31.03.2022. POST-QUANTUM ISOGENIES.

CSIDH & SIDH.

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

$E_0 : y^2 = x^3 + x$. $\qquad E_A : y^2 = x^3 + Ax^2 + x$.

$j(E_0) = 1728$

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

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

(Theorem 4.12 in Silverman for example)

We start from E_0 : $p+1 = 4 \cdot \underbrace{\ell_1 \cdot \ell_2 \cdot \ell_3 \cdot \ldots \cdot \ell_n}_{\text{many distinct small primes}}$

Vélu's formulas for a prime ℓ_i.

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

$\langle P \rangle = \{ \mathcal{O}, P, 2P, 3P, \ldots, [\ell_i - 1] P \}$

$= \{ \mathcal{O}, \underbrace{P, -P}_{(x_1, \pm y_1)}, \underbrace{2P, -2P}_{(x_2, \pm y_2)}, \ldots, [(\ell_i - 1)/2] P, [-(\ell_i-1)/2] P \}$.

$\ldots \quad (x_i, \pm y_i)$.

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

$$\tau_\ell = \prod_{i=1}^{\ell-1} x_i \qquad \sigma_\ell = \sum_{i=1}^{\ell-1} \left(x_i - \frac{1}{x_i} \right), \quad f_\ell(x) = x \prod_{i=1}^{\ell-1} \frac{x x_i - 1}{x - x_i}$$

$$\phi_\ell : E_A \to E_{A_\ell}$$
$$(x,y) \longmapsto (f_\ell(x), c_0 \, y \, f_\ell'(x))$$

$A_\ell = \tau_\ell (A - 3\sigma_\ell)$ and $c_0^2 = \tau_\ell$.

RECAP on QUADRATIC TWISTS.

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

twist: $E_A \to E_A'$

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

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

$E_A' : \delta . y^2 = x^3 + Ax^2 + x$ where δ is not a square in $\mathbb{F}_p$

$\frac{E_A'}{\delta^3} : \left(\frac{y}{\delta}\right)^2 = \left(\frac{x}{\delta}\right)^3 + \frac{A}{\delta}\left(\frac{x}{\delta}\right)^2 + \frac{1}{\delta^2}\left(\frac{x}{\delta}\right)$

$E_A'' : y^2 = x^3 + A/\delta \, x^2 + 1/\delta^2 \, x$.

$E_A \to E_A'' : (x,y) \mapsto (x/\delta, y\sqrt{\delta}/\delta)$

CSIDH considers curves up to $\mathbb{F}_p$-isomorphism,
$\to$ 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:
$\ell_i \neq 2$. Take a random point $P \in E(\mathbb{F}_p)$.
While $[(p+1)/\ell_i]\, P = \mathcal{O}$.
take another random point P on E.

it works because the index of ℓ_i in $(p+1)$ is 1. Notation: $\ell_i \,\|\, p+1$.
$\ell = 2$ is avoided because it is not an isogeny on E_0. It is an endomorphism.
Exercice: 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 j-invariant 1728

$E/\mathbb{F}_p$: $y^2 = x^3 + Ax^2 + x$, supersingular, $\#E(\mathbb{F}_p) = p+1$.
p is chosen so that $p+1 = 4 \cdot \ell_1 \cdot \ell_2 \cdot \ell_3 \cdots \ell_n$ with distinct primes ℓ_n.
$\to$ there is only one choice of ℓ-torsion subgroup on $E(\mathbb{F}_p)$.
$\#E(\mathbb{F}_{p^2}) = (p+1)^2 \to \ell_i^2 \mid \#E(\mathbb{F}_{p^2})$, and $E[\ell] \subseteq E(\mathbb{F}_{p^2})$.

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: $E_A \to E_{-A}$
$(x,y) \longmapsto (-x, -y\sqrt{-1}) \notin E(\mathbb{F}_p)$ 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.

- $P(x_{\ell_i}, y_{\ell_i}) \in E_A(\mathbb{F}_p)$ of order ℓ_i,
- $Q(-x'_{\ell_i}, -y'_{\ell_i}\sqrt{-1}) \in E_A(\mathbb{F}_p)$ where $(x'_{\ell_i}, y'_{\ell_i}) \in E_{-A}(\mathbb{F}_p)$ has order ℓ_i.

in both cases, x_{ℓ_i} and $-x'_{\ell_i}$ are in $\mathbb{F}_p$
$\to$ the computations take place in $\mathbb{F}_p$, not $\mathbb{F}_{p^2}$.

CSIDH and POST-QUANTUM CRYPTO. 31.03.2022.

$p = 4 \cdot \prod_{\substack{3 \leq l_i \leq 373 \\ \text{primes}}} l_i \cdot 587 - 1$ 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.
$2P(349, 133)$ ——.

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

now a 5-isogeny from E_{199}: $P(100 : 148)$ has order 5.
$2P\ (156 : 145)$ ——.
$3P\ (156 : 274) = -2P$
$4P\ (100 : 271) = -P$

$\tau_5 = (100 \cdot 156)^2 = 97^2 = 191$

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

$f_5(x) = x\left(\frac{x \cdot 100 - 1}{x - 100} \cdot \frac{x \cdot 156 - 1}{x - 156}\right)^2$ $C_0 = 97$.

$A_5 = \tau_5(A - 3\sigma_5) = 191(199 - 3 \cdot 105) = \cancel{29}.51$.

-> 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 $\mathbb{F}_p$: $P_5(345, 176)$ $2P_5 : (-189, 98)$.

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

-> do the same but with these two points:
$\tau_5 = 141$, $\sigma_5 = 206$, $A_5 = 0$ -> we are back to E_0.

$$\begin{tikzcd} E_0 \arrow[r, "\mathbb{F}_p\text{-}5\text{-torsion}"] \arrow[d, "\mathbb{F}_{p^2}\text{-}5\text{ torsion}"'] & E_{199} \arrow[r] \arrow[l, bend left, "\mathbb{F}_{p^2}\text{-}5\text{-torsion}"] & E_{51}. \\ E_{220} & & \end{tikzcd}$$

etc...

CSIDH and post-quantum crypto. 31.03.2022.

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

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

$\longrightarrow$ 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 $(\mathbb{Z}^n, +)$ on the set of isogenous curves E_A.

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

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

Alice

$a \xleftarrow{\text{random}} \mathbb{Z}^n$

$[l_1^{a_1}, l_2^{a_2}, l_3^{a_3}, \dots, l_n^{a_n}]$.

$\rightarrow$ apply the l_i-isogenies to E_0

$\rightarrow E^a$

Bob

$b \xleftarrow{\text{random}} \mathbb{Z}^n$

$[l_1^{b_1}, l_2^{b_2}, \dots, l_n^{b_n}]$

$\rightarrow$ apply the l_i isogenies to E_0

$\rightarrow E^b$

$\xrightarrow{E^a}$

$\xleftarrow{E^b}$

apply $[b]$ to E^a.

apply a to E^b.

it commutes:

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

Alice and bob shares 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 $\longleftrightarrow$ one j-invariant.

$$\begin{tikzcd} E \arrow[r, "\varphi_A"] \arrow[d, "\varphi_B"'] & E/A \arrow[d, "\varphi_{B'}"] \\ E/B \arrow[r, "\varphi_{A'}"] & E/\langle A,B\rangle \end{tikzcd}$$

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

Alice computes $\varphi_A : E \to \underbrace{E/A}$

the isogenous curve by the isogeny of kernel A.

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

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

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

$\to$

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, $\dots$, 2^i-isogenies, and $3, 3^2, \dots, 3^j$ 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 $(\ell+1)$ subgroups of order ℓ in $E(\mathbb{F}_{p^2})$, and each subgroup gives a new isogeny from E.

$(\ell+1)\cdot \ell - \ell = \ell^2$ 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 $(\ell-1)$ other subgroups are with x-coord. in $\mathbb{F}_{p^2}$.
So they are ignored.