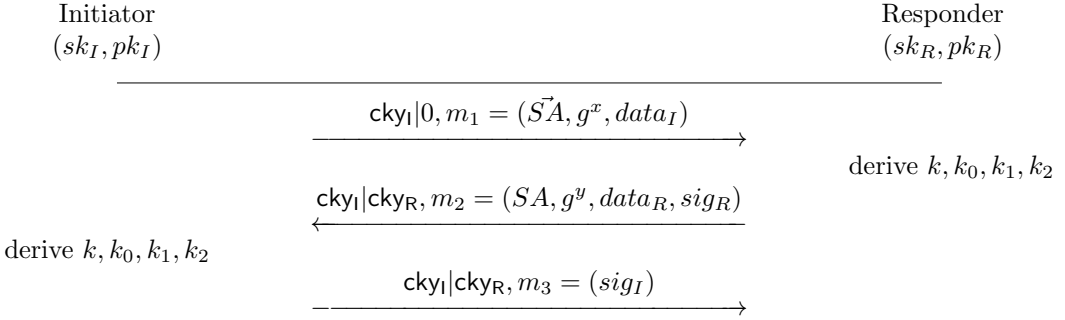
Initiator
$(sk_I, pk_I)$
Responder
$(sk_R, pk_R)$
$\mathsf{cky_I}|0, m_1 = (\vec{SA}, g^x, data_I)$
derive $k, k_0, k_1, k_2$
$\mathsf{cky_I}|\mathsf{cky_R}, m_2 = (SA, g^y, data_R, sig_R)$
derive $k, k_0, k_1, k_2$
$\mathsf{cky_I}|\mathsf{cky_R}, m_3 = (sig_I)$