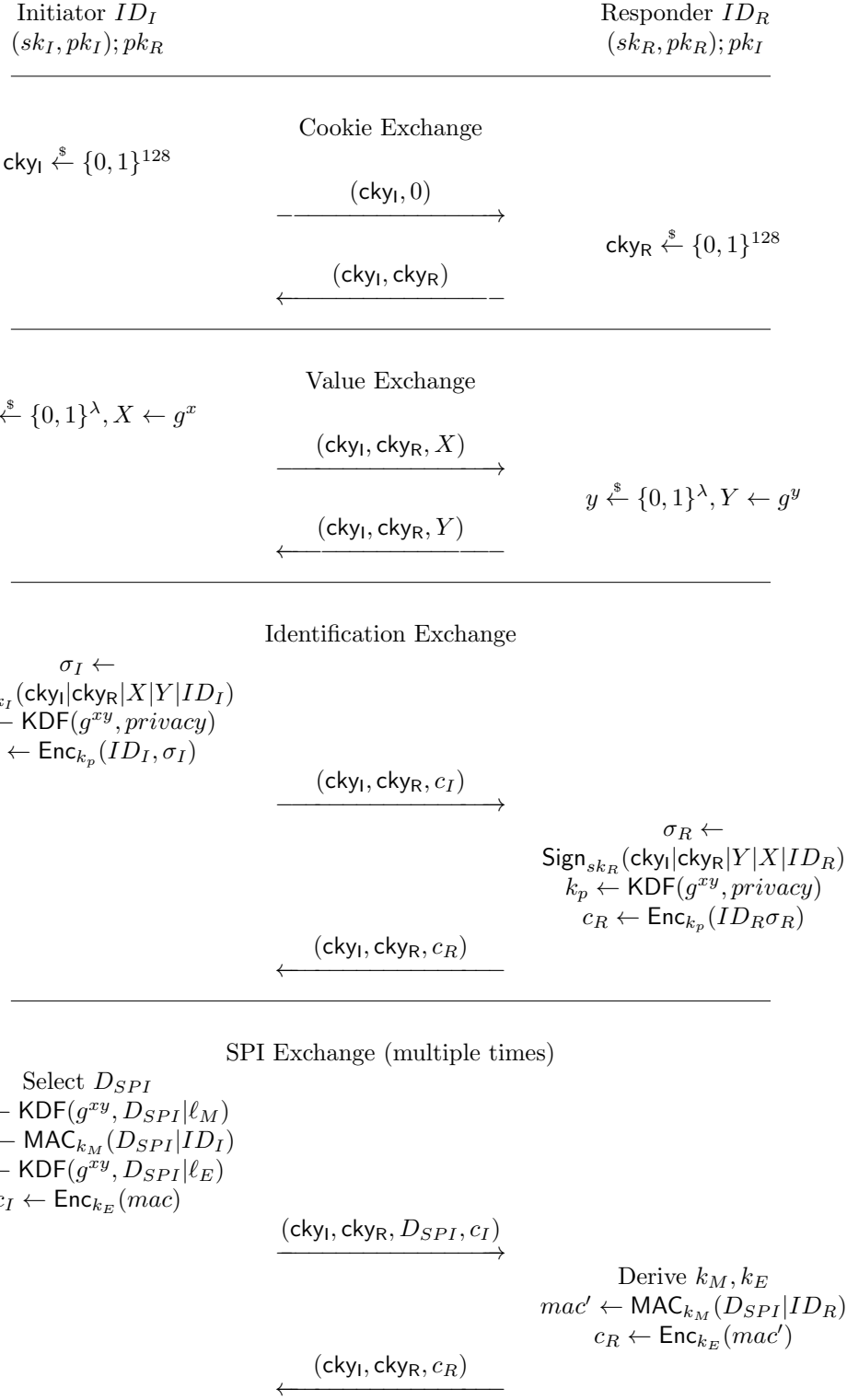
Initiator ID_I
$(sk_I, pk_I); pk_R$
Responder ID_R
$(sk_R, pk_R); pk_I$
Cookie Exchange
$\mathsf{cky_I} \xleftarrow{\$} \{0,1\}^{128}$
$(\mathsf{cky_I}, 0)$
$\mathsf{cky_R} \xleftarrow{\$} \{0,1\}^{128}$
$(\mathsf{cky_I}, \mathsf{cky_R})$
Value Exchange
$x \xleftarrow{\$} \{0,1\}^{\lambda}, X \leftarrow g^x$
$(\mathsf{cky_I}, \mathsf{cky_R}, X)$
$y \xleftarrow{\$} \{0,1\}^{\lambda}, Y \leftarrow g^y$
$(\mathsf{cky_I}, \mathsf{cky_R}, Y)$
Identification Exchange
$\sigma_I \leftarrow$
$\mathsf{Sign}_{sk_I}(\mathsf{cky_I}|\mathsf{cky_R}|X|Y|ID_I)$
$k_p \leftarrow \mathsf{KDF}(g^{xy}, privacy)$
$c_I \leftarrow \mathsf{Enc}_{k_p}(ID_I, \sigma_I)$
$(\mathsf{cky_I}, \mathsf{cky_R}, c_I)$
$\sigma_R \leftarrow$
$\mathsf{Sign}_{sk_R}(\mathsf{cky_I}|\mathsf{cky_R}|Y|X|ID_R)$
$k_p \leftarrow \mathsf{KDF}(g^{xy}, privacy)$
$c_R \leftarrow \mathsf{Enc}_{k_p}(ID_R\sigma_R)$
$(\mathsf{cky_I}, \mathsf{cky_R}, c_R)$
SPI Exchange (multiple times)
Select D_{SPI}
$k_M \leftarrow \mathsf{KDF}(g^{xy}, D_{SPI}|\ell_M)$
$mac \leftarrow \mathsf{MAC}_{k_M}(D_{SPI}|ID_I)$
$k_E \leftarrow \mathsf{KDF}(g^{xy}, D_{SPI}|\ell_E)$
$c_I \leftarrow \mathsf{Enc}_{k_E}(mac)$
$(\mathsf{cky_I}, \mathsf{cky_R}, D_{SPI}, c_I)$
Derive k_M, k_E
$mac' \leftarrow \mathsf{MAC}_{k_M}(D_{SPI}|ID_R)$
$c_R \leftarrow \mathsf{Enc}_{k_E}(mac')$
$(\mathsf{cky_I}, \mathsf{cky_R}, c_R)$