Initiator ID_I $(sk_I, pk_I); pk_R$		Responder ID_R $(sk_R, pk_R); pk_I$
$\mathsf{cky_I} \overset{\$}{\leftarrow} \{0,1\}^{64}$ $n_I \overset{\$}{\leftarrow} \{0,1\}^{\nu}$ $x \overset{\$}{\leftarrow} \{0,1\}^{\lambda}, X \leftarrow g^x$ $m_1 \leftarrow$ $(X, \vec{opt}, ID_I, ID_R, n_I, 0)$ $trans_1 \leftarrow$ $(ID_I \| ID_R \| n_I \| 0 \| X \| 0 \| \vec{opt})$ $\sigma_1 \leftarrow \mathsf{Sign}_{sk_I}(trans_1)$ $m_1' \leftarrow (m_1, \sigma_1)$		
	$\xrightarrow{(\mathsf{cky_I} \| 0, m_1')}$	
		$\mathsf{cky_R} \overset{\$}{\leftarrow} \{0,1\}^{64}$ $n_R \overset{\$}{\leftarrow} \{0,1\}^{\nu}$ $y \overset{\$}{\leftarrow} \{0,1\}^{\lambda}, Y \leftarrow g^y$ $m_2 \leftarrow$ $(Y, opt, ID_R, ID_I, n_R, n_I)$ $trans_2 \leftarrow$ $(ID_R \| ID_I \| n_R \| n_I \| Y \| X \| opt)$ $\sigma_2 \leftarrow \mathsf{Sign}_{sk_R}(trans_2)$ $m_2' \leftarrow (m_2, \sigma_2)$
	$\xleftarrow{(\mathsf{cky_I} \| \mathsf{cky_R}, m_2')}$	
$m_3 \leftarrow$ $(X, opt, ID_I, ID_R, n_I, n_R)$ $trans_3 \leftarrow$ $(ID_I \| ID_R \| n_I \| n_R \| X \| Y \| opt)$ $\sigma_3 \leftarrow \mathsf{Sign}_{sk_I}(trans_3)$ $m_3' \leftarrow (m_3, \sigma_3)$		
	$\xrightarrow{(\mathsf{cky_I} \| \mathsf{cky_R}, m_3')}$	
$k_{spi} \leftarrow$ $\mathsf{KDF}(n_I \| n_R, g^{xy} \| \mathsf{cky_I} \| \mathsf{cky_R})$		
		$k_{spi} \leftarrow$ $\mathsf{KDF}(n_I \| n_R, g^{xy} \| \mathsf{cky_I} \| \mathsf{cky_R})$