

Initiator ID_I
 $(sk_I, pk_I); pk_R$

Responder ID_R
 $(sk_R, pk_R); pk_I$

SHARE, EXCH, AUTH

$k_I \xleftarrow{\$} \{0, 1\}^\nu$
 $c_I \leftarrow \text{Enc}_{pk_R}(ID_I, k_I)$
 $x \xleftarrow{\$} \{0, 1\}^\lambda, X \leftarrow g^x$

$\xrightarrow{c_I, X}$

$k_R \xleftarrow{\$} \{0, 1\}^\nu$
 $c_R \leftarrow \text{Enc}_{pk_I}(k_R)$
 $k_{mac} \leftarrow h(k_I|k_R)$
 $y \xleftarrow{\$} \{0, 1\}^\lambda, Y \leftarrow g^y$
 $mac_R \leftarrow$
 $\text{MAC}_{k_{mac}}(X|Y|ID_R|ID_I)$

$\xleftarrow{c_R, Y, mac_R}$

$k_{mac} \leftarrow h(k_I|k_R)$
 $mac_I \leftarrow$
 $\text{MAC}_{k_{mac}}(Y|X|ID_I|ID_R)$

$\xrightarrow{mac_I}$

$k_{sess} \leftarrow \text{KDF}(g^{xy})$

$k_{sess} \leftarrow \text{KDF}(g^{xy})$