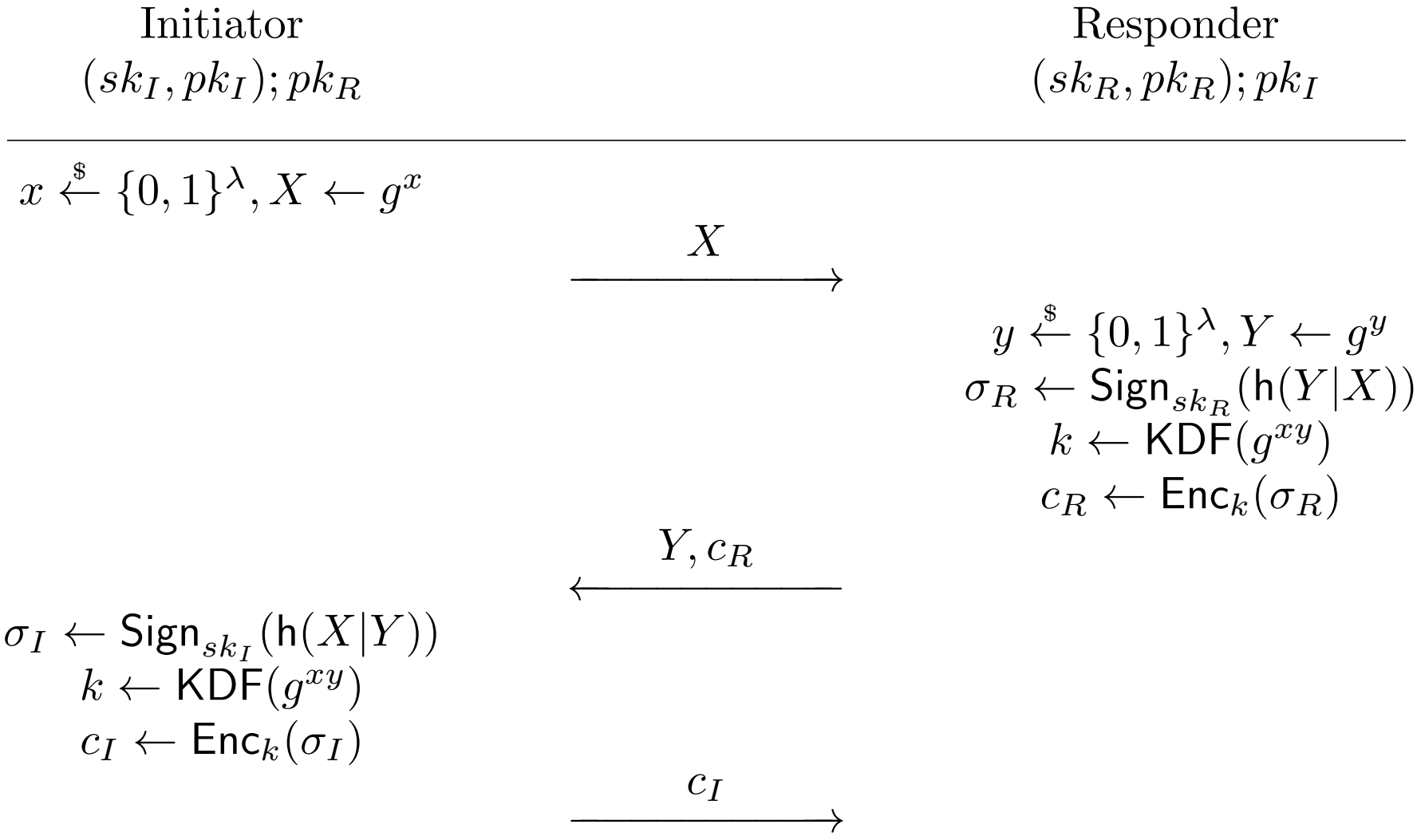
Initiator
$(sk_I, pk_I); pk_R$
Responder
$(sk_R, pk_R); pk_I$
$x \xleftarrow{\$} \{0,1\}^\lambda, X \leftarrow g^x$
X
$y \xleftarrow{\$} \{0,1\}^\lambda, Y \leftarrow g^y$
$\sigma_R \leftarrow \mathsf{Sign}_{sk_R}(\mathsf{h}(Y|X))$
$k \leftarrow \mathsf{KDF}(g^{xy})$
$c_R \leftarrow \mathsf{Enc}_k(\sigma_R)$
Y, c_R
$\sigma_I \leftarrow \mathsf{Sign}_{sk_I}(\mathsf{h}(X|Y))$
$k \leftarrow \mathsf{KDF}(g^{xy})$
$c_I \leftarrow \mathsf{Enc}_k(\sigma_I)$
c_I