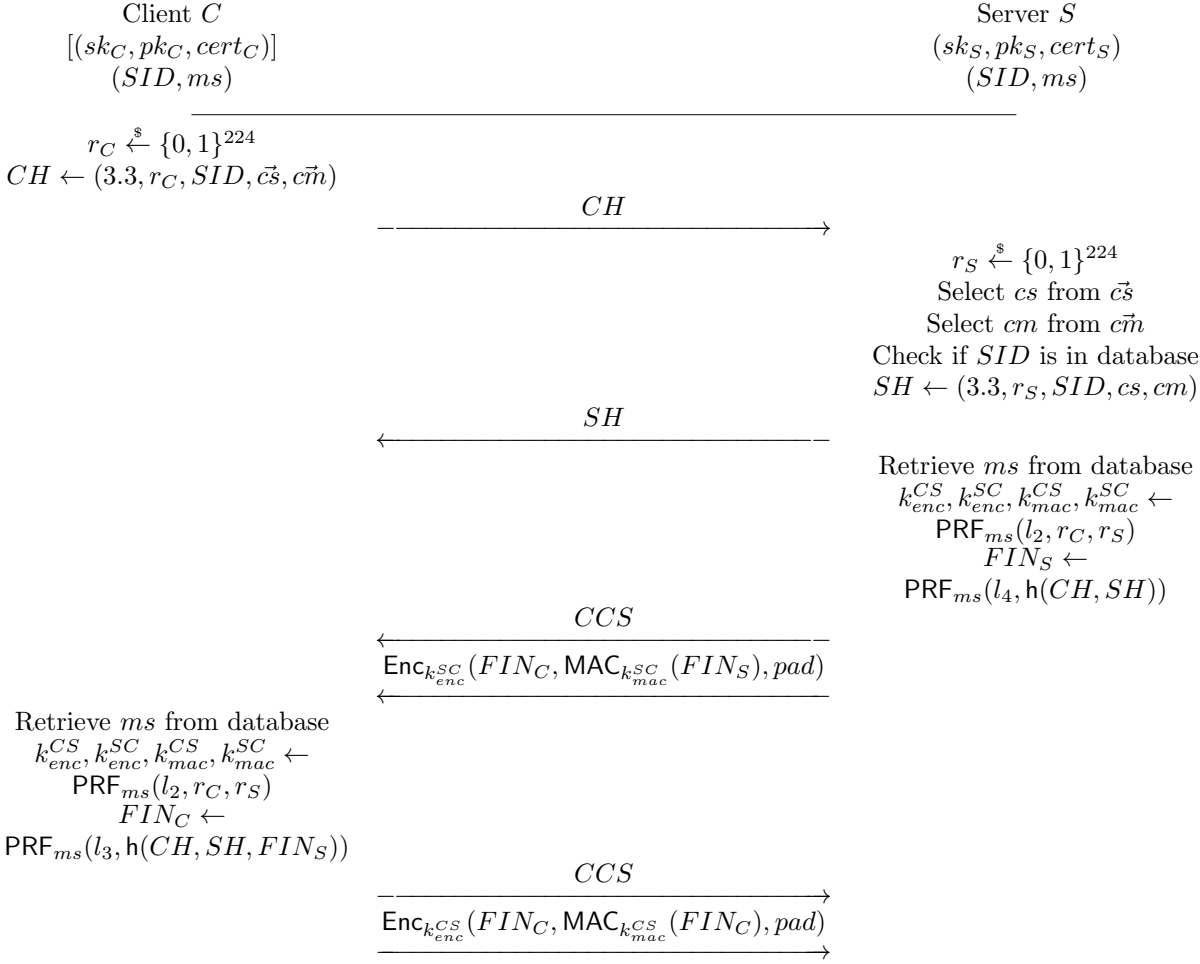
Client C
$[(sk_C, pk_C, cert_C)]$
(SID, ms)
Server S
$(sk_S, pk_S, cert_S)$
(SID, ms)
$r_C \xleftarrow{\$} \{0,1\}^{224}$
$CH \leftarrow (3.3, r_C, SID, \vec{cs}, \vec{cm})$
CH
$r_S \xleftarrow{\$} \{0,1\}^{224}$
Select cs from $\vec{cs}$
Select cm from $\vec{cm}$
Check if SID is in database
$SH \leftarrow (3.3, r_S, SID, cs, cm)$
SH
Retrieve ms from database
$k_{enc}^{CS}, k_{enc}^{SC}, k_{mac}^{CS}, k_{mac}^{SC} \leftarrow$
$\mathsf{PRF}_{ms}(l_2, r_C, r_S)$
$FIN_S \leftarrow$
$\mathsf{PRF}_{ms}(l_4, \mathsf{h}(CH, SH))$
CCS
$\mathsf{Enc}_{k_{enc}^{SC}}(FIN_C, \mathsf{MAC}_{k_{mac}^{SC}}(FIN_S), pad)$
Retrieve ms from database
$k_{enc}^{CS}, k_{enc}^{SC}, k_{mac}^{CS}, k_{mac}^{SC} \leftarrow$
$\mathsf{PRF}_{ms}(l_2, r_C, r_S)$
$FIN_C \leftarrow$
$\mathsf{PRF}_{ms}(l_3, \mathsf{h}(CH, SH, FIN_S))$
CCS
$\mathsf{Enc}_{k_{enc}^{CS}}(FIN_C, \mathsf{MAC}_{k_{mac}^{CS}}(FIN_C), pad)$