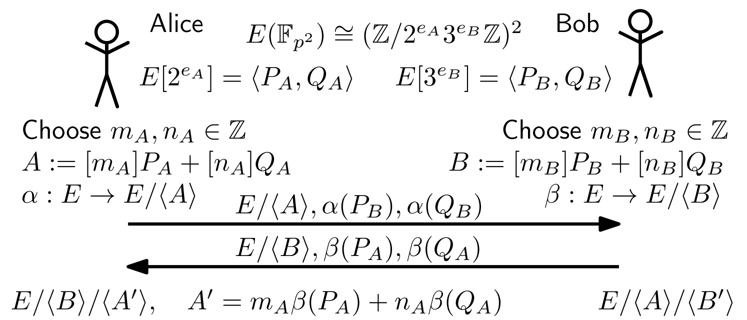

Alice $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z})^2$ Bob

$E[2^{e_A}] = \langle P_A, Q_A \rangle \qquad E[3^{e_B}] = \langle P_B, Q_B \rangle$

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

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

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

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

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

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

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

$E/\langle B \rangle, \beta(P_A), \beta(Q_A)$

$E/\langle B \rangle/\langle A' \rangle, \quad A' = m_A\beta(P_A) + n_A\beta(Q_A)$

$E/\langle A \rangle/\langle B' \rangle$