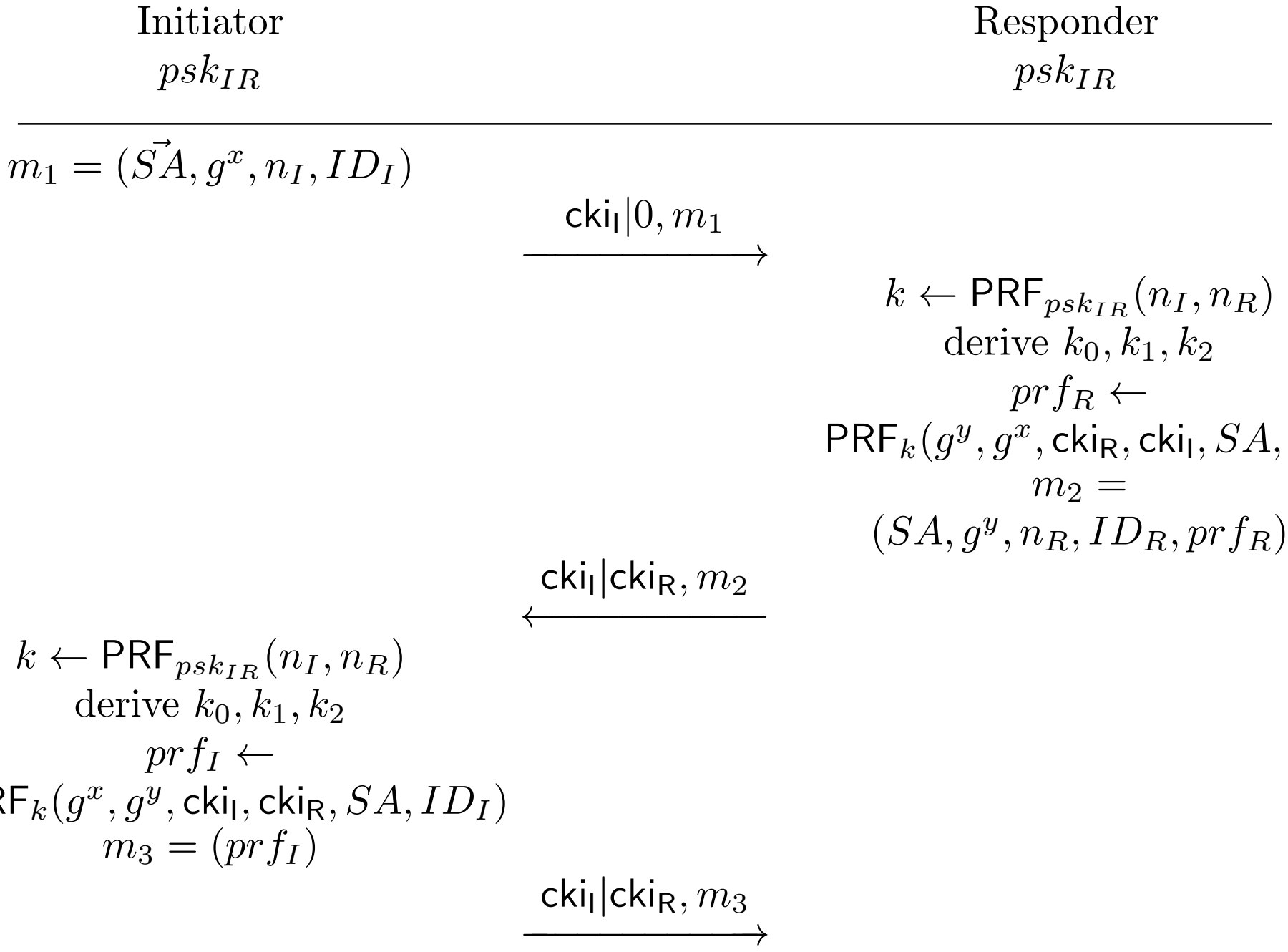
Initiator
psk_{IR}
Responder
psk_{IR}
$m_1 = (\vec{SA}, g^x, n_I, ID_I)$
$\mathsf{cki_I}|0, m_1$
$k \leftarrow \mathsf{PRF}_{psk_{IR}}(n_I, n_R)$
derive k_0, k_1, k_2
$prf_R \leftarrow$
$\mathsf{PRF}_k(g^y, g^x, \mathsf{cki_R}, \mathsf{cki_I}, SA, ID_I$
$m_2 =$
$(SA, g^y, n_R, ID_R, prf_R)$
$\mathsf{cki_I}|\mathsf{cki_R},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