
= \{&P, 2P,\\
&3P, 4P,
\end{aligned}
$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

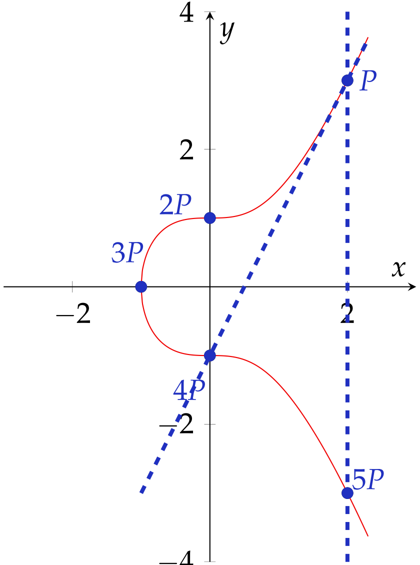
$$
\begin{aligned}
E(\mathbb{F}_5) &= \{(2,3),(0,-1),\\
&\qquad (-1,0),(0,1),\\
&\qquad (2,-3),P_\infty\}.\\
&= \{P, 2P,\\
&\qquad 3P, 4P,
\end{aligned}
$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

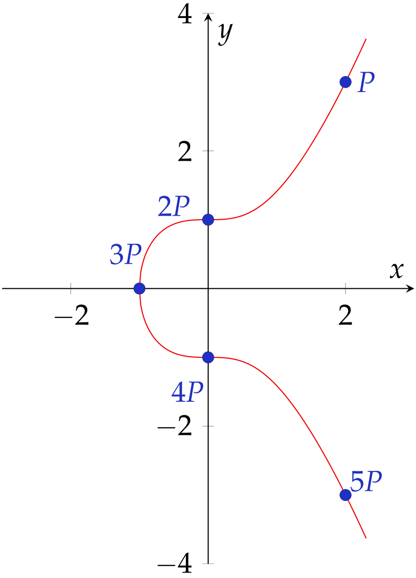
$$
\begin{aligned}
E(\mathbb{F}_5) = \{&(2,3), (0,-1),\\
&(-1,0), (0,1),\\
&(2,-3), P_\infty\}.\\
= \{&P, 2P,\\
&3P, 4P,\\
&5P,
\end{aligned}
$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

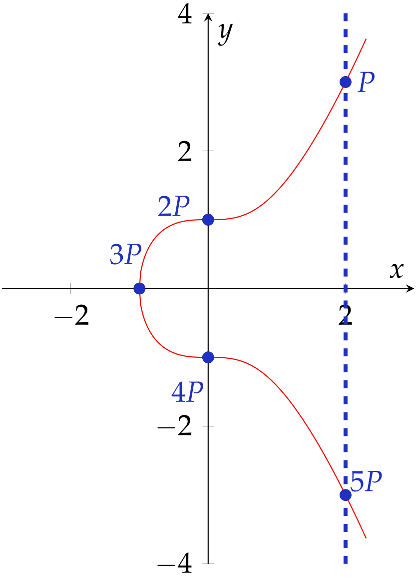
$$\begin{aligned} E(\mathbb{F}_5) = \{&(2,3),(0,-1),\\ &(-1,0),(0,1),\\ &(2,-3),P_\infty\}.\\ = \{&P, 2P,\\ &3P, 4P,\\ &5P,\end{aligned}$$



Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

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

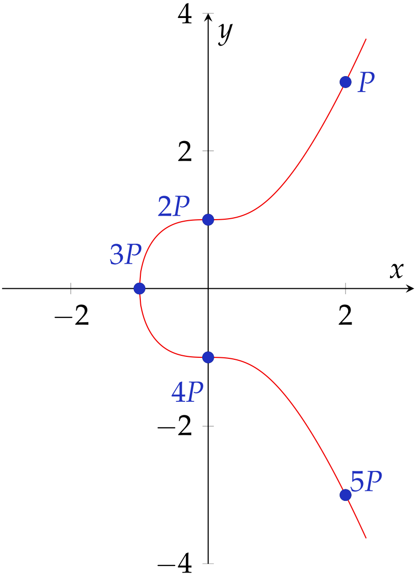


Elliptic curves

- $E : y^2 = x^3 + 1.$
- Recall

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

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



Elliptic curves

Example

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

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 $\#E(\mathbb{F}_p) = p + 1$.

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

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

Elliptic curves

Definition

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

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 $P = (2, 3)$.

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.

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.

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

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

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 $(p+1)/2$.

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

Elliptic curves and isogenies

Definition

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

Elliptic curves and isogenies

Definition

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

Example

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

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

Elliptic curves and isogenies

Definition

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

Example

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

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

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

Elliptic curves and isogenies

Definition

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

Example

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

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

Elliptic curves and isogenies

Definition

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

Example

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

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

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

Elliptic curves and isogenies

Definition

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

Example

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

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

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

Elliptic curves and isogenies

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

Example

- Exercise: show that

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

  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.

Elliptic curves and isogenies

Definition

An isogeny of elliptic curves over $\mathbb{F}_p$ is a non-zero morphism $E \to E'$ 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

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

is an isogeny.

Elliptic curves and isogenies

Example

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

Elliptic curves and isogenies

Example

$$\begin{array}{rccl} f: & E_{51} & \to & E_9 \\ & (x,y) & \mapsto & \Big(\frac{x^3-183x^2+73x+30}{(x+118)^2}, \\ & & & y\frac{x^3-65x^2-104x+174}{(x+118)^3}\Big). \end{array}$$

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 $x = -118$.

Elliptic curves and isogenies

Example

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

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 $(x,y) = (-118, \pm 51)$.

Elliptic curves and isogenies

Example

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

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.

Elliptic curves and isogenies

Example

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

Elliptic curves and isogenies

Example

$$
\begin{array}{rccl}
f: & E_{51} & \to & E_9 \\
 & (x,y) & \mapsto & \Big(\frac{x^3-183x^2+73x+30}{(x+118)^2}, \\
 & & & y\frac{x^3-65x^2-104x+174}{(x+118)^3}\Big).
\end{array}
$$

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

Elliptic curves and isogenies

Example

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

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

Elliptic curves and isogenies

Example

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

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

Elliptic curves and isogenies

Example

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

Elliptic curves and isogenies

Example

$$\begin{array}{llll} f: & E_{51} & \to & E_9 \\ & (x,y) & \mapsto & \Big(\frac{x^3-183x^2+73x+30}{(x+118)^2}, \\ & & & y\frac{x^3-65x^2-104x+174}{(x+118)^3} \Big). \end{array}$$

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

Elliptic curves and isogenies

Example

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

- $\ker(f)$ 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.

Elliptic curves and isogenies

Example

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

- $\ker(f)$ 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.

Elliptic curves and isogenies

Example

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

- $\ker(f)$ 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 $g : E_9 \to E_{51}$ with cyclic kernel generated by $f(Q)$.

Elliptic curves and isogenies

Example

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

- $\ker(f)$ 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 $g : E_9 \to E_{51}$ with cyclic kernel generated by $f(Q)$.
- $g \circ f : E_{51} \to E_{51}$ is the multiplication-by-3 map.

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 $f : E \to E'$ 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 $f : E \to E'$ be an ℓ-isogeny.

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 $f : E \to E'$ 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 $f : E \to E'$ be an ℓ-isogeny. Then there exists a unique (up to isomorphism) ℓ-isogeny $f^\vee : E' \to E$ such that $f^\vee \circ f$ is the multiplication-by-ℓ map on E.

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 $f : E \to E'$ 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 $f : E \to E'$ be an ℓ-isogeny. Then there exists a unique (up to isomorphism) ℓ-isogeny $f^\vee : E' \to E$ 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 $E_9/\mathbb{F}_{419} : y^2 = x^3 + 9x^2 + x$.

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 $f : E \to E'$ 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 $f : E \to E'$ be an ℓ-isogeny. Then there exists a unique (up to isomorphism) ℓ-isogeny $f^\vee : E' \to E$ 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 $f : E_{51} \to E_9$ with kernel generated by $(-118, 51)$ is the 3-isogeny $f^\vee : E_9 \to E_{51}$ with kernel generated by $(286, 107\sqrt{380})$.

Isogeny graphs

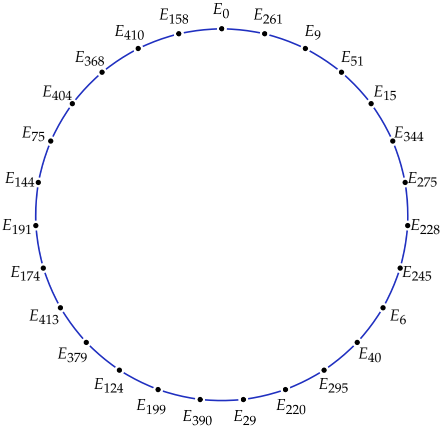
Graph of 3-isogenies over $\mathbb{F}_{419}$.

Example

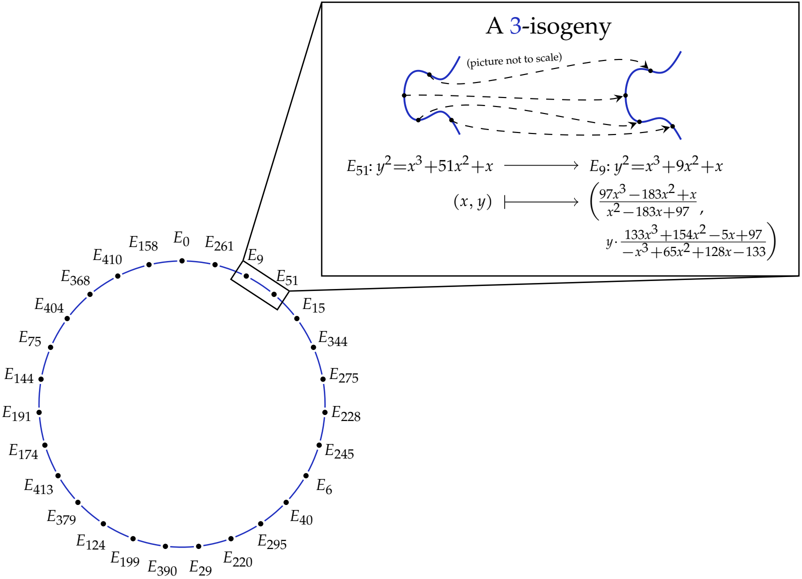
Isogeny graphs

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

Example



Isogeny graphs



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 $E - E'$ respresents an ℓ-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

Isogeny graphs

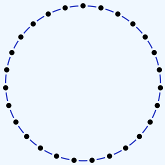
Definition

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 $E - E'$ respresents an ℓ-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

- In our example

G_3:



Isogeny graphs

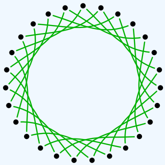
Definition

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 $E - E'$ respresents an ℓ-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

- In our example

G_5:



Isogeny graphs

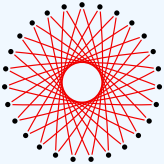
Definition

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 $E - E'$ respresents an ℓ-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

- In our example

G_7:



Isogeny graphs

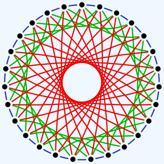
Definition

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 $E - E'$ respresents an ℓ-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

- In our example

$G_3 \cup G_5 \cup G_7$



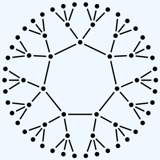
Isogeny graphs

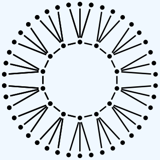
Definition

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 $E - E'$ respresents an ℓ-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

- Generally, the G_ℓ look something like

G_3: 

G_5: 

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 $E \to E$.

Endomorphisms

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

Definition
An endomorphism of an elliptic curve E is a morphism $E \to E$.

Example

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

$$\begin{array}{rccc} [n]: & E & \to & E \\ & (x,y) & \mapsto & n(x,y). \end{array}$$

Endomorphisms

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

Definition

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

Example

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

$$\begin{array}{rccc} [n]: & E & \to & E \\ & (x,y) & \mapsto & n(x,y). \end{array}$$

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

$$\begin{array}{rccc} \pi: & E & \to & E \\ & (x,y) & \mapsto & (x^p, y^p). \end{array}$$

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 $[-p]$.

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 $\mathrm{End}_{\mathbb{F}_p}(E)$.

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 $\mathrm{End}_{\mathbb{F}_p}(E)$.
- We can define a ring homomorphism

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

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 $\mathrm{End}_{\mathbb{F}_p}(E)$.
- We can define a ring homomorphism

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

- 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 $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$.

Group actions

Remember: we wanted to replace exponentiation

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

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

$$H \times S \to S.$$

Group actions

Remember: we wanted to replace exponentiation

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

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

$$H \times S \to S.$$

Now we can do it!

Group actions

Definition

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

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

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

Group actions

Definition

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

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

such that $\mathrm{id} * s = s$ 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.

Group actions

Definition

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

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

such that $\mathrm{id} * s = s$ 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 $\mathbb{Z}[\sqrt{-p}]$.

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 $\mathcal{O}$.

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

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

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 $I = \langle \alpha \rangle$.

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 $J \subset \mathcal{O}$:

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

Class groups

Definition

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

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

[2] modulo details

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 $\mathcal{O}$ is[2]

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

[2] modulo details

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 $\mathcal{O}$ is[2]

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

Miracle fact: the ideal class group is a group!

[2] modulo details

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 $p \geq 5$.

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.

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 $I \subset \mathrm{End}_{\mathbb{F}_p}(E)$ be an ideal. Then

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

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

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 $I \subset \mathrm{End}_{\mathbb{F}_p}(E)$ be an ideal. Then

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

  is a subgroup of $E(\overline{\mathbb{F}_p})$.
- Define $f_I : E \to E'$ to be the isogeny with kernel H_I.

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 $I \subset \mathrm{End}_{\mathbb{F}_p}(E)$ be an ideal. Then

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

  is a subgroup of $E(\overline{\mathbb{F}_p})$.
- Define $f_I : E \to E'$ to be the isogeny with kernel H_I.

The CSIDH group action is:

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

Class group action

The CSIDH group action is:

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

Class group action

The CSIDH group action is:

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

- 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:

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

- 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 $\langle [\ell], \pi - [1] \rangle$.

Class group action

The CSIDH group action is:

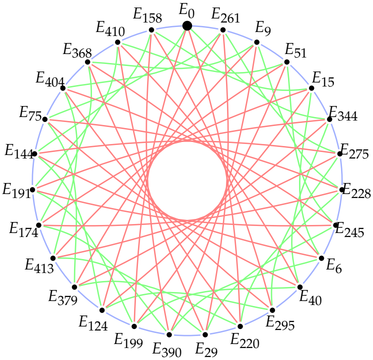
$$\begin{array}{ccc} \mathrm{Cl}(\mathrm{End}_{\mathbb{F}_p}(E)) \times S & \to & S \\ (I, E) & \mapsto & I * E := f_I(E). \end{array}$$

- 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 $\langle [\ell], \pi - [1] \rangle$.
- A $'-'$ direction isogeny on the ℓ-isogeny graph is the action of $\langle [\ell], \pi + [1] \rangle$.

Diffie-Hellman with CSIDH

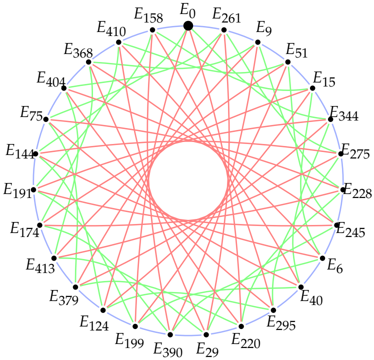
Alice

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



Bob

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



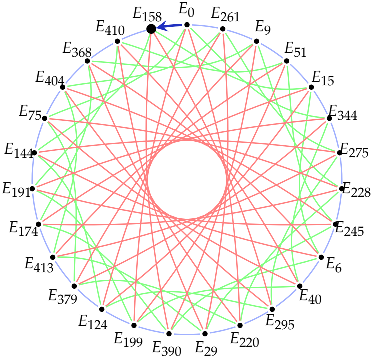
Diffie-Hellman with CSIDH

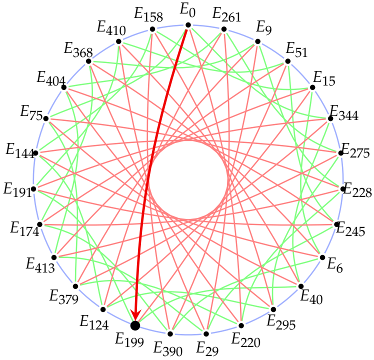
Alice

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

Bob

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





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

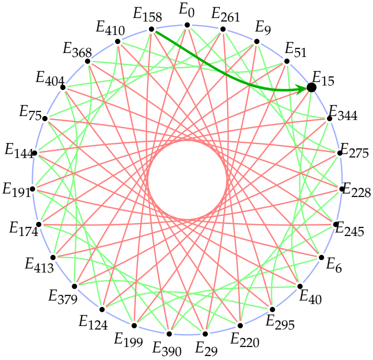
Diffie-Hellman with CSIDH

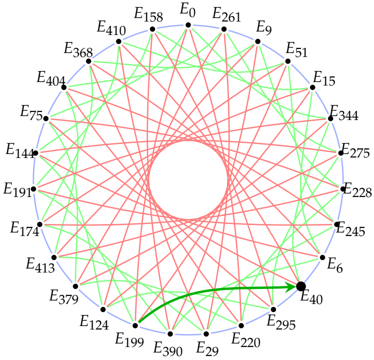
Alice

$$a = [+, \underset{\uparrow}{-}, +, -]$$

Bob

$$b = [+, \underset{\uparrow}{+}, -, +]$$





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

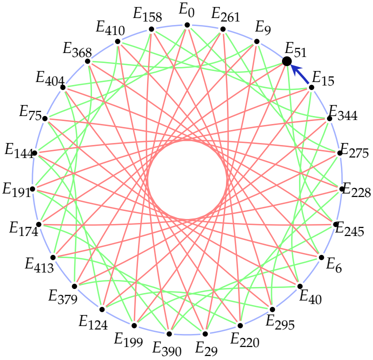
Diffie-Hellman with CSIDH

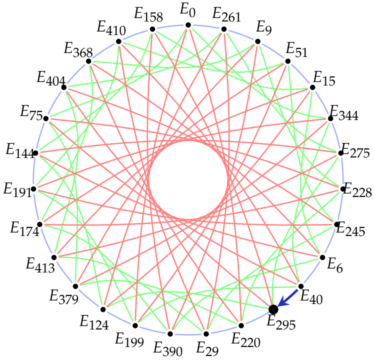
Alice

$$a = [+, -, \underset{\uparrow}{+}, -]$$

Bob

$$b = [+, +, \underset{\uparrow}{-}, +]$$



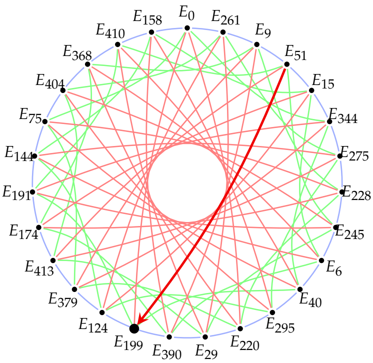


$$E_{15} = \langle 3, \pi - 1 \rangle * E_{51} \quad E_{295} = \langle 3, \pi + 1 \rangle * E_{40}$$

Diffie-Hellman with CSIDH

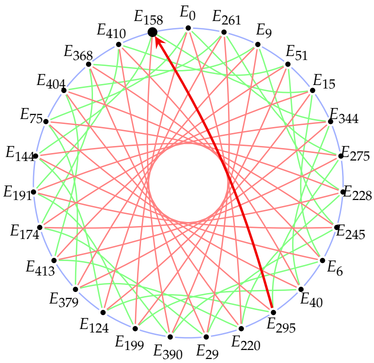
Alice

$$a = [\color{blue}{+}, \color{green}{-}, \color{blue}{+}, \color{red}{-}]$$
$$\uparrow$$



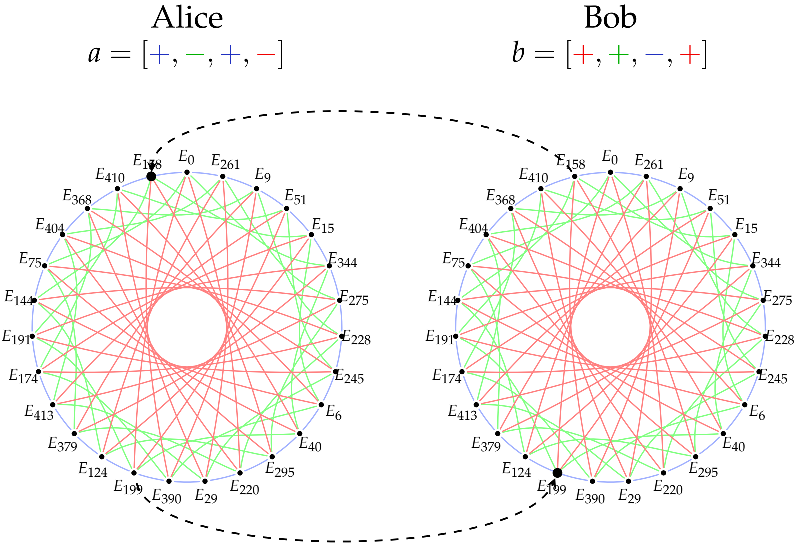
Bob

$$b = [\color{red}{+}, \color{green}{+}, \color{blue}{-}, \color{red}{+}]$$
$$\uparrow$$



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

Diffie-Hellman with CSIDH



(exchange of public keys)

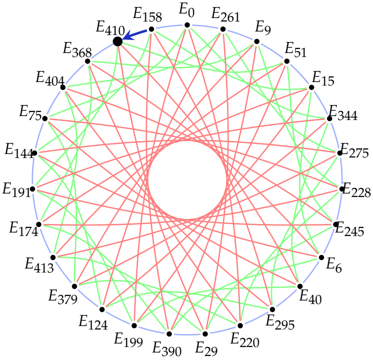
Diffie-Hellman with CSIDH

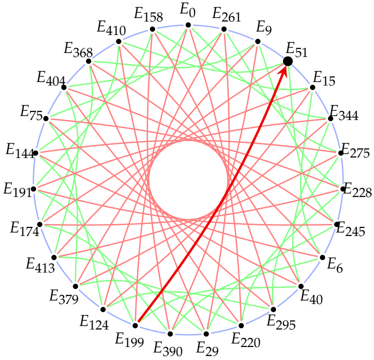
Alice

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

Bob

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

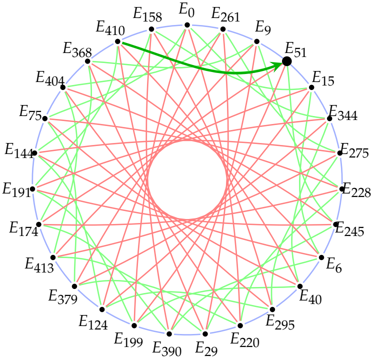


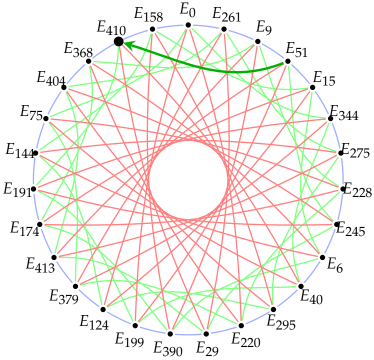


$$E_{410} = \langle 3, \pi - 1 \rangle * E_{158} \quad E_{51} = \langle 7, \pi - 1 \rangle * E_{199}$$

Diffie-Hellman with CSIDH

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



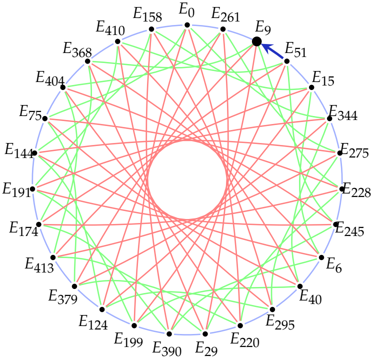


$$E_{51} = \langle 5, \pi + 1 \rangle * E_{410} \quad E_{410} = \langle 5, \pi - 1 \rangle * E_{51}$$

Diffie-Hellman with CSIDH

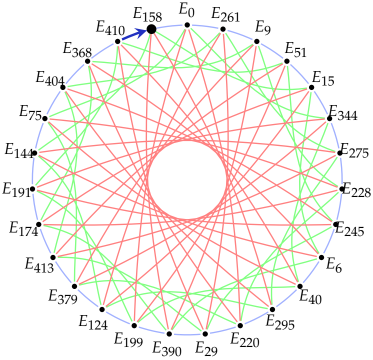
Alice

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



Bob

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

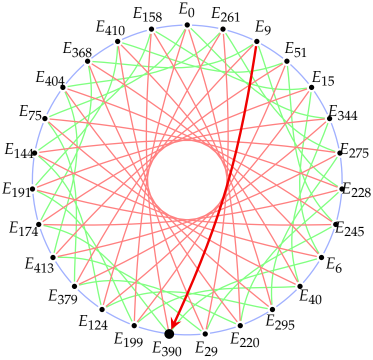


$$E_9 = \langle 3, \pi - 1 \rangle * E_{51} \quad E_{158} = \langle 3, \pi + 1 \rangle * E_{410}$$

Diffie-Hellman with CSIDH

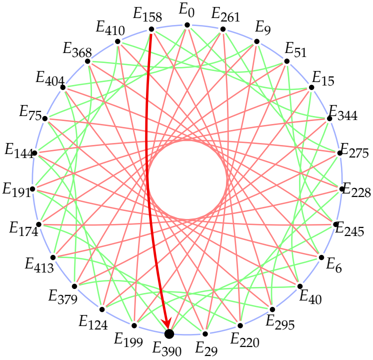
Alice

$a = [+, -, +, \underset{\uparrow}{-}]$



Bob

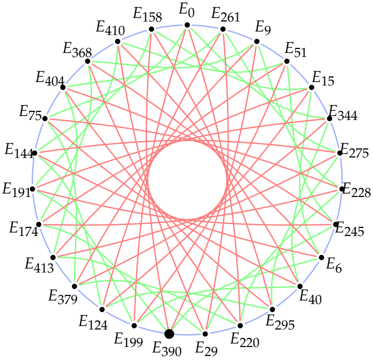
$b = [+, +, -, \underset{\uparrow}{+}]$

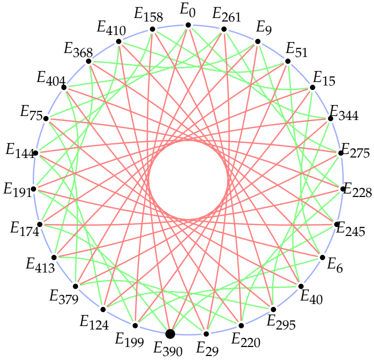


$$E_{390} = \langle 7, \pi + 1 \rangle * E_9 \quad E_{390} = \langle 7, \pi - 1 \rangle * E_{158}$$

Diffie-Hellman with CSIDH

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





(shared secret key is E_{390})

Design choices

- Choose small odd primes $\ell_1, \ldots, \ell_n$.

Design choices

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

Design choices

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

Design choices

- Choose small odd primes $\ell_1, \ldots, \ell_n$.
- 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.

Design choices

- Choose small odd primes $\ell_1, \ldots, \ell_n$.
- 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 $\ell_1, \ldots, \ell_n$.

Design choices

- Choose small odd primes $\ell_1, \ldots, \ell_n$.
- 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 $\ell_1, \ldots, \ell_n$.
- All arithmetic for computing ℓ_i-isogenies is now over $\mathbb{F}_p$. (For more: see David's talk).

Design choices

- Choose small odd primes $\ell_1, \ldots, \ell_n$.
- 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 $\ell_1, \ldots, \ell_n$.
- 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.

Design choices

- Choose small odd primes $\ell_1, \ldots, \ell_n$.
- 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 $\ell_1, \ldots, \ell_n$.
- 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.

Why CSIDH?

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

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)

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

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: $\sim 85\,\text{ms}$ for a full key exchange

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: $\sim 85\,\text{ms}$ for a full key exchange
- Flexible: compatible with 0-RTT protocols such as QUIC; recent preprint uses CSIDH for 'SeaSign' signatures

Work in progress & future work

- Fast, constant-time implementation. For constant-time ideas, see [BLMP].

Work in progress & future work

- Fast, constant-time implementation. For constant-time ideas, see [BLMP].
- More applications.

Work in progress & future work

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


Thank you!

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)

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

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