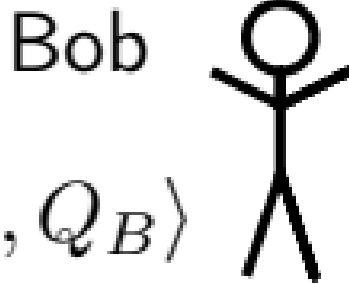


Alice

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

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



Bob