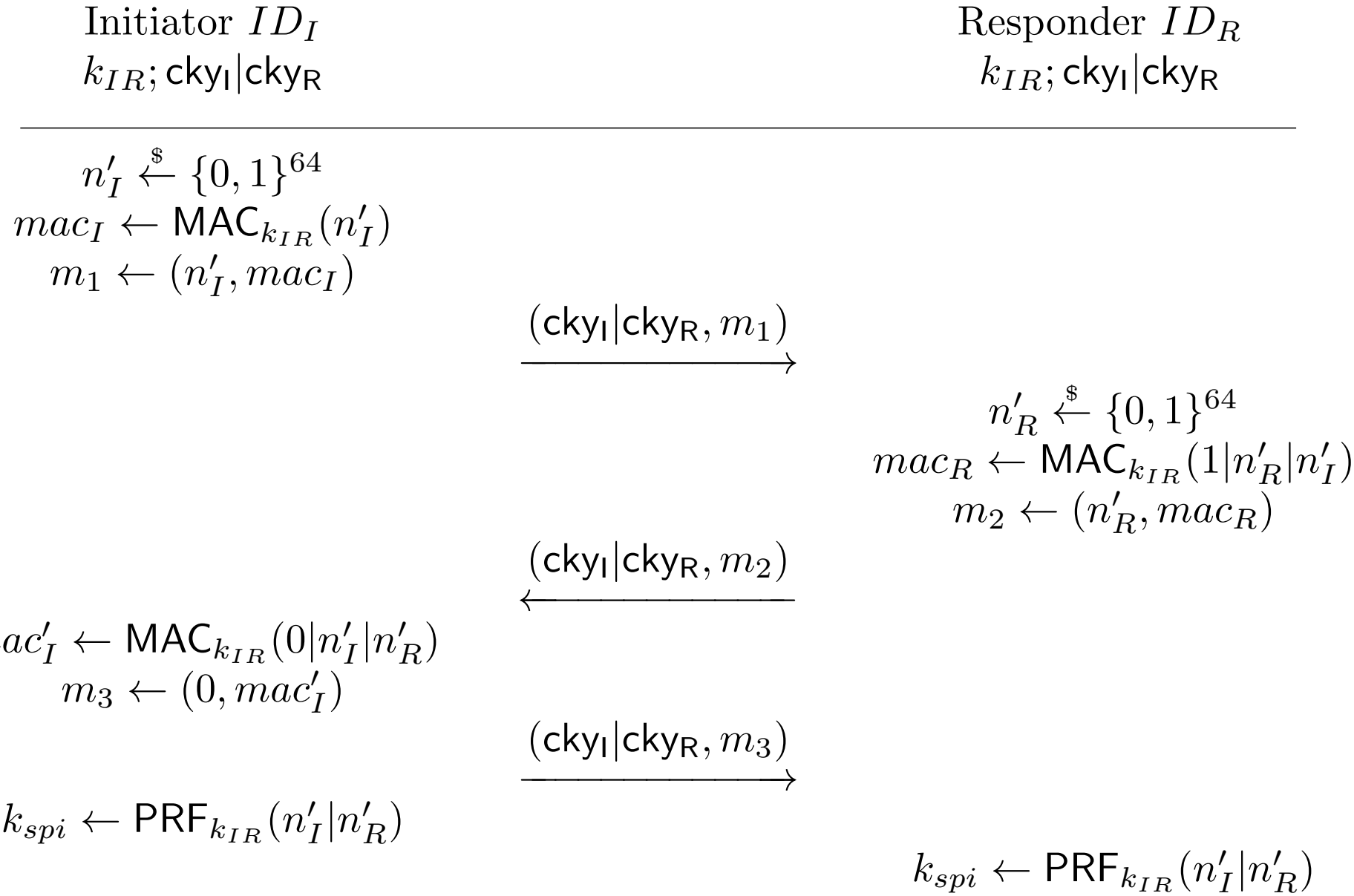
Initiator ID_I
k_{IR}; $\mathsf{cky_I}|\mathsf{cky_R}$
Responder ID_R
k_{IR}; $\mathsf{cky_I}|\mathsf{cky_R}$
$n'_I \xleftarrow{\$} \{0,1\}^{64}$
$mac_I \leftarrow \mathsf{MAC}_{k_{IR}}(n'_I)$
$m_1 \leftarrow (n'_I, mac_I)$
$(\mathsf{cky_I}|\mathsf{cky_R}, m_1)$
$n'_R \xleftarrow{\$} \{0,1\}^{64}$
$mac_R \leftarrow \mathsf{MAC}_{k_{IR}}(1|n'_R|n'_I)$
$m_2 \leftarrow (n'_R, mac_R)$
$(\mathsf{cky_I}|\mathsf{cky_R}, m_2)$
$mac'_I \leftarrow \mathsf{MAC}_{k_{IR}}(0|n'_I|n'_R)$
$m_3 \leftarrow (0, mac'_I)$
$(\mathsf{cky_I}|\mathsf{cky_R}, m_3)$
$k_{spi} \leftarrow \mathsf{PRF}_{k_{IR}}(n'_I|n'_R)$
$k_{spi} \leftarrow \mathsf{PRF}_{k_{IR}}(n'_I|n'_R)$