



Alice

$$E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z})^2$$

$$E[2^{e_A}] = \langle P_A, Q_A \rangle$$

$$E[3^{e_B}] = \langle P_B, Q_B \rangle$$



Choose $m_A, n_A \in \mathbb{Z}$

$$A := [m_A]P_A + [n_A]Q_A$$

$$\alpha : E \rightarrow E/\langle A \rangle$$

$$E/\langle A \rangle, \alpha(P_B), \alpha(Q_B)$$

Choose $m_B, n_B \in \mathbb{Z}$

$$B := [m_B]P_B + [n_B]Q_B$$

$$\beta : E \rightarrow E/\langle B \rangle$$

