

DDH & attacks from genus theory

$$E/\mathbb{F}_q \quad \text{End}_{\mathbb{F}_q}(E) = \mathbb{O} \quad \text{order in } \mathbb{Q}(\sqrt{\ell^2 - 4g})$$

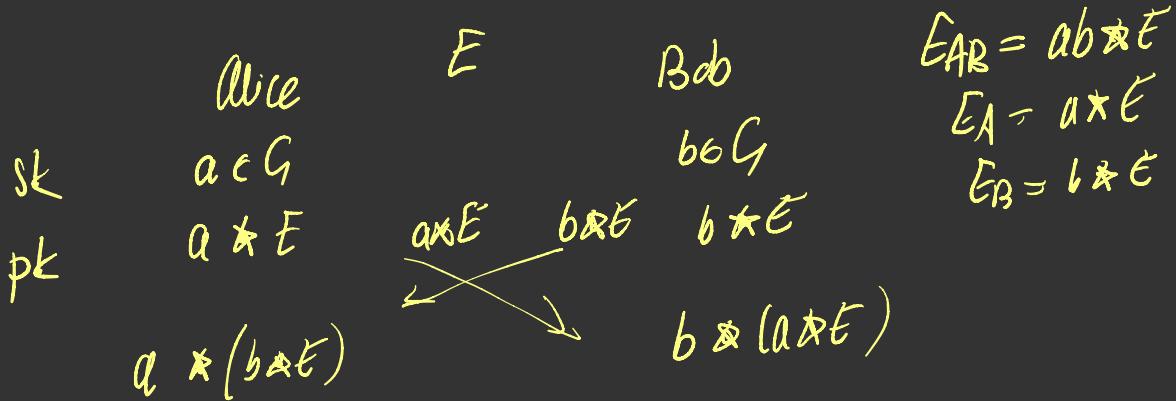
$$\# E(\mathbb{F}_q) = q + 1 - t$$

$$\ell^2 - 4g \quad \text{disc of } x^2 - tx + q \quad \leftarrow \\ G \in \mathbb{Z}[\pi] \quad \pi \text{ Frobenius, root of}$$

$$\text{Ell}_q(O, t) = \left\{ E' / \mathbb{F}_q : \begin{array}{l} \text{End}(E') = \mathbb{O} \\ \text{Fr}(E') = t \\ \# E'(\mathbb{F}_q) = q + 1 - t \end{array} \right\}_{\mathbb{F}_q = \mathbb{Z}}$$

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

Group G acting on a set X , free and transitive



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

↳ CDH assumption

Protocol $E, E_A, E_B \rightsquigarrow$ we can derive
information about E_{AB}

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

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

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

CSV: There exist characters χ s.t.

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

χ character on \mathbb{Q}/\mathbb{O}

χ quadratic character

$$\S 2 \quad \frac{\text{Pairings}}{E \times E} \rightarrow \mathbb{F}_2$$

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

$$e_N(P, Q) = \sum_{n=1}^N e_n \in \mathbb{F}_2$$

m odd prime

$$E \rightarrow E' = [a] \not\cong E$$

$$[a] \in \mathcal{O}(0)$$

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

$$\varphi_a : E \rightarrow E' \quad \deg \varphi_a = \text{norm } a$$

If we can say anything about $\deg \varphi_a \pmod m$

we get information about every $a \in [a]$

$$(\deg \varphi_a \pmod m)_{a \in [a]}$$

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

$p \in E(\mathbb{F}_q)[m]$ then degree of my isogeny
 $p' \in E'(\mathbb{F}_q)[m]$ $\varphi: E \rightarrow E'$

is, up to squares mod m

$$\deg \varphi = \begin{bmatrix} \log_{T_m(p, 0)} & \log |T_m(p', p)| \\ \log T_m(p, 0) & \end{bmatrix}$$

$$\begin{array}{ccc} E & \xrightarrow{a} & E_A \\ b \downarrow & & \downarrow b \\ E_B & \xrightarrow{a} & E_{AB} \stackrel{?}{=} E_C \end{array}$$