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

Wouter Castryck\textsuperscript{1}  Tanja Lange\textsuperscript{2}  Chloe Martindale\textsuperscript{2}  
Lorenz Panny\textsuperscript{2}  Joost Renes\textsuperscript{3}

\textsuperscript{1}KU Leuven  \textsuperscript{2}TU Eindhoven  \textsuperscript{3}RU Nijmegen

ECC Autumn School, Osaka, 17-18 November 2018
"six, said"
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 \((G, \ast)\) is a finite group. Examples:

\(\triangleright\ (G, \ast) = (\mathbb{F}_p - \{0\}, \times).\)

\(\triangleright\ (G, \ast) = (E(\mathbb{F}_p), +),\) where \(+\) is the elliptic curve addition that was defined in Mehdi’s lecture.
Traditional Diffie-Hellman key exchange

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

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

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

$$\mathbb{Z} \times G \rightarrow G$$

$$(x, g) \mapsto g \ast \cdots \ast g.$$
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

\[
\mathbb{Z} \times G \rightarrow G \\
(x, g) \mapsto g \ast \cdots \ast g.
\]

Examples:

- \(g \in \mathbb{F}_p - \{0\}\), then \((x, g) \mapsto g^x\).
Traditional Diffie-Hellman key exchange

Suppose that \((G, \ast)\) is a finite group. Examples:

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

For a finite group \((G, \ast)\) we have a map

\[
\mathbb{Z} \times G \rightarrow G \\
(x, g) \mapsto g \ast \cdots \ast g.
\]

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 \((G, \ast)\) is a finite group. Examples:

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

For a finite group \((G, \ast)\) we have a map

\[
\mathbb{Z} \times G \rightarrow G \\
(x, g) \mapsto g \ast \cdots \ast g. \\
x \text{ times}
\]

Examples:

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

For simplicity, for a finite group \((G, \ast)\) and \(x \in \mathbb{Z}\), we’ll write \(g^x\) for \(g \ast \cdots \ast g\) \(x \text{ times}\).
Traditional Diffie-Hellman key exchange

For a finite group \((G, \ast)\), if \(g \in G\) and \(x \in \mathbb{Z}\), we write
\[ g^x = g \ast \cdots \ast g. \]
Traditional Diffie-Hellman key exchange

For a finite group \((G, \ast)\), if \(g \in G\) and \(x \in \mathbb{Z}\), we write
\[
g^x = g \ast \cdots \ast g. \quad \text{\textit{x times}}
\]

\(a \in \mathbb{Z}\)

\(g \in G\)

\(b \in \mathbb{Z}\)
Traditional Diffie-Hellman key exchange

For a finite group \((G, \ast)\), if \(g \in G\) and \(x \in \mathbb{Z}\), we write
\[
g^x = g \ast \cdots \ast g.
\]

\(\underbrace{\ast \cdots \ast}_{x \text{ times}}\)

\(a \in \mathbb{Z}\)

\(g \in G\)

\(g^a \rightarrow g^b \leftarrow b \in \mathbb{Z}\)
Traditional Diffie-Hellman key exchange

For a finite group \((G, \ast)\), if \(g \in G\) and \(x \in \mathbb{Z}\), we write
\[ g^x = g \ast \cdots \ast g. \]

\(x\) times

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

\[ g \in G \]
\[ g^a \]
\[ \rightarrow \]
\[ g^b \]
\[ \leftarrow \]

\[ b \in \mathbb{Z} \]
\[ (g^a)^b \]
Traditional Diffie-Hellman key exchange

For a finite group \((G, \ast)\), if \(g \in G\) and \(x \in \mathbb{Z}\), we write \(g^x = g \ast \cdots \ast g\).
Traditional Diffie-Hellman key exchange

For a finite group \((G, \ast)\), if \(g \in G\) and \(x \in \mathbb{Z}\), we write
\[
g^x = g \ast \cdots \ast g.
\]
\(x\) times

\[a \in \mathbb{Z}\]

\((g^b)^a\)

\[g \in G\]

\[g^a\]

\[
\rightarrow
\]

\[g^b\]

\[
\leftarrow
\]

\[b \in \mathbb{Z}\]

\((g^a)^b\)

\[k = (g^a)^b = g^{a \cdot b} = g^{b \cdot a} = (g^b)^a.\]

\[\text{Computing } a \text{ or } b \text{ given } g^a \text{ and } g^b \text{ should be hard (i.e. slow).}\]
Traditional Diffie-Hellman key exchange

For a finite group \((G, \ast)\), if \(g \in G\) and \(x \in \mathbb{Z}\), we write
\[
g^x = g \ast \cdots \ast g.
\]

\[
a \in \mathbb{Z} \quad \rightarrow \quad (g^b)^a
\]

\[
g \in G
\]

\[
g^a \quad \rightarrow \quad g^b
\]

\[
b \in \mathbb{Z} \quad \leftarrow \quad (g^a)^b
\]

\[\quad \]

\[\blacktriangleright \] \(k = (g^a)^b = g^{a \cdot b} = g^{b \cdot a} = (g^b)^a\).

\[\blacktriangleright \] Computing \(a\) or \(b\) given \(g^a\) and \(g^b\) should be hard (i.e. slow).

\[\blacktriangleright \] 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 $g^{13}$. 

\[
\begin{align*}
g^0 & \quad g^1 & \quad g^2 & \quad g^3 & \quad g^4 & \quad g^5 & \quad g^6 & \quad g^7 & \quad g^8 & \quad g^9 & \quad g^{10} & \quad g^{11} & \quad g^{12} & \quad g^{13} & \quad g^{14} & \quad g^{15} & \quad g^{16} & \quad g^{17} & \quad g^{18} & \quad g^{19} & \quad g^{20} & \quad g^{21} & \quad g^{22} & \quad g^{23} \\
1 & \quad 2 & \quad 4 & \quad 8 & \quad 16 & \quad 32 & \quad 64 & \quad 128 & \quad 256 & \quad 512 & \quad 1024 & \quad 2048 & \quad 4096 & \quad 8192 & \quad 16384 & \quad 32768 & \quad 65536 & \quad 131072 & \quad 262144 & \quad 524288 & \quad 1048576 & \quad 2097152 & \quad 4194304 & \quad 8388608 & \quad 16777216 \\
\end{align*}
\]
Square-and-multiply

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

![Diagram showing the computation of $g^{13}$ in a group of order 23, with powers of $g$ from 0 to 22 displayed in a ring structure. The computation path is indicated by arrows connecting $g^0$ to $g^{13}$. ]
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 (naive) 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).

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).
Alice uses the knowledge that 
\[ 13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \] 
to compute \( g^{13} \).
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) 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) 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

$$\mathbb{Z} \times G \rightarrow G$$

$$(x, g) \mapsto g^x := g \ast \cdots \ast g.$$  

$x$ times

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

$$
\mathbb{Z} \times G \to G \\
(x, g) \mapsto g^x := g \ast \cdots \ast g. \quad (x \text{ times})
$$

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

$$
\mathbb{Z} \times G \rightarrow G \\
(x, g) \mapsto g^x := g \ast \cdots \ast g. \quad \text{x times}
$$

Alice can compute $g^x$ in polynomial time.

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

$\Rightarrow$ Idea:

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

$$
H \times S \rightarrow S.
$$
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: \([\text{right, then left}] = [\text{left, then right}]\), etc.
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:
\[ g^{13} = g^0, \text{ etc.} \]
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^* g^0 \]

, etc.
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^4 \ast g \ast g^0 \], etc.
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 * g^4 * g^0 \]

, etc.
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g \cdot g^0 = g^0, \text{ etc.} \]
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g \cdot g^0 = g^8 \cdot g^0 \], etc.
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g^0 = g^4 \cdot g^8 \cdot g^0, \text{ etc.} \]
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g \cdot g^0 = g \cdot g^4 \cdot g^8 \cdot g^0 \], etc.
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g \cdot g^0 = g \cdot g^4 \cdot g^8 \cdot g^0 = g^0, \text{ etc.} \]
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g \cdot g^0 = g \cdot g^4 \cdot g^8 \cdot g^0 = g^4 \cdot g^0, \text{ etc.} \]
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g^0 = g \cdot g^4 \cdot g^8 \cdot g^0 = g \cdot g^4 \cdot g^0, \text{ etc.} \]
What do we keep from traditional (EC)DH?

Cycles are compatible:
\[ g^{13} = g^8 \cdot g^4 \cdot g \cdot g^0 = g \cdot g^4 \cdot g^8 \cdot g^0 = g^8 \cdot g \cdot g^4 \cdot g^0, \text{ etc.} \]
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

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

\[ \begin{array}{c}
E_0 \\
E_9 \\
E_51 \\
E_261 \\
E_0_{158}
\end{array} \]

Bob

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

\[ \begin{array}{c}
E_0 \\
E_9 \\
E_51 \\
E_261 \\
E_0_{158}
\end{array} \]
Diffie-Hellman on ‘nice’ graphs

Alice

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

Bob

\[ b = [+, +, -, +] \]
Diffie-Hellman on ‘nice’ graphs

Alice

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

Bob

\[ b = [+, +, -, +] \]
Diffie-Hellman on ‘nice’ graphs

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

Bob
\[ b = [+, +, -, +] \]
Diffie-Hellman on ‘nice’ graphs

Alice

\[ a = \{+, -, +, -\} \]

Bob

\[ b = \{+, +, -, +\} \]
Diffie-Hellman on ‘nice’ graphs

Alice

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

Bob

\[ b = [+, +, -, +] \]
Diffie-Hellman on ‘nice’ graphs

Alice

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

Bob

$$b = [+ , + , - , +]$$
Diffie-Hellman on ‘nice’ graphs

Alice

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

Bob

\[ b = [+,+,−,+] \]
Diffie-Hellman on ‘nice’ graphs

**Alice**

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

**Bob**

\[ b = [+, +, -, +] \]
Diffie-Hellman on ‘nice’ graphs

Alice

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

Bob

\[ b = [+, +, -, +] \]
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 $P_\infty$ 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

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’.

Example

Define $E/\mathbb{F}_5 : y^2 = x^3 + 1$. Then $E(\mathbb{F}_5) = \{(0,1), (0,-1), (2,3), (2,-3), (-1,0)\}$.
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 $\text{deg}(f) = 3$ with a ‘point at infinity’.

- There is a geometric group law called $+$ on the rational points of $E$. 

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

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 $P_\infty$ 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

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

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

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

$$= \{P, 2P, \}.$$
Elliptic curves

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

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

$$= \{P, 2P, 4P\}.$$
Elliptic curves

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

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

\[ = \{P, 2P, 3P\} \]
Elliptic curves

- $E : y^2 = x^3 + 1$.
- Recall
  
  $E(\mathbb{F}_5) = \{(2, 3), (0, -1), (-1, 0), (0, 1), (2, -3), P_\infty\}$.
  
  $= \{P, 2P, 3P, \}$.
Elliptic curves

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

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

$= \{P, 2P,\allowbreak 3P, 4P,\}$
Elliptic curves

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

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

$$= \{P, 2P, \quad 3P, 4P, \quad 2P, 3P, 4P\}.$$
Elliptic curves

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

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

$$= \{P, 2P, 3P, 4P, 5P, \}.$$
Elliptic curves

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

\[
E(\mathbb{F}_5) = \{(2, 3), (0, -1), (-1, 0), (0, 1), (2, -3), P_\infty\}.
= \{P, 2P, 3P, 4P, 5P\}.
\]
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

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

$$= \{P, 2P, 3P, 4P, 5P, 6P\}.$$

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

![Graph of an elliptic curve with points marked at (2,3), (0,-1), (-1,0), (0,1), (2,-3), and the origin.]
Elliptic curves

Example

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

Example

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

Definition

An elliptic curve \( E \) defined over a finite prime field \( \mathbb{F}_p \) with \( p \geq 5 \) is \textit{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

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

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

Example
$E(\mathbb{F}_p) \cong \mathbb{C}_p + 1$; generated by a point $P$ of order $p+1$, or $E(\mathbb{F}_p) \cong \mathbb{C}_2 \times \mathbb{C}_{(p+1)/2}$ and contains a point $P$ of order $(p+1)/2$.

In either case, if $\ell | (p+1)$ is an odd prime, then $p+1/\ell P$ is a point of order $\ell$. 

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 $P = (2, 3)$. 
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 \emph{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 \( P = (2, 3) \).

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

\( \triangleright \) \( (-1, 0) = 3(2, 3) \) 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 \textit{n-torsion point} if \( nP = P_{\infty} \). An \( n \)-torsion point \( P \) is a \textit{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 \( (p+1)/2 \).
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 $\ell$. 
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 $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

$$[2] : E_{51} \to E_{51}$$
$$(x, y) \mapsto 2 \cdot (x, y) := (x, y) + (x, y)$$
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 $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

\[
[2] : \quad E_{51} \to E_{51} \\
(x, y) \mapsto 2 \cdot (x, y) := (x, y) + (x, y)
\]

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

$$[2] : E_{51} \to E_{51}
(x, y) \mapsto 2 \cdot (x, y) := (x, y) + (x, y)$$
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 $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

\[
[2] : E_{51} \rightarrow E_{51}
\]
\[
(x, y) \mapsto 2 \cdot (x, y) := (x, y) + (x, y)
\]

- $[2](P_\infty) = P_\infty + P_\infty = P_\infty$. 
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 $E_{51}/\mathbb{F}_{419} : y^2 = x^3 + 51x^2 + x$

\[
[2] : \quad E_{51} \quad \to \quad E_{51}
\]
\[
(x, y) \quad \mapsto \quad 2 \cdot (x, y) := (x, y) + (x, y)
\]

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

$$[2] : \quad E_{51} \quad \to \quad E_{51}$$

$$(x, y) \mapsto \left( \frac{\frac{1}{2} x^4 - 18 x^3 - 163 x^2 - 18 + \frac{1}{2}}{8 x (x^2 + 9 x + 1)}, \frac{y (x^6 + 18 x^5 + 5 x^4 - 5 x^2 - 18 x - 1)}{(8 x (x^2 + 9 x + 1))^2} \right).$$

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

$$f : \quad E_{51} \to E_{9}$$

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

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

is an isogeny.
Elliptic curves and isogenies

Example

\[ f : \quad E_{51} \rightarrow E_9 \]
\[ (x, y) \mapsto \left( \frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \]
\[ \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right). \]
Elliptic curves and isogenies

Example

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

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

- If \((x, y) \in \ker(f)\) then \((x, y) = P_\infty \) or \( x = -118 \).
Elliptic curves and isogenies

Example

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

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

- 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

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

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

- 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

\[ f : \quad E_{51} \quad \rightarrow \quad E_9 \]

\[ (x, y) \quad \mapsto \quad \left( \frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2} , \right. \]

\[ \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right) . \]
Elliptic curves and isogenies

Example

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

\[ \ker(f) = \{(-118, 51), (-118, -51), P_\infty\}. \]
Elliptic curves and isogenies

Example

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

\[ \text{ker}(f) = \{ (-118, 51), (-118, -51), P_{\infty} \}. \]

\[ \text{ker}(f) \text{ is a subgroup of } E_{51}(\overline{\mathbb{F}_{419}}) \text{ (because } f \text{ induces a morphism of groups)}. \]
Elliptic curves and isogenies

Example

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

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

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

Example

\[ f : \quad E_{51} \quad \rightarrow \quad E_9 \]
\[ (x, y) \quad \mapsto \quad \left( \frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \right. \]
\[ \left. y \frac{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right) . \]
Elliptic curves and isogenies

Example

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

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

Example

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

- \( \ker(f) \) 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.
Elliptic curves and isogenies

Example

\[ f : E_{51} \to E_9 \]
\[ (x, y) \mapsto \left( \frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \frac{y}{(x+118)^3} \right). \]

- \( \ker(f) \) 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 \( E_9 \).
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.
- 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 \( f(Q) \).
Elliptic curves and isogenies

Example

\[ f : \quad E_{51} \rightarrow E_{9} \]
\[ (x, y) \mapsto \left( \frac{x^3 - 183x^2 + 73x + 30}{(x+118)^2}, \frac{y}{x^3 - 65x^2 - 104x + 174}{(x+118)^3} \right). \]

- \( \ker(f) \) 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.
Elliptic curves and isogenies

Definition
Let $E, E' / \mathbb{F}_p$ be elliptic curves and let $\ell$ be a prime different from $p$. An $\ell$-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 $\ell$-isogeny.
Elliptic curves and isogenies

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

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 $(286, 107\sqrt{380})$. 

23 / 40
Elliptic curves and isogenies

Definition
Let $E, E'/\mathbb{F}_p$ be elliptic curves and let $\ell$ be a prime different from $p$. An $\ell$-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 $\ell$-isogeny. Then there exists a unique (up to isomorphism) $\ell$-isogeny $f^\vee : E' \to E$ such that $f^\vee \circ f$ is the multiplication-by-$\ell$ 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 $\ell$ be a prime different from $p$. An $\ell$-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 $\ell$-isogeny. Then there exists a unique (up to isomorphism) $\ell$-isogeny $f^\vee : E' \to E$ such that $f^\vee \circ f$ is the multiplication-by-$\ell$ 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

$E_{51} \leftrightarrow E_9$   $E_{51} \rightarrow E_9$
Isogeny graphs
Graph of 3-isogenies over $\mathbb{F}_{419}$.
Example
Isogeny graphs

A 3-isogeny

\[ E_{51}: y^2 = x^3 + 51x^2 + x \quad \rightarrow \quad E_9: y^2 = x^3 + 9x^2 + x \]

\[(x, y) \quad \rightarrow \quad \left( \frac{97x^3 - 183x^2 + x}{x^2 - 183x + 97}, \frac{133x^3 + 154x^2 - 5x + 97}{-x^3 + 65x^2 + 128x - 133} \right) \]
Isogeny graphs

**Definition**
Let $p$ and $\ell$ be distinct primes. The isogeny graph $G_\ell$ 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 $\ell$-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.
Isogeny graphs

Definition
Let $p$ and $\ell$ be distinct primes. The isogeny graph $G_\ell$ 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 $E \to E'$ respresents an $\ell$-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 $\ell$ be distinct primes. The isogeny graph $G_{\ell}$ 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 $E \rightarrow E'$ respresents an $\ell$-isogeny $E \rightarrow E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

In our example

$G_5$: 

![Diagram of the isogeny graph $G_5$]
Isogeny graphs

Definition
Let $p$ and $\ell$ be distinct primes. The isogeny graph $G_\ell$ 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 $E \rightarrow E'$ respresents an $\ell$-isogeny $E \rightarrow E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

- In our example


$G_7$:
Isogeny graphs

Definition
Let $p$ and $\ell$ be distinct primes. The isogeny graph $G_\ell$ 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 $E \rightarrow E'$ respresents an $\ell$-isogeny $E \rightarrow E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

In our example
Isogeny graphs

Definition
Let $p$ and $\ell$ be distinct primes. The isogeny graph $G_\ell$ 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 $E \to E'$ respresents an $\ell$-isogeny $E \to E'$ defined over $\mathbb{F}_p$ together with its dual isogeny.

- Generally, the $G_\ell$ look something like

\[ G_3: \quad G_5: \]
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 $E \rightarrow E$. 
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

$$[n] : E \to E \quad (x, y) \mapsto n(x, y).$$
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

\[
[n] : \quad E \rightarrow E \\
(x, y) \mapsto n(x, y).
\]

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

\[
\pi : \quad E \rightarrow E \\
(x, y) \mapsto (x^p, y^p).
\]
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 $[-p]$. 

Fact: if $p \equiv 3 \pmod{8}$, $p \geq 5$, and $E_{\mathbb{A}}/\mathbb{F}_p$:

$$y^2 = x^3 + Ax^2 + x$$

is supersingular, then $\text{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$. 
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 $\text{End}_{\mathbb{F}_p}(E)$. 

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

$$\mathbb{Z}[^{\sqrt{}}-p] \to \text{End}_{\mathbb{F}_p}(E)$$

$$n \mapsto [n]$$

$$\sqrt{-p} \mapsto \pi.$$
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

$$
\mathbb{Z}[\sqrt{-p}] \to \text{End}_{\mathbb{F}_p}(E)
$$

$$
n \mapsto [n]
$$

$$
\sqrt{-p} \mapsto \pi.
$$

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

Remember: we wanted to replace exponentiation

\[ \mathbb{Z} \times G \rightarrow G \]
\[ (x, g) \mapsto g^x := g \cdot \cdots \cdot g \]

by a group action of a group \( H \) on a set \( S \):

\[ H \times S \rightarrow S. \]
Group actions

Remember: we wanted to replace exponentiation

\[ \mathbb{Z} \times G \rightarrow G \]
\[ (x, g) \mapsto g^x := g \ast \cdots \ast g. \]

by a group action of a group \( H \) on a set \( S \):

\[ H \times S \rightarrow S. \]

Now we can do it!
**Group actions**

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

\[
H \times S \rightarrow S
\]

\[
(h, s) \mapsto h \ast s
\]

such that \(\text{id} \ast s = s\) and \(h_1 \ast (h_2 \ast s) = (h_1 \cdot h_2) \ast s\) 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

\[
H \times S \rightarrow S \\
(h, s) \mapsto h \ast s
\]

such that \(\text{id} \ast s = s\) and \(h_1 \ast (h_2 \ast s) = (h_1 \cdot h_2) \ast s\) 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

\[
H \times S \rightarrow S \\
(h, s) \mapsto h \ast s
\]

such that \(\text{id} \ast s = s\) and \(h_1 \ast (h_2 \ast s) = (h_1 \cdot h_2) \ast s\) 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

$$\langle \alpha \rangle \cdot I = \langle \beta \rangle \cdot J.$$
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\(^2\)

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

\(^2\text{modulo details}\)
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

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

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 $E_A/F_p : y^2 = x^3 + Ax^2 + x$ with $p \equiv 3 \pmod{8}$ and $p \geq 5$. How?

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

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

is a subgroup of $E(\overline{F}_p)$.
Class group action

The class group of the endomorphism ring \( \mathbb{Z}[\sqrt{-p}] \) acts on the set \( S \) of supersingular elliptic curves \( E_{A/F_p} : y^2 = x^3 + Ax^2 + x \) 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

\[
H_I = \bigcap_{\alpha \in I} \ker(\alpha)
\]

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 \( p \equiv 3 \) (mod 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
  \[
  H_I = \bigcap_{\alpha \in I} \ker(\alpha)
  \]
  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:

\[
\text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S \to S
\]

\[
(I, E) \mapsto f_I(E).
\]
The CSIDH group action is:

\[
\text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S \rightarrow S \\
(I, E) \mapsto I \ast E := f_I(E).
\]
Class group action

The CSIDH group action is:

\[
\text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S \rightarrow S
\]

\[
(I, E) \mapsto I \ast E := f_I(E).
\]

- The isogeny \(f_I\) is an \(\ell\)-isogeny if and only if \(I = \langle [\ell], \pi \pm [1] \rangle\).
Class group action

The CSIDH group action is:

\[
\text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S \to S
\]

\[ (I, E) \mapsto I \ast E := f_I(E). \]

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

The CSIDH group action is:

$$\text{Cl}(\text{End}_{\mathbb{F}_p}(E)) \times S \rightarrow S$$

$$(I, E) \quad \mapsto \quad I \ast E := f_I(E).$$

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

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

Bob
\[ b = [+, +, -, +] \]
Diffie-Hellman with CSIDH

Alice

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

Bob

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

\[
E_{158} = \langle 3, \pi - 1 \rangle \ast E_0 \quad E_{199} = \langle 7, \pi - 1 \rangle \ast E_0
\]
Diffie-Hellman with CSIDH

Alice

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

Bob

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

$$E_{15} = \langle 5, \pi + 1 \rangle \ast E_{158}$$

$$E_{40} = \langle 5, \pi - 1 \rangle \ast E_{199}$$
Diffie-Hellman with CSIDH

Alice

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

Bob

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

\[ E_{15} = \langle 3, \pi - 1 \rangle \cdot E_{51} \quad E_{295} = \langle 3, \pi + 1 \rangle \cdot E_{40} \]
Diffie-Hellman with CSIDH

Alice

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

Bob

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

\[ E_{199} = \langle 7, \pi + 1 \rangle \ast E_{51} \]

\[ E_{158} = \langle 7, \pi - 1 \rangle \ast E_{295} \]
Diffie-Hellman with CSIDH

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

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

(exchange of public keys)
Diffie-Hellman with CSIDH

Alice

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

Bob

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

\[ E_{410} = \langle 3, \pi - 1 \rangle \ast E_{158} \quad E_{51} = \langle 7, \pi - 1 \rangle \ast E_{199} \]
Diffie-Hellman with CSIDH

Alice

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

Bob

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

\[ E_{51} = \langle 5, \pi + 1 \rangle \ast E_{410} \]

\[ E_{410} = \langle 5, \pi - 1 \rangle \ast E_{51} \]
Diffie-Hellman with CSIDH

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

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

\[ E_9 = \langle 3, \pi - 1 \rangle \cdot E_{51} \quad E_{158} = \langle 3, \pi + 1 \rangle \cdot E_{410} \]
Diffie-Hellman with CSIDH

Alice

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

Bob

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

\[ E_{390} = \langle 7, \pi + 1 \rangle \ast E_9 \quad E_{390} = \langle 7, \pi - 1 \rangle \ast E_{158} \]
Diffie-Hellman with CSIDH

Alice

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

Bob

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

(shared secret key is \( E_{390} \))
Design choices

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

- Make sure $p = 4 \cdot \ell_1 \cdot \cdots \cdot \ell_n - 1$ is prime.

- Fix $E_0 / F_p$: $y^2 = x^3 + x$.

- Then $E_0$ is supersingular.

- Exercise: show that there is a point of order $\ell_i$ in $E_0(F_p)$ for every $\ell_1, \ldots, \ell_n$.

- All arithmetic for computing $\ell_i$-isogenies is now over $F_p$.

- (For more: see David’s talk).

- Every $G_{\ell_i}$ containing $E_0$ is a disjoint union of cycles.

- Every node of $G_{\ell_i}$ is of the form $E_A$: $y^2 = x^3 + Ax^2 + x$ can be compressed to just $A \in F_p$ giving tiny keys.
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 $E_0/\mathbb{F}_p : y^2 = x^3 + x$. 

Then $E_0$ is supersingular. Exercise: show that there is a point of order $\ell_i$ in $E_0(\mathbb{F}_p)$ for every $\ell_1, \ldots, \ell_n$.

All arithmetic for computing $\ell_i$-isogenies is now over $\mathbb{F}_p$. (For more: see David's talk).

Every $G_{\ell_i}$ containing $E_0$ is a disjoint union of cycles.

Every node of $G_{\ell_i}$ 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.
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 $E_0/F_p : y^2 = x^3 + x$.
- Then $E_0$ is supersingular. Exercise: show that there is a point of order $\ell_i$ in $E_0(F_p)$ for every $\ell_1, \ldots, \ell_n$. 

All arithmetic for computing $\ell_i$-isogenies is now over $F_p$ (For more: see David’s talk).

Every $G_{\ell_i}$ containing $E_0$ is a disjoint union of cycles.

Every node of $G_{\ell_i}$ is of the form $E_A : y^2 = x^3 + Ax^2 + x$ can be compressed to just $A \in F_p$ giving tiny keys.
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 $\ell_i$ in $E_0(\mathbb{F}_p)$ for every $\ell_1, \ldots, \ell_n$.
- All arithmetic for computing $\ell_i$-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 $\ell_i$ in $E_0(\mathbb{F}_p)$ for every $\ell_1, \ldots, \ell_n$.
- All arithmetic for computing $\ell_i$-isogenies is now over $\mathbb{F}_p$. (For more: see David’s talk).
- Every $G_{\ell_i}$ 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 $E_0/F_p : y^2 = x^3 + x$.

Then $E_0$ is supersingular. Exercise: show that there is a point of order $\ell_i$ in $E_0(F_p)$ for every $\ell_1, \ldots, \ell_n$.

- All arithmetic for computing $\ell_i$-isogenies is now over $F_p$. (For more: see David’s talk).

- Every $G_{\ell_i}$ containing $E_0$ is a disjoint union of cycles.
- Every node of $G_{\ell_i}$ is of the form $E_A : y^2 = x^3 + Ax^2 + x$ can be compressed to just $A \in F_p$ 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 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: ~85 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!
Mentioned in this talk:

- Castryck, Lange, Martindale, Panny, Renes:
  *CSIDH: An Efficient Post-Quantum Commutative Group Action*

- [BLMP] Bernstein, Lange, Martindale, Panny:
  *Quantum circuits for the CSIDH: optimizing quantum evaluation of isogenies*

- 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*

- 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 $\mathbb{F}_p$*

- De Feo, Kieffer, Smith:
  *Towards practical key exchange from ordinary isogeny graphs*

- 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*

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

<table>
<thead>
<tr>
<th>CSIDH-log $p$</th>
<th>intended NIST level</th>
<th>public key size</th>
<th>private key size</th>
<th>time (full exchange)</th>
<th>cycles (full exchange)</th>
<th>stack memory</th>
<th>classical security</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSIDH-512</td>
<td>1</td>
<td>64 b</td>
<td>32 b</td>
<td>85 ms</td>
<td>212e6</td>
<td>4368 b</td>
<td>128</td>
</tr>
<tr>
<td>CSIDH-1024</td>
<td>3</td>
<td>128 b</td>
<td>64 b</td>
<td></td>
<td></td>
<td></td>
<td>256</td>
</tr>
<tr>
<td>CSIDH-1792</td>
<td>5</td>
<td>224 b</td>
<td>112 b</td>
<td></td>
<td></td>
<td></td>
<td>448</td>
</tr>
</tbody>
</table>