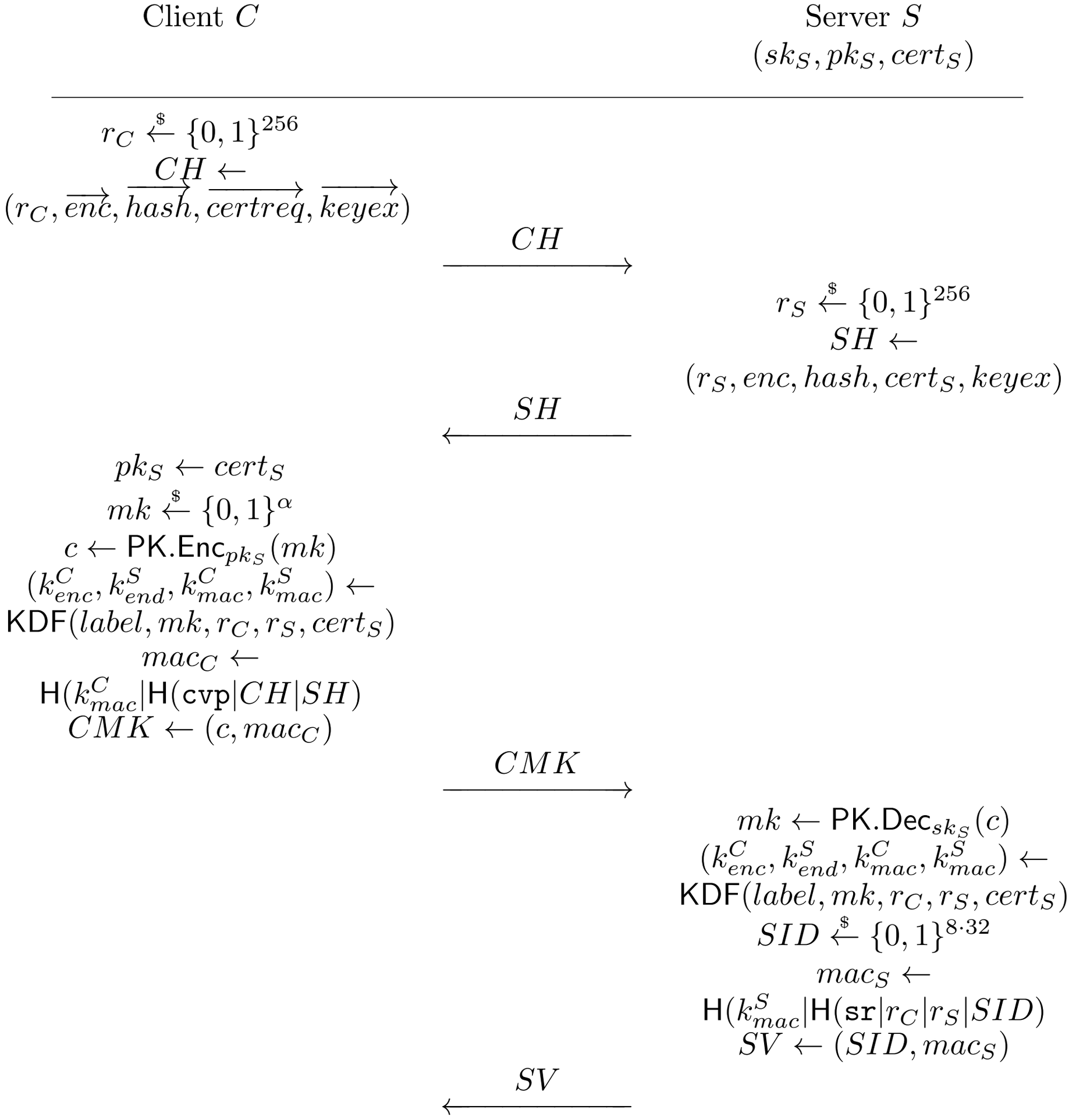
Client C
Server S
$(sk_S, pk_S, cert_S)$
$r_C \xleftarrow{\$} \{0,1\}^{256}$
$CH \leftarrow$
$(r_C, \overrightarrow{enc}, \overrightarrow{hash}, \overrightarrow{certreq}, \overrightarrow{keyex})$
CH
$r_S \xleftarrow{\$} \{0,1\}^{256}$
$SH \leftarrow$
$(r_S, enc, hash, cert_S, keyex)$
SH
$pk_S \leftarrow cert_S$
$mk \xleftarrow{\$} \{0,1\}^{\alpha}$
$c \leftarrow \mathsf{PK.Enc}_{pk_S}(mk)$
$(k^C_{enc}, k^S_{end}, k^C_{mac}, k^S_{mac}) \leftarrow$
$\mathsf{KDF}(label, mk, r_C, r_S, cert_S)$
$mac_C \leftarrow$
$\mathsf{H}(k^C_{mac}|\mathsf{H}(\mathtt{cvp}|CH|SH)$
$CMK \leftarrow (c, mac_C)$
CMK
$mk \leftarrow \mathsf{PK.Dec}_{sk_S}(c)$
$(k^C_{enc}, k^S_{end}, k^C_{mac}, k^S_{mac}) \leftarrow$
$\mathsf{KDF}(label, mk, r_C, r_S, cert_S)$
$SID \xleftarrow{\$} \{0,1\}^{8\cdot 32}$
$mac_S \leftarrow$
$\mathsf{H}(k^S_{mac}|\mathsf{H}(\mathtt{sr}|r_C|r_S|SID)$
$SV \leftarrow (SID, mac_S)$
SV