

Public parameters:  $(EC(a, b), P, q)$

*Alice*

*Bob*

$$a \xleftarrow{\$} \mathbb{Z}_q$$
$$\alpha \leftarrow a \cdot P$$

$$\xrightarrow{\alpha}$$

$$b \xleftarrow{\$} \mathbb{Z}_q$$
$$\beta \leftarrow b \cdot P$$

$$\xleftarrow{\beta}$$

$$k \leftarrow a \cdot \beta = ab \cdot P$$

$$k \leftarrow b \cdot \alpha = ba \cdot P$$