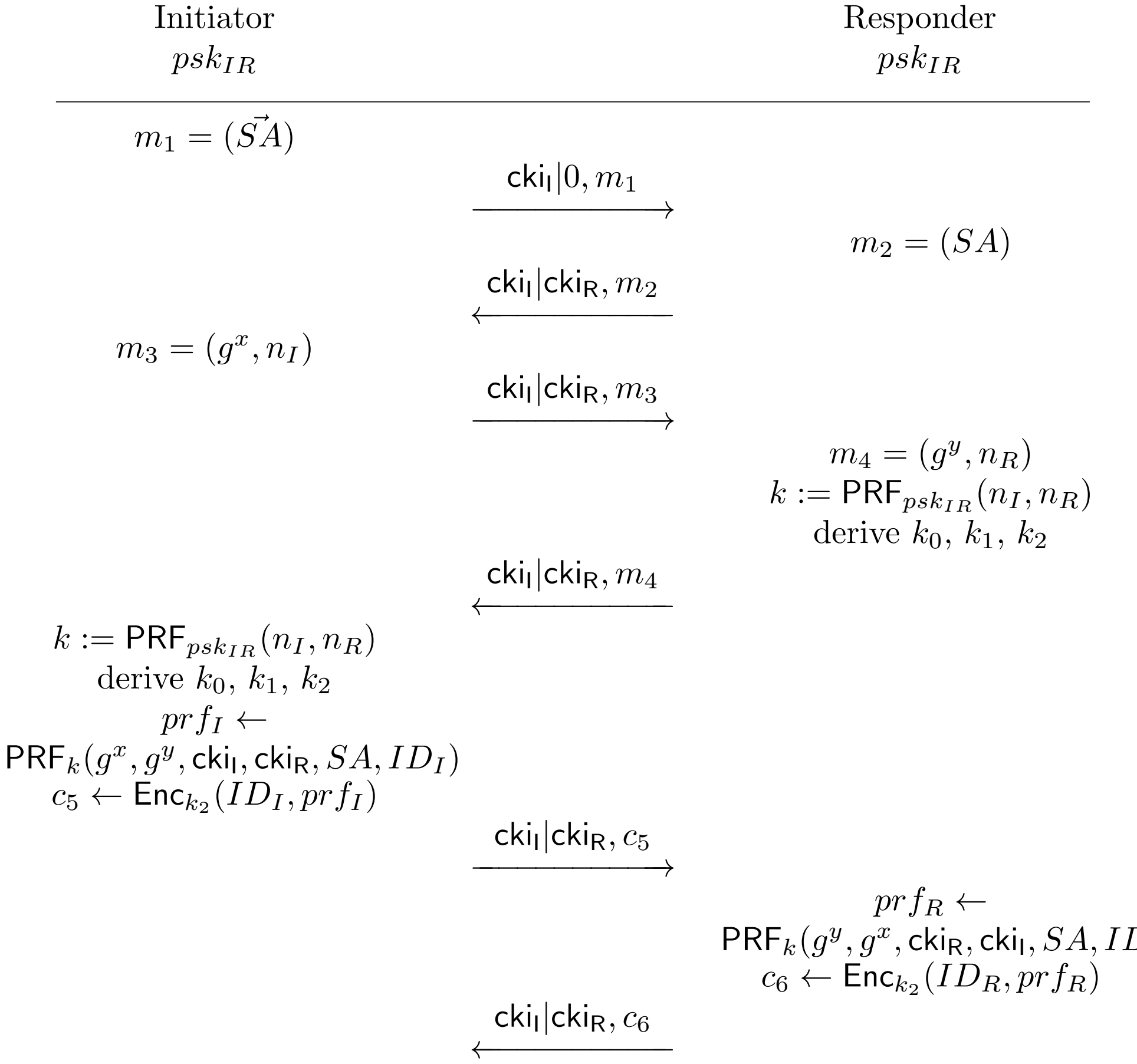
Initiator
psk_{IR}
Responder
psk_{IR}
$m_1 = (\vec{SA})$
$\mathsf{cki_I}|0, m_1$
$m_2 = (SA)$
$\mathsf{cki_I}|\mathsf{cki_R}, m_2$
$m_3 = (g^x, n_I)$
$\mathsf{cki_I}|\mathsf{cki_R}, m_3$
$m_4 = (g^y, n_R)$
$k := \mathsf{PRF}_{psk_{IR}}(n_I, n_R)$
derive k_0, k_1, k_2
$\mathsf{cki_I}|\mathsf{cki_R}, m_4$
$k := \mathsf{PRF}_{psk_{IR}}(n_I, n_R)$
derive k_0, k_1, k_2
$prf_I \leftarrow$
$\mathsf{PRF}_k(g^x, g^y, \mathsf{cki_I}, \mathsf{cki_R}, SA, ID_I)$
$c_5 \leftarrow \mathsf{Enc}_{k_2}(ID_I, prf_I)$
$\mathsf{cki_I}|\mathsf{cki_R}, c_5$
$prf_R \leftarrow$
$\mathsf{PRF}_k(g^y, g^x, \mathsf{cki_R}, \mathsf{cki_I}, SA, ID_I$
$c_6 \leftarrow \mathsf{Enc}_{k_2}(ID_R, prf_R)$
$\mathsf{cki_I}|\mathsf{cki_R}, c_6$