DDH & attacks from genus theory

$E/\mathbb{F}_q$ $\qquad \mathrm{End}_{\mathbb{F}_q}(E) = \mathcal{O}$ order in $\mathbb{Q}(\sqrt{t^2-4q})$

$\# E(\mathbb{F}_q) = q+1-t$

t^2-4q disc of $x^2 - tx + q$

$\mathcal{O} \supseteq \mathbb{Z}[\pi]$ $\quad \pi$ Frobenius, root of

$$\mathrm{Ell}_q(\mathcal{O},t) = \left\{ E'/\mathbb{F}_q : \begin{array}{l} \mathrm{End}(E') = \mathcal{O} \\ \mathrm{tr}(E') = t \\ \# E'(\mathbb{F}_q) = q+1-t \end{array} \right\} \Big/ \mathbb{F}_q\text{-iso}$$

$G = \mathrm{Cl}(\mathcal{O})$ acts on the set $X = \mathrm{Ell}_q(\mathcal{O},t)$

Group G acting on a set X, free and transitive

	Alice	E		Bob
sk	$a \in G$			$b \in G$
pk	$a \star E$	$a\star E$	$b \star E$	$b \star E$
	$a \star (b \star E)$			$b \star (a \star E)$

$E_{AB} = ab \star E$

$E_A = a \star E$

$E_B = b \star E$

secure if Alice and Bob are the only ones who know E_{AB}

↳ CDH assumption

Protocol E, E_A, E_B ⟿ we can derive information about E_{AB}

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

$j(E_{AB})$ as shared key

DDH: There's nothing predictable about E_{AB} if we only see E, E_A, E_B.

CSV: there sometimes exist characters χ s.t.

$$\chi(E_{AB}) = \chi(E_A) \cdot \chi(E_B)$$

χ character on $Cl(\mathcal{O})$

χ quadratic character

§7 Pairings $E/\mathbb{F}_q$

$$E \times E \to \mathbb{F}_q$$

bilinear maps

Weil pairing $E[N] \times E[N] \to \mu_N$

$e_N(P, Q) = \zeta_N \in \mathbb{F}_q$

m odd prime

$$E \to E' = [\mathfrak{a}] \ast E$$

$$[\mathfrak{a}] \in Cl(\mathcal{O})$$

for every $\mathfrak{a} \in [\mathfrak{a}]$, we have an isogeny

$$\varphi_{\mathfrak{a}} : E \to E' \quad \deg \varphi_{\mathfrak{a}} = \mathrm{norm}(\mathfrak{a})$$

If we can say anything about $\deg \varphi_{\mathfrak{a}} \bmod m$

we get information about every $\mathfrak{a} \in [\mathfrak{a}]$

$$(\deg \varphi_{\mathfrak{a}} \bmod m)_{\mathfrak{a} \in [\mathfrak{a}]}$$

E, E' isogenous curves $\quad val_m(\#E(\mathbb{F}_q)) = 1$

$P \in E(\mathbb{F}_q)[m]$ $\quad$ then degree of any isogeny

$P' \in E'(\mathbb{F}_q)[m]$ $\quad \varphi : E \to E'$

is, up to squares mod m

$$\deg \varphi = \boxed{\log_{T_m(P,P)} \log(T_m(P',P'))}$$

$$\begin{tikzcd}
E \arrow[r, "a"] \arrow[d, "b"'] & E_A \arrow[d, "b"] & \\
E_B \arrow[r, "a"'] & E_{AB} \arrow[r, phantom, "\overset{?}{=}"] & E_C
\end{tikzcd}$$

$G = cl(\mathcal{O})$ $\quad$ $\mathcal{O}$ order in im. quad field

$\circlearrowright$

$X = Ell$ $\leftarrow$ elliptic curves / $\mathbb{F}_q$

$\mathrm{End}_{\mathbb{F}_q}(E) \cong \mathcal{O}$

trace $t = \# E(\mathbb{F}_q) - q - 1$ is fixed

$G \circlearrowright X$ is free and transitive

<u>DH key exchange</u>

E $\leftarrow$ starting pt

	Alice	Bob
		b
sk	a	$b * E$
pk	$a * E$	

$a * (b * E)$ $\qquad\qquad$ $b * (a * E)$

1) Secure if Alice and Bob the only ones who hold $E_{AB} = ab * E$ $\Big\}$ CDH

DDH $\simeq$ E, E_A, E_B then E_{AB} "looks random"

publickeys

you can't use E, E_A, E_B to predict anything about E_{AB}

How many supersingular curves are there

$\approx \frac{p}{12}$ = # supersingular j-invariants in $\mathbb{F}_{p^2}$

$\sqrt{p}$ = # supersingular curves over $\mathbb{F}_p$, up to iso

$\approx$ # $Cl(\mathbb{Z}[\sqrt{-p}])$

p mod 8	
1 mod 4	$h(-4p)$
3 mod 8	$h(-4p)+h(-p)$
7 mod 8	$2 \cdot h(-p)$

$h(-\Delta) \approx \sqrt{|\Delta|}$

Wouter week 3

Ex 1.1. there are p different A's
only $\sqrt{p}$ of them are supersingular curve $\Big\} \frac{\sqrt{p}}{p}$

§ 2 Pairings

m odd prime, $E/\mathbb{F}_q$

$$T_m : E(\mathbb{F}_q)[m] \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) \to \mu_m$$

$\mu_m \subseteq \mathbb{F}_q \iff m \mid q-1$

$$(P, Q) \longmapsto T_m(P, Q)$$

$$\varphi : E \to E'$$

$$P, Q \longmapsto \varphi(P), \varphi(Q)$$

$$T_m(\varphi(P), \varphi(Q)) = T_m(P, Q)^{\deg \varphi}$$

$$\longmapsto \deg \varphi \pmod{m}$$

"Hard problem": $E \to E'$ under some secret isogeny φ

find pair $P, P' = \varphi(P)$

Get-around: isogenies

$$\begin{cases} \text{rational map: points in } E(\mathbb{F}_q) \text{ map to } E'(\mathbb{F}_q) \\ \text{group homo: } E[m] \longrightarrow E'[m] \end{cases}$$

1) if $E(\mathbb{F}_q)[m] = \langle P \rangle$
$E'(\mathbb{F}_q)[m] = \langle P' \rangle$ $\Longrightarrow \varphi(P) = k \cdot P'$

k unknown

E E'

(conditions apply)

computing these Tate pairings determines

$\deg \varphi \bmod m$, up to squares mod m

for any isogeny $\varphi : E \to E'$

DDH If all these conditions hold, and we can compute deg of isog $(E \to E_A)$ mod m up to squares

$$\begin{tikzcd} E \arrow[r, "a"] \arrow[d] & E_A \arrow[d] \\ E_B \arrow[r, "a"] & E_{AB} \end{tikzcd}$$

...

$E_{AB} \overset{?}{=} E_C$ E_C random

deg of isog $(E_B \to E_{AB})$ ...

$\chi(E, E_A) = \left(\frac{\deg \varphi}{m} \right)$ ← Legendre symbol

$= \begin{cases} 1 & \text{if } \deg \varphi \text{ always square mod } m \\ -1 & \text{if } \deg \varphi \text{ always non-square} \end{cases}$

always: for any isogeny $\varphi : E \to E'$

Conditions: $\mu_m \subseteq \mathbb{F}_q$, $E(\mathbb{F}_q)[m^\infty] = \langle P \rangle$ P of order m

SIDH

$$\begin{tikzcd} E \arrow[r, "2^n"] \arrow[d, "3^m"'] & E_A \\ E_B & E_C \stackrel{?}{\cong} E_{AB} \end{tikzcd}$$

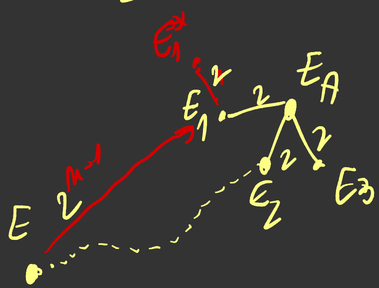
E_{AB} is 3^m-isogenous to E_A
2^n- isogenous to E_B

A) Decide whether E_C is 3^m-isog to E_A
B) 2^n- isog to E_B

CSIDH
E, E'
always
$E' = a * E$
for some a

I) Galbraith - Vercauteren Comp problems in isog...
II) Jao - Urbanik? Sok

DDH to CDH ~~reduction~~ isogeny finding



n = #steps in SIDH
= poly size
= $O(\log p)$

Input to these problems
p, $\mathbb{F}_{p^2}$, $E_0/\mathbb{F}_{p^2}$....

write it down using $\log_2 p$ bits
polynomial time = poly in $\log_2 p$

$2^n \approx \sqrt{p}$
$n \approx \frac{1}{2} \log p$