

## CSIDH &amp; SIDH.

CSIDH: a supersingular curve in Montgomery form, defined over  $\mathbb{F}_p$ .

$$E_0: y^2 = x^3 + x.$$

$$E_A: y^2 = x^3 + Ax^2 + x.$$

$$j(E_0) = 1728.$$

if  $p \equiv 3 \pmod{4}$ ,  $E_0$  is supersingular, and  $\#E_0(\mathbb{F}_p) = p+1$ .

Moreover,  $\#E_0(\mathbb{F}_{p^2}) = (p+1)^2 = p^2 + 1 - (-2p) \rightarrow t_{\mathbb{F}_{p^2}} = -2p$ .

(Theorem 4.12 in Silverman for example)

We start from  $E_0$ :  $p+1 = 4 \cdot \underbrace{l_1 \cdot l_2 \cdot l_3 \cdot \dots \cdot l_m}_{\text{many distinct small primes}}$ .

Velu's formulas for a prime  $l_i$ .

Choose  $P$  of order  $l_i$ ,  $\langle P \rangle$  is a subgroup of prime order  $l_i$ .

$$\begin{aligned} \langle P \rangle &= \{0, P, 2P, 3P, \dots, [l_i-1]P\} \\ &= \{0, \underbrace{P, -P, 2P, -2P, \dots, [(l_i-1)/2]P, [-(l_i-1)/2]P}\}_{(x_i, \pm y_i)}. \end{aligned}$$

Let  $x_i$  be the  $x$ -coordinate of  $[i]P$ .

$$\tau_l = \prod_{i=1}^{l-1} x_i \quad \sigma_l = \sum_{i=1}^{l-1} \left( x_i - \frac{1}{x_i} \right), \quad f_l(x) = x \prod_{i=1}^{l-1} \frac{x x_i - 1}{x - x_i}$$

$$\phi_l: E_A \rightarrow E_{A_l}$$

$$(x, y) \mapsto (f_l(x), c_0 y f_l'(x))$$

$$A_l = \tau_l(A - 3\sigma_l) \quad \text{and} \quad c_0^2 = \tau_l.$$

## RECAP ON QUADRATIC TWISTS.

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

$$E'_A: S \cdot y^2 = x^3 + Ax^2 + x \quad \text{where } S \text{ is not a square in } \mathbb{F}_p$$

$$\text{twist: } E_A \rightarrow E'_A$$

$$(x, y) \mapsto (x, \sqrt{S}y)$$

$$\in \mathbb{F}_{p^2}$$

$$\frac{E'_A}{S^3} = \left( \frac{y}{S} \right)^2 = \left( \frac{x}{S} \right)^3 + \frac{A}{S} \left( \frac{x}{S} \right)^2 + \frac{1}{S^2} \left( \frac{x}{S} \right)$$

$$E''_A: y^2 = x^3 + A/S x^2 + 1/S^2 x$$

$$E_A \rightarrow E''_A: (x, y) \mapsto (x/S, y\sqrt{S}/S)$$

CSIDH considers curves up to  $\mathbb{F}_p$ -isomorphism,

→ quadratic twists are seen as two distinct curves.

Toy example:  $p = 419$ , so that  $p+1 = 4 \times 3 \times 5 \times 7$ .

find a point of order  $l_i$ :

$l_i \neq 2$ . Take a random point  $P \in E(\mathbb{F}_p)$ .

While  $[(p+1)/l_i] P = \mathcal{O}$ :

take another random point  $P$  on  $E$ .

it works because the index of  $l_i$  in  $(p+1)$  is  $\perp$ . Notation:  $l_i \parallel p+1$ .

$l=2$  is avoided because it is not an isogeny on  $E_0$ . It is an ~~endo~~ <sup>endo</sup> morphism.

Exercise: check that with the 2-torsion point  $(0,0)$ , the 2-isogeny of kernel  $(0,0)$  lands to an isomorphic curve  $y^2 = x^3 + A'x$  of ~~invariant~~ <sup>j-invariant</sup> 1728

$E/\mathbb{F}_p: y^2 = x^3 + Ax^2 + x$ , supersingular,  $\#E(\mathbb{F}_p) = p+1$ .

$p$  is chosen so that  $p+1 = 4 \cdot l_1 \cdot l_2 \cdot l_3 \cdots l_m$  with distinct primes  $l_m$ .

→ there is only one choice of  $l$ -torsion subgroup on  $E(\mathbb{F}_p)$ .

$\#E(\mathbb{F}_{p^2}) = (p+1)^2 \rightarrow l_i^2 \mid \#E(\mathbb{F}_{p^2})$ , and  $E[l] \subseteq E(\mathbb{F}_{p^2})$ .

How to identify each subgroup?

Let  $P$  of order  $l_i$  in  $E(\mathbb{F}_p)$ .  $P(x_p, y_p)$ .

Consider the image of  $P$  under the quadratic twist map, where  $\delta = -1$ :

twist:  $E_A \rightarrow E_{-A}$

$(x, y) \mapsto (-x, -y\sqrt{-1}) \notin E(\mathbb{F}_p)$  because  $\sqrt{-1} \notin \mathbb{F}_p$ .

Now just do it the other way; consider  $E_{-A}$ , and find a point of order 5  $(x'_5, y'_5)$  on  $E_{-A}(\mathbb{F}_p)$ . Then  $(-x'_5, -y'_5\sqrt{-1}) \in E_A(\mathbb{F}_{p^2})$  and has order 5.

Hence there are two choices of generators of order  $l_i$  subgroups that are convenient.

- $P(x_{l_i}, y_{l_i}) \in E_A(\mathbb{F}_p)$  of order  $l_i$ ,

- $Q(-x'_{l_i}, -y'_{l_i}\sqrt{-1}) \in E_A(\mathbb{F}_{p^2})$  where  $(x'_{l_i}, y'_{l_i}) \in E_{-A}(\mathbb{F}_p)$  has order  $l_i$ .

in both cases,  $x_{l_i}$  and  $-x'_{l_i}$  are in  $\mathbb{F}_p$

→ the computations take place in  $\mathbb{F}_p$ , not  $\mathbb{F}_{p^2}$ .

$p = 4 \cdot \prod_{3 \leq l_i \leq 373} l_i \cdot 587 - 1$  so that  $p+1 = 4 \cdot$  a product of 74 distinct primes.

$p$  has 511 bits.  $E_0: y^2 = x^3 + x$ . supersingular of order  $p+1$ .

back to our toy example

$p = 419, p+1 = 4 \cdot 3 \cdot 5 \cdot 7. E_0: y^2 = x^3 + x. P(-185, 73)$  has order 5.

$E_{199}: y^2 = x^3 + 199x^2 + x.$

$2P(349, 133)$  ———.

now a 5-isogeny from  $E_{199}$ :

$P(-100: 148)$  has order 5.

$2P(-156: 145)$  ———.

$\tau_5 = (100 - 156)^2 = 97^2 = 194$

$3P(156: 274) = -2P$   
 $4P(100: 271) = -P$

$\sigma_5 = 2 \left( 100 - \frac{1}{100} + 156 - \frac{1}{156} \right) = 2 \cdot 262 = 105$

$f_5(x) = x \left( \frac{x \cdot 100 - 1}{x - 100} \cdot \frac{x \cdot 156 - 1}{x - 156} \right)^2 \quad c_0 = 97.$

$A_5 = \tau_5 (A - 3\sigma_5) = 194 (-199 - 3 \cdot 105) = 51.$

→ this 5-isogeny lands on  $E_{51}: y^2 = x^3 + 51x^2 + x.$

what is the other one?

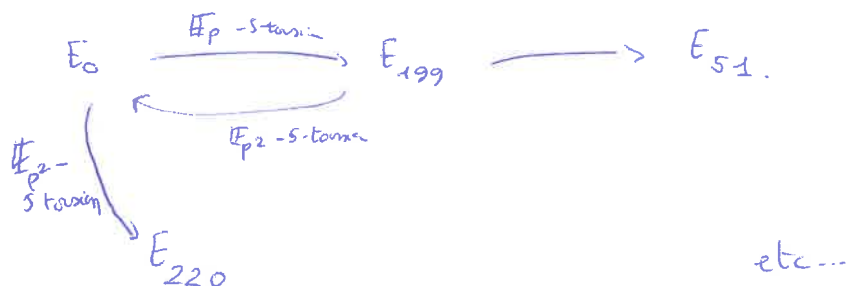
consider  $E_{-199}: y^2 = x^3 - 199x^2 + x$  the quadratic twist.

it has a 5-torsion point over  $\mathbb{F}_p: P_5(345, 176) \text{ and } (-189, 98).$

→  $(-345, -176i), (-189, -98i)$  are 5-torsion points on  $E_{199} (\mathbb{F}_{p^2})$ .  
 $= (74, 243i) \quad (230, 321i).$

→ do the same but with these two points:

$\tau_5 = 141, \sigma_5 = 206, A_5 = 0 \rightarrow$  we are back to  $E_0$ .



$E \leftrightarrow$  coefficient  $A$  in Montgomery form (with  $B=1$ )

$l_i \rightarrow l_i$ -isogeny with kernel in  $\mathbb{F}_p$ .

$\rightarrow l_i$ -isogeny with kernel  $(-x'_i, i y'_i)$  and  $(x'_i, y'_i) \in E_{-A}(\mathbb{F}_p)$ .

"left" and "right" isogenies for each prime  $l_i > 2$ .

**COMMUTATIVE GROUP ACTION**

$$[+3, +3, -5, -7, -7, +5, -7, -3] \rightarrow [(+3) \times 1, (5) \times 0, (-7) \times 3].$$

$\rightarrow$  apply 1 times a 3-isogeny "+", and 3 times a 7-isogeny "-".

"GROUP ACTION" of  $(\mathbb{Z}^m, +)$  on the set of isogenous curves  $E_A$ .

$\mathbb{Z}^m$ : the number of times each isogeny is applied

$m$ : the number of distinct primes  $l_i > 2$ .

Alice

$$a \leftarrow \text{random } \mathbb{Z}^m$$

$$[l_1^{a_1}, l_2^{a_2}, l_3^{a_3}, \dots, l_m^{a_m}]$$

$\rightarrow$  apply the  $l_i$ -isogenies to  $E_0$

$\rightarrow E^a$

Bob

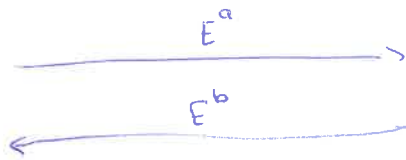
$$b \leftarrow \text{random } \mathbb{Z}^m$$

$$[l_1^{b_1}, l_2^{b_2}, \dots, l_m^{b_m}]$$

$\rightarrow$  apply the  $l_i$  isogenies to  $E_0$

$\rightarrow E^b$

apply  $a$  to  $E^b$



apply  $[b]$  to  $E^a$ .

it commutes:

$$E^{ab} = E^{ba}$$

Alice and Bob share a curve coefficient  $A_{ab}$ .

**HARD PROBLEM:** given  $E_0, E^a, E^b$ , compute  $E^{ab}$ .

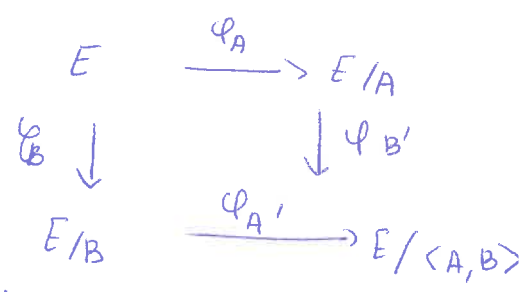
given  $E_0, E^a$ , compute  $a$ .

$\rightarrow$  compute an isogeny between two elliptic curves (that are known to be isogenous).

SIDH (older than CSIDH).

Consider curves over  $\mathbb{F}_{p^2}$ . (supersingular).

one curve  $\leftrightarrow$  one  $j$ -invariant.



Alice and Bob pick secret subgroups  $A$  and  $B$  of  $E$ .

Alice computes  $\varphi_A: E \rightarrow E/A$   
the isogenous curve by the isogeny of kernel  $A$ .

Bob computes  $\varphi_B: E \rightarrow E/B$ .

Alice and Bob exchange  $E/A$  and  $E/B$ .

Problem: how to continue? The usual setting is  $\# E(\mathbb{F}_{p^2}) = (p+1)^2 = 2^i 3^d$

in CSIDH, we used the fact that we don't need the explicit description of the kernel points to compute the isogeny:

Alice needs to know if she applies "left" or "right" isogenies, that's all.  
(Bob)  
because there are only 2 choices of  $l$ -isogenies, and each choice is clearly identified.

in SIDH, there are 2-isogenies, 4-isogenies, ...,  $2^2$ -isogenies, and 3,  $3^2$ , ...,  $3^d$  isogenies.

$p = 431 = 2^4 \cdot 3^3 - 1$ .  $P(382, 369)$  has order  $p+1$ .

isogenies are decomposed into 2- and 3- isogenies.

there are  $(l+1)$  subgroups of order  $l$  in  $E(\mathbb{F}_{p^2})$ , and each subgroup gives a new isogeny from  $E$ .

$(l+1) \cdot l - l = l^2$  points of order  $l$ .

But with CSIDH, there are only two subgroups such that the  $x$ -coordinates of the points are in  $\mathbb{F}_p$ , the  $(l-1)$  other subgroups are with  $x$ -coord. in  $\mathbb{F}_{p^2}$ . So they are ignored.