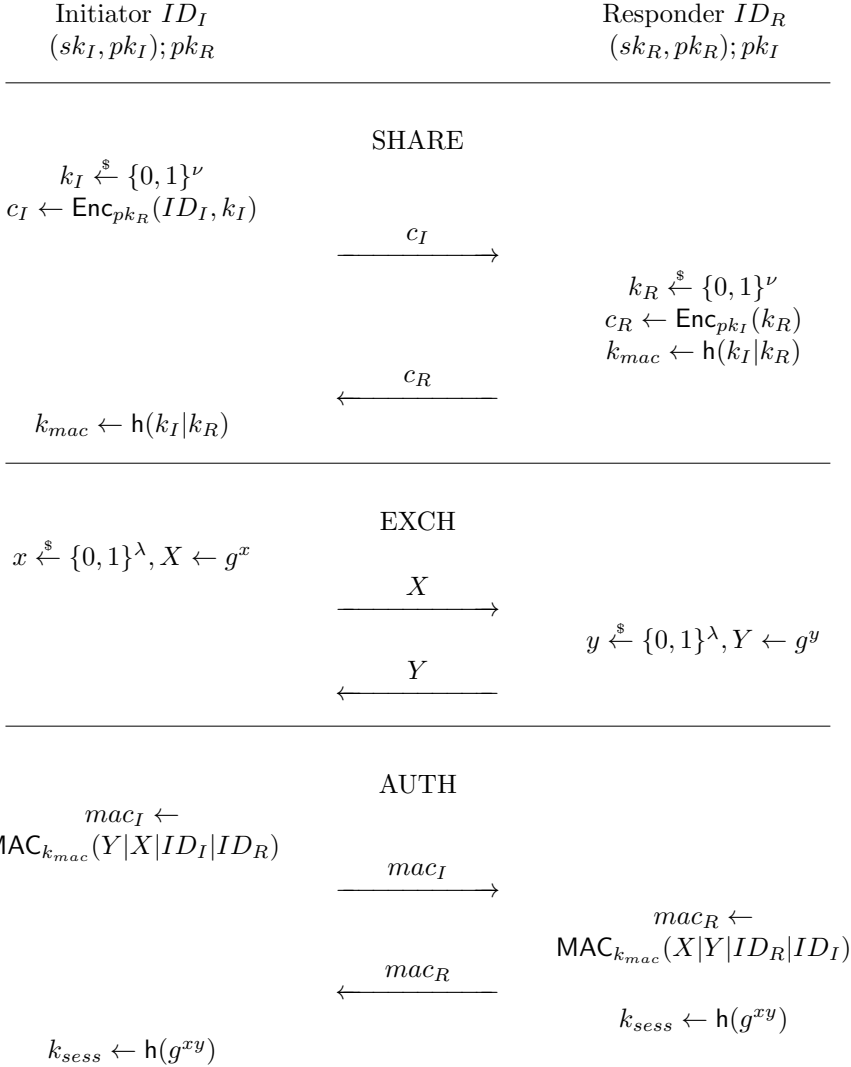
Initiator ID_I
$(sk_I, pk_I); pk_R$
Responder ID_R
$(sk_R, pk_R); pk_I$
SHARE
$k_I \xleftarrow{\$} \{0,1\}^\nu$
$c_I \leftarrow \mathsf{Enc}_{pk_R}(ID_I, k_I)$
c_I
$k_R \xleftarrow{\$} \{0,1\}^\nu$
$c_R \leftarrow \mathsf{Enc}_{pk_I}(k_R)$
$k_{mac} \leftarrow \mathsf{h}(k_I|k_R)$
c_R
$k_{mac} \leftarrow \mathsf{h}(k_I|k_R)$
EXCH
$x \xleftarrow{\$} \{0,1\}^\lambda, X \leftarrow g^x$
X
$y \xleftarrow{\$} \{0,1\}^\lambda, Y \leftarrow g^y$
Y
AUTH
$mac_I \leftarrow$
$\mathsf{MAC}_{k_{mac}}(Y|X|ID_I|ID_R)$
mac_I
$mac_R \leftarrow$
$\mathsf{MAC}_{k_{mac}}(X|Y|ID_R|ID_I)$
mac_R
$k_{sess} \leftarrow \mathsf{h}(g^{xy})$
$k_{sess} \leftarrow \mathsf{h}(g^{xy})$