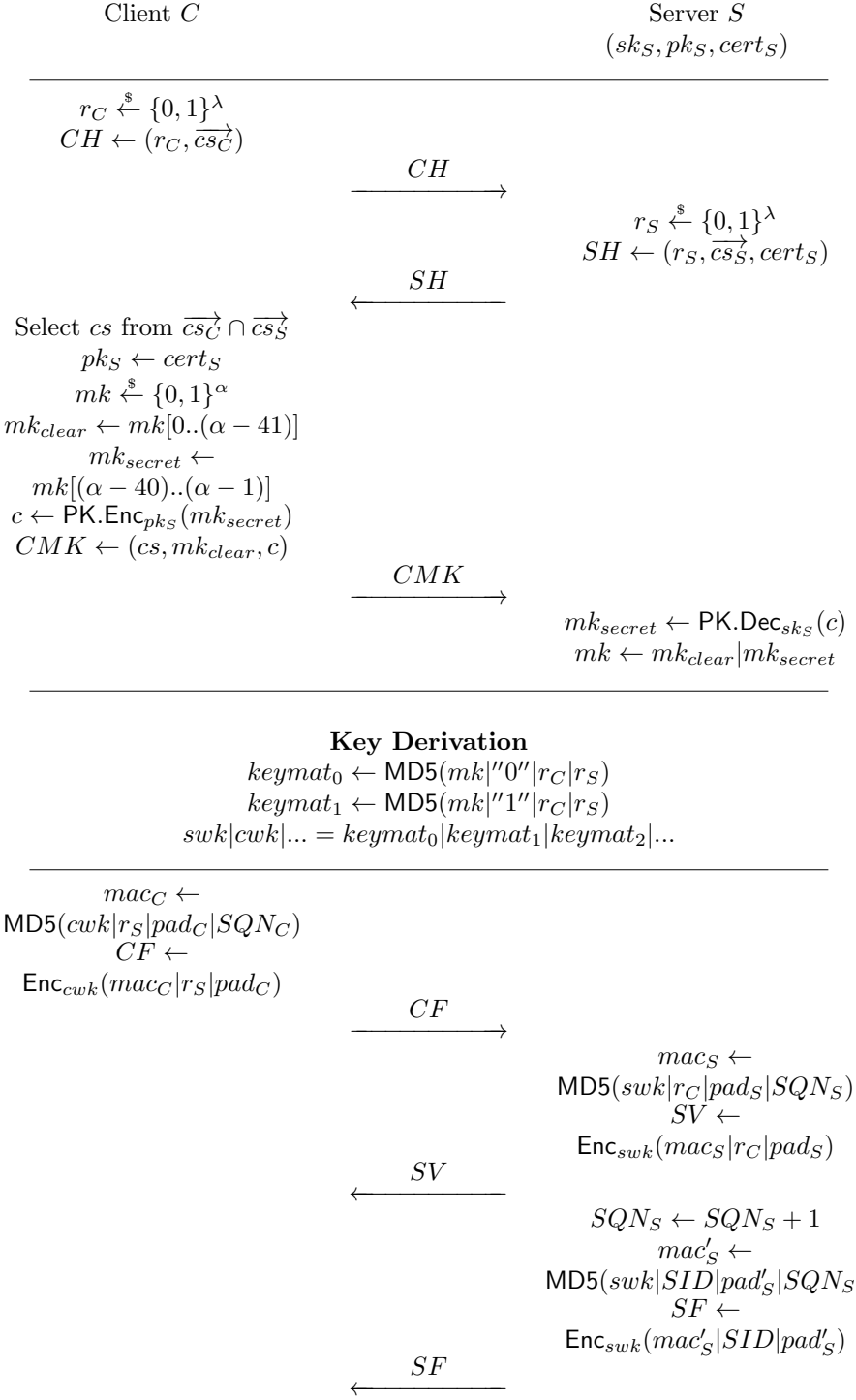
Client C
Server S
$(sk_S, pk_S, cert_S)$
$r_C \xleftarrow{\$} \{0,1\}^\lambda$
$CH \leftarrow (r_C, \overrightarrow{cs_C})$
CH
$r_S \xleftarrow{\$} \{0,1\}^\lambda$
$SH \leftarrow (r_S, \overrightarrow{cs_S}, cert_S)$
SH
Select cs from $\overrightarrow{cs_C} \cap \overrightarrow{cs_S}$
$pk_S \leftarrow cert_S$
$mk \xleftarrow{\$} \{0,1\}^\alpha$
$mk_{clear} \leftarrow mk[0..(\alpha - 41)]$
$mk_{secret} \leftarrow$
$mk[(\alpha - 40)..(\alpha - 1)]$
$c \leftarrow \mathsf{PK.Enc}_{pk_S}(mk_{secret})$
$CMK \leftarrow (cs, mk_{clear}, c)$
CMK
$mk_{secret} \leftarrow \mathsf{PK.Dec}_{sk_S}(c)$
$mk \leftarrow mk_{clear}|mk_{secret}$
Key Derivation
$keymat_0 \leftarrow \mathsf{MD5}(mk|''0''|r_C|r_S)$
$keymat_1 \leftarrow \mathsf{MD5}(mk|''1''|r_C|r_S)$
$swk|cwk|... = keymat_0|keymat_1|keymat_2|...$
$mac_C \leftarrow$
$\mathsf{MD5}(cwk|r_S|pad_C|SQN_C)$
$CF \leftarrow$
$\mathsf{Enc}_{cwk}(mac_C|r_S|pad_C)$
CF
$mac_S \leftarrow$
$\mathsf{MD5}(swk|r_C|pad_S|SQN_S)$
$SV \leftarrow$
$\mathsf{Enc}_{swk}(mac_S|r_C|pad_S)$
SV
$SQN_S \leftarrow SQN_S + 1$
$mac'_S \leftarrow$
$\mathsf{MD5}(swk|SID|pad'_S|SQN_S)$
$SF \leftarrow$
$\mathsf{Enc}_{swk}(mac'_S|SID|pad'_S)$
SF