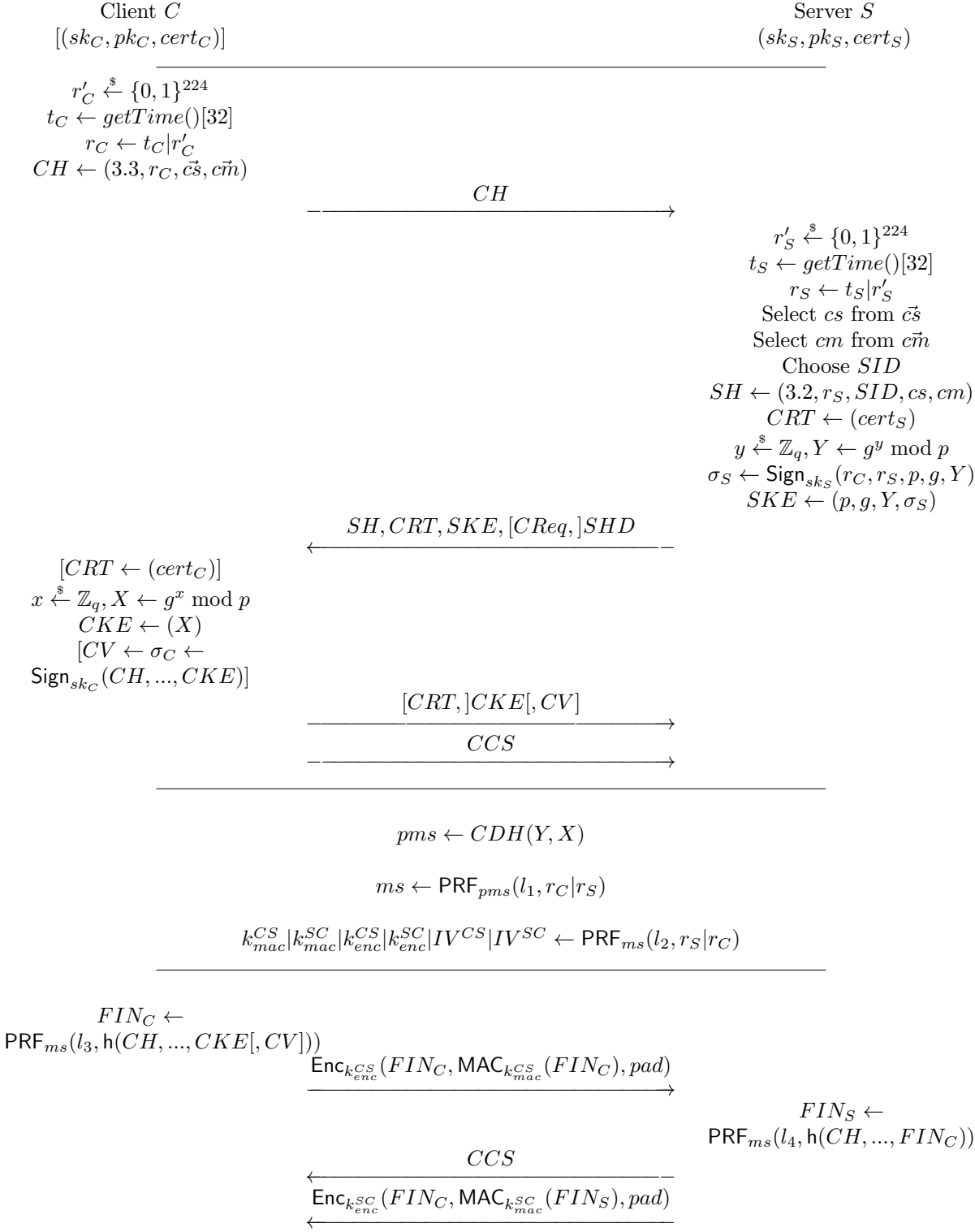
Client C
$[(sk_C, pk_C, cert_C)]$
Server S
$(sk_S, pk_S, cert_S)$
$r'_C \xleftarrow{\$} \{0,1\}^{224}$
$t_C \leftarrow getTime()[32]$
$r_C \leftarrow t_C | r'_C$
$CH \leftarrow (3.3, r_C, \vec{cs}, \vec{cm})$
CH
$r'_S \xleftarrow{\$} \{0,1\}^{224}$
$t_S \leftarrow getTime()[32]$
$r_S \leftarrow t_S | r'_S$
Select cs from $\vec{cs}$
Select cm from $\vec{cm}$
Choose SID
$SH \leftarrow (3.2, r_S, SID, cs, cm)$
$CRT \leftarrow (cert_S)$
$y \xleftarrow{\$} \mathbb{Z}_q, Y \leftarrow g^y \bmod p$
$\sigma_S \leftarrow \mathsf{Sign}_{sk_S}(r_C, r_S, p, g, Y)$
$SKE \leftarrow (p, g, Y, \sigma_S)$
$SH, CRT, SKE, [CReq,]SHD$
$[CRT \leftarrow (cert_C)]$
$x \xleftarrow{\$} \mathbb{Z}_q, X \leftarrow g^x \bmod p$
$CKE \leftarrow (X)$
$[CV \leftarrow \sigma_C \leftarrow$
$\mathsf{Sign}_{sk_C}(CH, ..., CKE)]$
$[CRT,]CKE[, CV]$
CCS
$pms \leftarrow CDH(Y, X)$
$ms \leftarrow \mathsf{PRF}_{pms}(l_1, r_C | r_S)$
$k^{CS}_{mac} | k^{SC}_{mac} | k^{CS}_{enc} | k^{SC}_{enc} | IV^{CS} | IV^{SC} \leftarrow \mathsf{PRF}_{ms}(l_2, r_S | r_C)$
$FIN_C \leftarrow$
$\mathsf{PRF}_{ms}(l_3, \mathsf{h}(CH, ..., CKE[, CV]))$
$\mathsf{Enc}_{k^{CS}_{enc}}(FIN_C, \mathsf{MAC}_{k^{CS}_{mac}}(FIN_C), pad)$
$FIN_S \leftarrow$
$\mathsf{PRF}_{ms}(l_4, \mathsf{h}(CH, ..., FIN_C))$
CCS
$\mathsf{Enc}_{k^{SC}_{enc}}(FIN_C, \mathsf{MAC}_{k^{SC}_{mac}}(FIN_S), pad)$