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	$a \star E$	$a \star E \quad b \star E$	$b \star E$
	$a \star (b \star E)$		$b \star (a \star E)$

$E_{AB} = ab \star E$

$E_A = a \star E$

$E_B = b \star E$

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 $\quad E/\mathbb{F}_q$

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

bilinear map $\quad$ Weil pairing $\quad E[N] \times E[N] \to \mu_N$

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

m odd prime

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

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

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

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

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' isogeneous 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

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

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