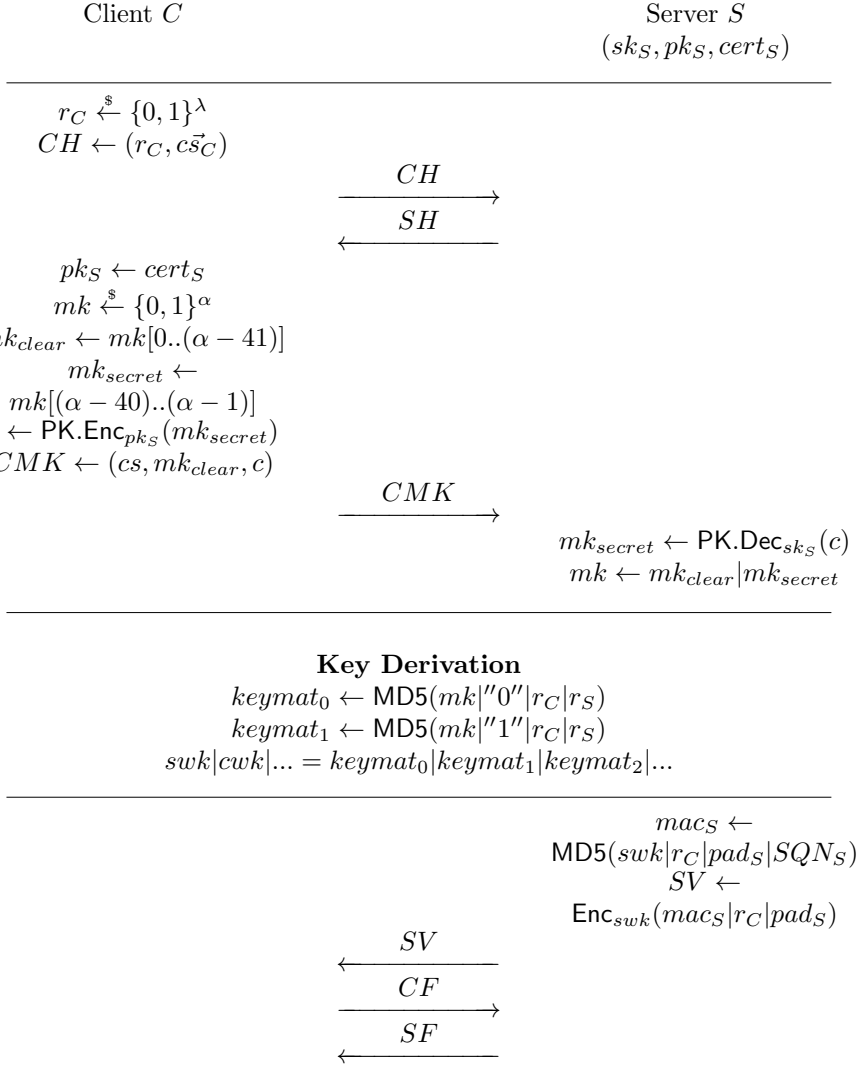
Client C
Server S
$(sk_S, pk_S, cert_S)$
$r_C \xleftarrow{\$} \{0,1\}^\lambda$
$CH \leftarrow (r_C, c\vec{s}_C)$
CH
SH
$pk_S \leftarrow cert_S$
$mk \xleftarrow{\$} \{0,1\}^\alpha$
$mk_{clear} \leftarrow mk[0..(\alpha - 41)]$
$mk_{secret} \leftarrow$
$mk[(\alpha - 40)..(\alpha - 1)]$
$c \leftarrow \mathsf{PK.Enc}_{pk_S}(mk_{secret})$
$CMK \leftarrow (cs, mk_{clear}, c)$
CMK
$mk_{secret} \leftarrow \mathsf{PK.Dec}_{sk_S}(c)$
$mk \leftarrow mk_{clear}|mk_{secret}$
Key Derivation
$keymat_0 \leftarrow \mathsf{MD5}(mk|''0''|r_C|r_S)$
$keymat_1 \leftarrow \mathsf{MD5}(mk|''1''|r_C|r_S)$
$swk|cwk|... = keymat_0|keymat_1|keymat_2|...$
$mac_S \leftarrow$
$\mathsf{MD5}(swk|r_C|pad_S|SQN_S)$
$SV \leftarrow$
$\mathsf{Enc}_{swk}(mac_S|r_C|pad_S)$
SV
CF
SF