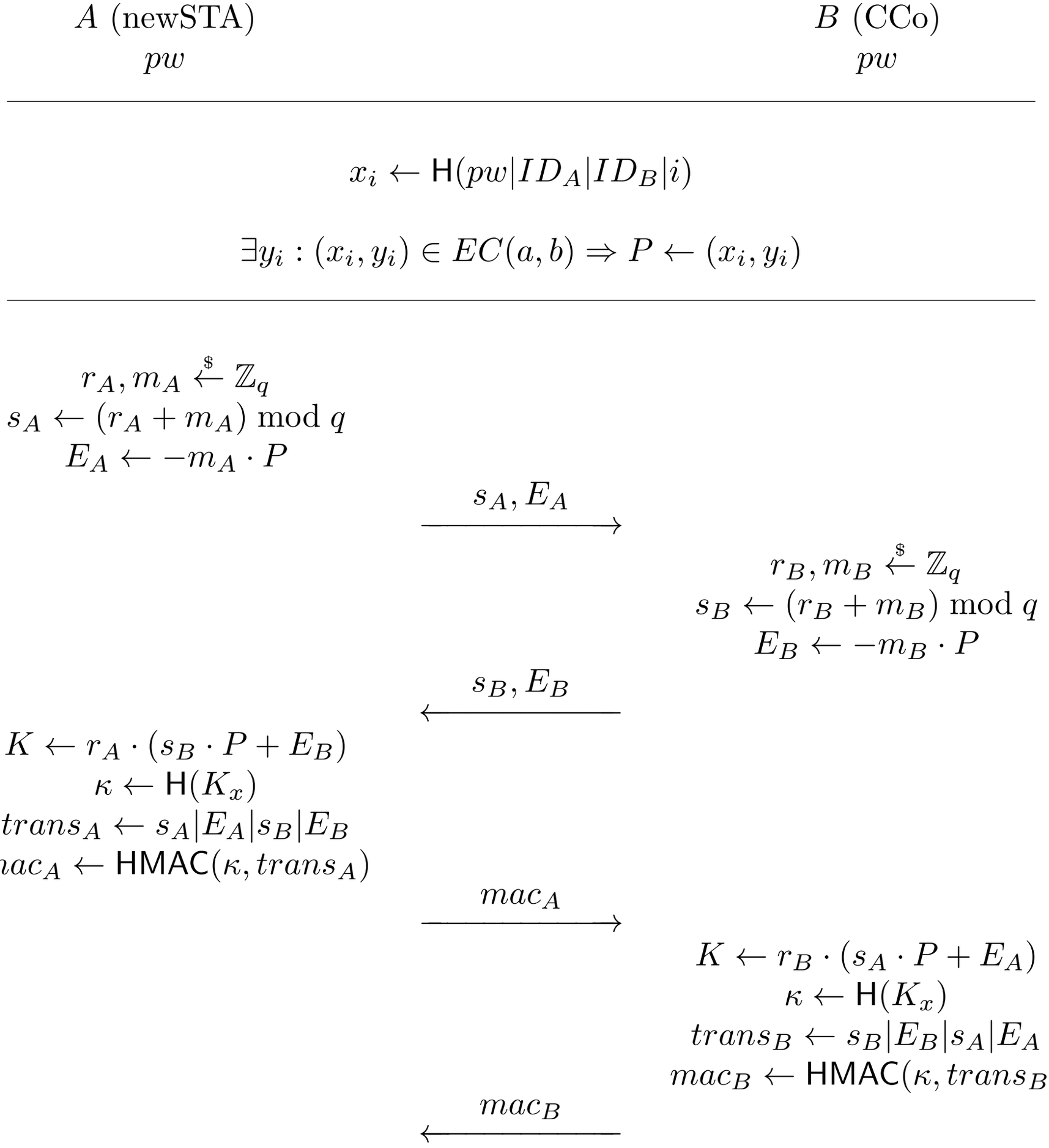
A (newSTA)
pw
B (CCo)
pw
$x_i \leftarrow \mathsf{H}(pw|ID_A|ID_B|i)$
$\exists y_i : (x_i, y_i) \in EC(a,b) \Rightarrow P \leftarrow (x_i, y_i)$
$r_A, m_A \xleftarrow{\$} \mathbb{Z}_q$
$s_A \leftarrow (r_A + m_A) \bmod q$
$E_A \leftarrow -m_A \cdot P$
s_A, E_A
$r_B, m_B \xleftarrow{\$} \mathbb{Z}_q$
$s_B \leftarrow (r_B + m_B) \bmod q$
$E_B \leftarrow -m_B \cdot P$
s_B, E_B
$K \leftarrow r_A \cdot (s_B \cdot P + E_B)$
$\kappa \leftarrow \mathsf{H}(K_x)$
$trans_A \leftarrow s_A|E_A|s_B|E_B$
$mac_A \leftarrow \mathsf{HMAC}(\kappa, trans_A)$
mac_A
$K \leftarrow r_B \cdot (s_A \cdot P + E_A)$
$\kappa \leftarrow \mathsf{H}(K_x)$
$trans_B \leftarrow s_B|E_B|s_A|E_A$
$mac_B \leftarrow \mathsf{HMAC}(\kappa, trans_B)$
mac_B