
Initiator
(sk_I, pk_I)
(k_0, k_1, k_2), $(\mathsf{cky_I}|\mathsf{cky_R})$
Responder
(sk_R, pk_R)
(k_0, k_1, k_2), $(\mathsf{cky_I}|\mathsf{cky_R})$
$\mathsf{cky_I}|\mathsf{cky_R}, c_1 = \mathsf{Enc}_{k_2}(mac'_1, \overrightarrow{SA'}, n'_I[, g^{x'}])$
$\mathsf{cky_I}|\mathsf{cky_R}, c_2 = \mathsf{Enc}_{k_2}(mac'_2, SA', n'_R[, g^{y'}])$
$\mathsf{cky_I}|\mathsf{cky_R}, c_3 = \mathsf{Enc}_{k_2}(mac'_3)$
derive k_{SPI}