SUPERSINGULAR ISOGENY KEY EXCHANGE

Marek Hubbell

14.01.2021

How do we digitally exchange keys in the age of quantum computers?

Diffie Hellman

$$
\begin{tikzcd}
g \arrow[r, "\hat{\ } a"] \arrow[d, "\hat{\ } b"'] & g^{a} \arrow[d, "\hat{\ } b"] \\
g^{b} \arrow[r, "\hat{\ } a"'] & g^{ab}
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
? \arrow[r, "?"] \arrow[d, "?"'] & ? \arrow[d, "?"] \\
? \arrow[r, "?"'] & ?
\end{tikzcd}
$$

Target Field

Our extension field is as follows:

- $\mathbb{F}_p$ with $p \equiv 3 \, mod \, 4$

Target Field

Our extension field is as follows:

- $\mathbb{F}_p$ with $p \equiv 3 \, mod \, 4$
- represented as $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 + 1 = 0$

Target Field

Our extension field is as follows:

- $\mathbb{F}_p$ with $p \equiv 3 \, mod \, 4$
- represented as $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 + 1 = 0$
- all elements are $u + vi$ where $u, v \in \mathbb{F}_p$

Target Field

Our extension field is as follows:

- $\mathbb{F}_p$ with $p \equiv 3 \, mod \, 4$
- represented as $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 + 1 = 0$
- all elements are $u + vi$ where $u, v \in \mathbb{F}_p$

We are only interested in $\lfloor p/12 \rfloor + z$ where $z \in \{0, 1, 2\}$

j-invariants

using elliptic curves in *Montgomery form*:

$$E_a : y^2 = x^3 + ax^2 + x$$

j-invariants

using elliptic curves in *Montgomery form*:

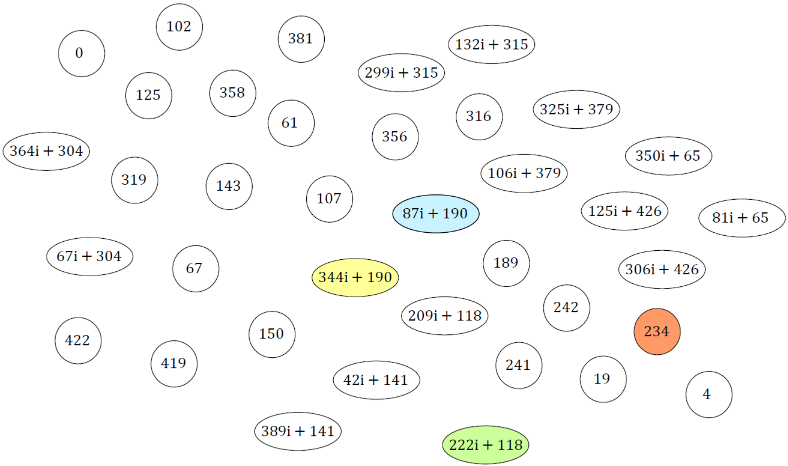
$$E_a : y^2 = x^3 + ax^2 + x$$

has the j-invariant:

$$j\left(E_a\right) = \frac{256(a^2-3)^3}{(a^2-4)}$$

There are multiple a values that correspond to the same j-invariant

j-invariants



j-invariants in $\mathbb{F}_{431^2}$

source: https://eprint.iacr.org/2019/1321.pdf

j-invariant

$$\begin{tikzcd}
j(E) \arrow[r, "?"] \arrow[d, "?"'] & j(E_a) \arrow[d, "?"] \\
j(E_b) \arrow[r, "?"'] & j(E_{ab})
\end{tikzcd}$$

Supersingular curves

Torsion Group

Definition

Torsion Points Let $n \in \mathbb{N}$. The set of n-torsion points of the group E is denoted by

$$E[n] = \{P \in E : [n]P = O\}.$$

Note that this set is the kernel of the multiplication-by-n map.

Supersingular curves

Torsion Group

Definition

Torsion Points Let $n \in \mathbb{N}$. The set of n-torsion points of the group E is denoted by

$$E[n] = \{P \in E : [n]P = O\}.$$

Note that this set is the kernel of the multiplication-by-n map.

Suprersingular Curves

Definition (Supersingular)

An elliptic curve E over a finite field $\mathbb{F}_q$ is called supersingular, if $\mathrm{char}(\mathbb{F}_q)$ divides $t = q + 1 - \#E(\mathbb{F}_q)$.

Supersingular curves

Torsion Group

Definition

Torsion Points Let $n \in \mathbb{N}$. The set of n-torsion points of the group E is denoted by

$$E[n] = \{P \in E : [n]P = O\}.$$

Note that this set is the kernel of the multiplication-by-n map.

Simplest definition:

$$\text{p-tortion in } \mathbb{F}_{p^2}: \quad E[p] = 0$$

These curves have some nice properties, like their j-invariants always being in $\mathbb{F}_{p^2}$:

Maps

Using Montgomery form $E_a : y^2 = x^3 + ax^2 + x$, we can do x-only arithmetic, map on the same curve or from one curve to another:

$$x \mapsto f(x)$$

or more fully:

$$(x, y) \mapsto (f(x), c \cdot yf'(x))$$

where f' is the derivative of f

Isogeny definition

An Isogeny is simply a map:

$$\phi : E \to E'$$

Maps

Point doubling using Montgomery form:

$$x \mapsto \frac{(x^2-1)^2}{4x(x^2+ax+1)}$$

Maps

Point doubling using Montgomery form:

$$x \mapsto \frac{(x^2-1)^2}{4x(x^2+ax+1)}$$

The denominator here determines which points are of order 2, these points are sent to $\mathcal{O}$ when they go through this isogeny.

Maps

Point doubling using Montgomery form:

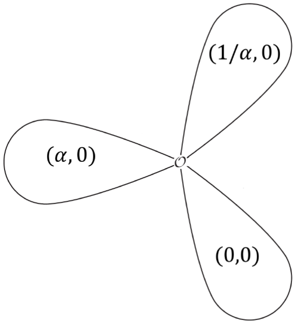
$$x \mapsto \frac{(x^2-1)^2}{4x(x^2+ax+1)}$$

The denominator here determines which points are of order 2, these points are sent to $\mathcal{O}$ when they go through this map.

These points form the *kernel* of the multiplication-by-2 map, in other words they are the *2-tortion*

$$G = \left\{\mathcal{O}, (\alpha, 0), (\tfrac{1}{\alpha}, 0), (0, 0)\right\}$$

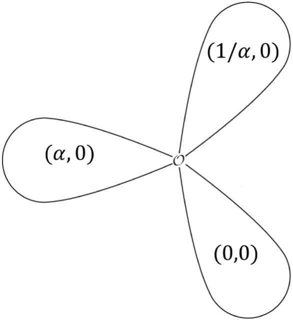
Tortions



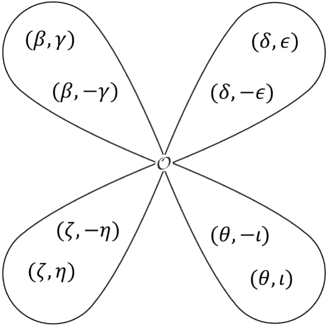
2-tortion

source: https://eprint.iacr.org/2019/1321.pdf

Tortions



2-tortion



3-tortion

This holds true for all ℓ where $p \nmid \ell$

---

source: https://eprint.iacr.org/2019/1321.pdf

Isogenies

The point doubling operation is described by its Kernel, a group G of points on the curve:

$$G = \left\{\mathcal{O}, (\alpha, 0), (\tfrac{1}{\alpha}, 0), (0, 0)\right\}$$

Nothing new - we multiply the point by 2 and get a new point on the same curve...

Isogenies

The point doubling operation is described by its Kernel, a group G of points on the curve:

$$G = \left\{\mathcal{O}, (\alpha, 0), (\tfrac{1}{\alpha}, 0), (0, 0)\right\}$$

Nothing new - we multiply the point by 2 and get a new point on the same curve...

However, what if we take an operation that has $G = \{\mathcal{O}, (\alpha, 0)\}$?

This will land us on a <u>new</u> curve with a different j-invariant!

Isogenies

We call a structure preserving mapping an *isogeny* when it is surjective and G is finite, i.e.:

$$\phi : E \to E' \text{ with kernel G}$$

Isogenies

We call a structure preserving mapping an *isogeny* when it is surjective and G is finite, i.e.:

$$\phi : E \to E' \text{ with kernel G}$$

Any finite subgroup G of points in E give rise to an isogeny. However most will map to the same curve (E = E')

We can find an isogeny from the corresponding group using *Vélu's formula*

Isogenies

$$
\begin{tikzcd}
j(E) \arrow[r, "\Phi"] \arrow[d, "\Psi"'] & j(E_a) \arrow[d, "?"] \\
j(E_b) \arrow[r, "?"'] & j(E_{ab})
\end{tikzcd}
$$

Isogenies - properties

- Isogenies are algebraic group homomorphisms:

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

- We can compose Isogenies:

$$\phi : E \to E' \text{ and } \psi : E' \to E''$$

$$(\psi \circ \phi)\text{: } E \to E''$$

$\to$ This is useful because complicated Isogenies can be broken down into simpler ones

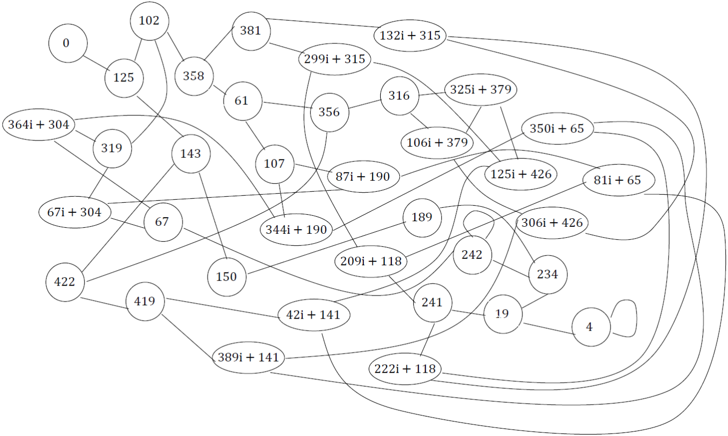
- Operations on Isogenies stay in $\mathbb{F}_{p^2}$

- The degree of the Isogeny $= \#$G

Isogenies

$$
\begin{tikzcd}
j(E) \arrow[r, "\Phi_1 \circ \ldots \circ \Phi_n"] \arrow[d, "\Psi_1 \circ \ldots \circ \Psi_n"'] & j(E_a) \arrow[d, "?"] \\
j(E_b) \arrow[r, "?"'] & j(E_{ab})
\end{tikzcd}
$$

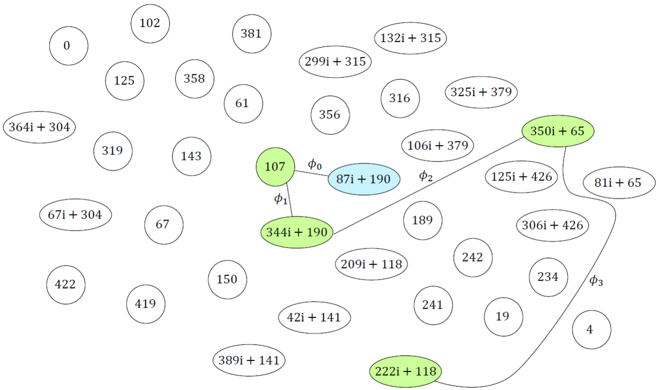
Graphs



2-Isogeny Graph

source: https://eprint.iacr.org/2019/1321.pdf

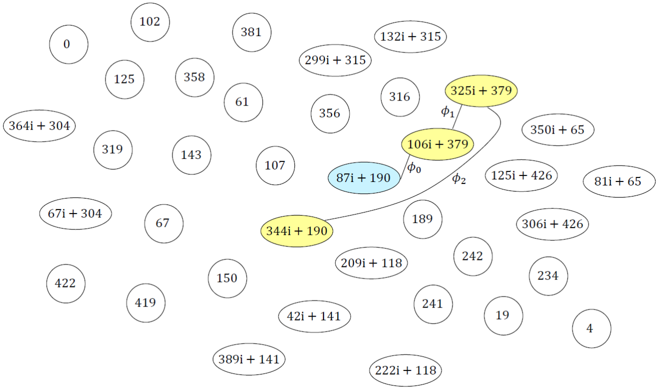
SIDH



Alice computes 4 isogenies on 2-isogeny graph

source: https://eprint.iacr.org/2019/1321.pdf

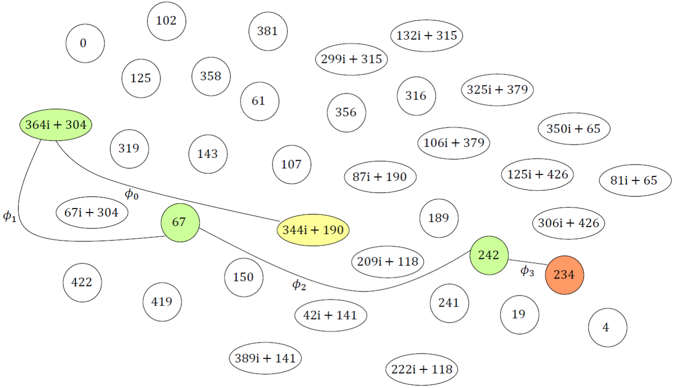
SIDH



Bob computes 3 isogenies on 3-isogeny graph

source: https://eprint.iacr.org/2019/1321.pdf

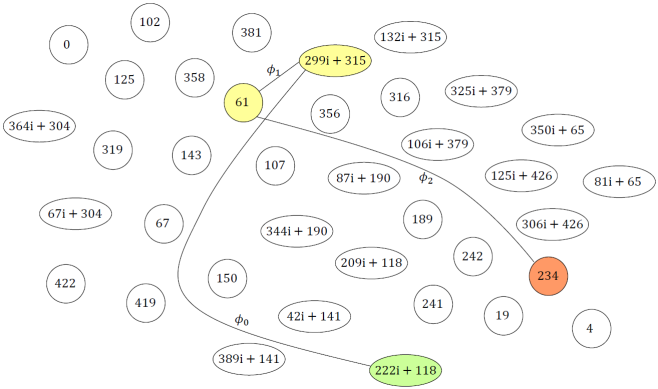
SIDH



Alice computes 4 isogenies from Bob's point on 2-isogeny graph

source: https://eprint.iacr.org/2019/1321.pdf

SIDH



Bob computes 3 isogenies from Alice's point on 3-isogeny graph

source: https://eprint.iacr.org/2019/1321.pdf

SIDH - Security

- Hard problem - hard to find isogenies that connect 2 j-invariants
  - Classical algorithm complexity O($p^{1/4}$)
  - Quantumn algorithm complexity O($p^{1/6}$)
- Size of graph grows exponentially with p
  - Alice and Bob won't visit same point
  - Number of intemediate j-invariants grows
- Graph properties
  - expander graphs - No way to rearrange to simplify graph
  - connected - there is a path to every node
  - $(\ell + 1)$ regular - each node has $\ell + 1$ edges*
  - rapid mixing - logarithmic no. of steps away from any other node

Isogenies

$$\begin{tikzcd}
j(E) \arrow[rr, "\Phi_1 \circ \ldots \circ \Phi_n"] \arrow[d, "\psi_1 \circ \ldots \circ \psi_n"'] & & j(E_a) \arrow[d, "\psi'_1 \circ \ldots \circ \psi'_n"] \\
j(E_b) \arrow[rr, "\Phi'_1 \circ \ldots \circ \Phi'_n"'] & & j(E_{ab})
\end{tikzcd}$$

NIST Post Quantum Competition

PKE/KEM Finalists

- CRYSTALS-KYBER
- NTRU
- SABER
- Classic McEliece

Alternate candidates

- FrodoKEM
- NTRU Prime
- BIKE
- HQC
- SIKE

Bibliography

- naehrwert, "(post-quantum) isogeny cryptography."
- C. Costello, "Supersingular isogeny key exchange for beginners," in *Selected Areas in Cryptography – SAC 2019* (K. G. Paterson and D. Stebila, eds.), vol. 11959, pp. 21–50, Springer International Publishing.
  Series Title: Lecture Notes in Computer Science.
- D. Urbanik, "A friendly introduction to supersingular isogeny diffie-hellman," p. 9.
- W. Castryck, "Elliptic curves are quantum dead, long live elliptic curves | COSIC."
- A. Sutherland, "MIT18_783s19_lec6.pdf."
- C. Costello, "Microsoft research webinar | post-quantum cryptography: Supersingular isogenies for beginners.".