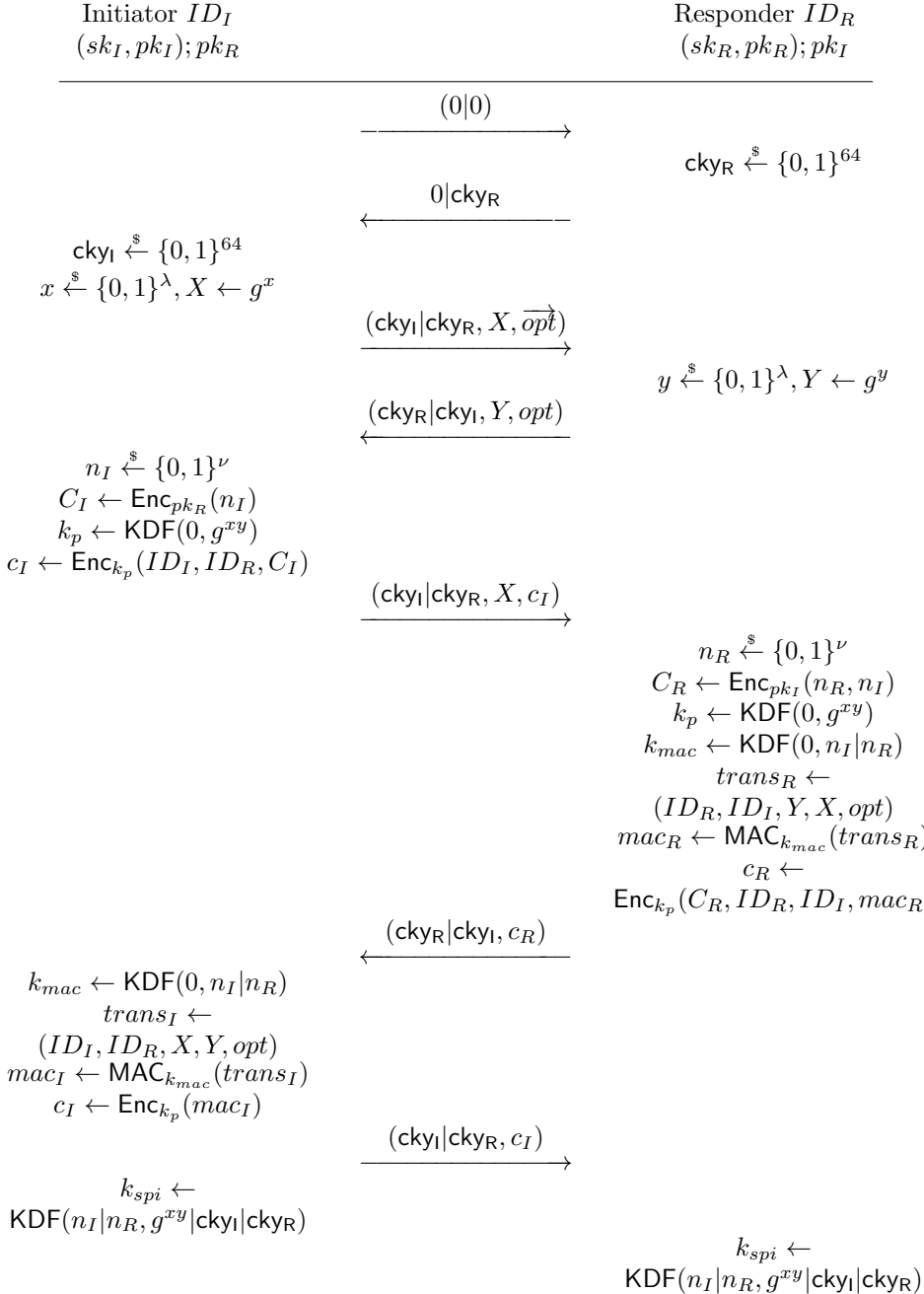
Initiator ID_I
$(sk_I, pk_I); pk_R$
Responder ID_R
$(sk_R, pk_R); pk_I$
$(0|0)$
$\mathsf{cky_R} \xleftarrow{\$} \{0,1\}^{64}$
$0|\mathsf{cky_R}$
$\mathsf{cky_I} \xleftarrow{\$} \{0,1\}^{64}$
$x \xleftarrow{\$} \{0,1\}^{\lambda}, X \leftarrow g^x$
$(\mathsf{cky_I}|\mathsf{cky_R}, X, \overrightarrow{opt})$
$y \xleftarrow{\$} \{0,1\}^{\lambda}, Y \leftarrow g^y$
$(\mathsf{cky_R}|\mathsf{cky_I}, Y, opt)$
$n_I \xleftarrow{\$} \{0,1\}^{\nu}$
$C_I \leftarrow \mathsf{Enc}_{pk_R}(n_I)$
$k_p \leftarrow \mathsf{KDF}(0, g^{xy})$
$c_I \leftarrow \mathsf{Enc}_{k_p}(ID_I, ID_R, C_I)$
$(\mathsf{cky_I}|\mathsf{cky_R}, X, c_I)$
$n_R \xleftarrow{\$} \{0,1\}^{\nu}$
$C_R \leftarrow \mathsf{Enc}_{pk_I}(n_R, n_I)$
$k_p \leftarrow \mathsf{KDF}(0, g^{xy})$
$k_{mac} \leftarrow \mathsf{KDF}(0, n_I|n_R)$
$trans_R \leftarrow$
(ID_R, ID_I, Y, X, opt)
$mac_R \leftarrow \mathsf{MAC}_{k_{mac}}(trans_R)$
$c_R \leftarrow$
$\mathsf{Enc}_{k_p}(C_R, ID_R, ID_I, mac_R)$
$(\mathsf{cky_R}|\mathsf{cky_I}, c_R)$
$k_{mac} \leftarrow \mathsf{KDF}(0, n_I|n_R)$
$trans_I \leftarrow$
(ID_I, ID_R, X, Y, opt)
$mac_I \leftarrow \mathsf{MAC}_{k_{mac}}(trans_I)$
$c_I \leftarrow \mathsf{Enc}_{k_p}(mac_I)$
$(\mathsf{cky_I}|\mathsf{cky_R}, c_I)$
$k_{spi} \leftarrow$
$\mathsf{KDF}(n_I|n_R, g^{xy}|\mathsf{cky_I}|\mathsf{cky_R})$
$k_{spi} \leftarrow$
$\mathsf{KDF}(n_I|n_R, g^{xy}|\mathsf{cky_I}|\mathsf{cky_R})$