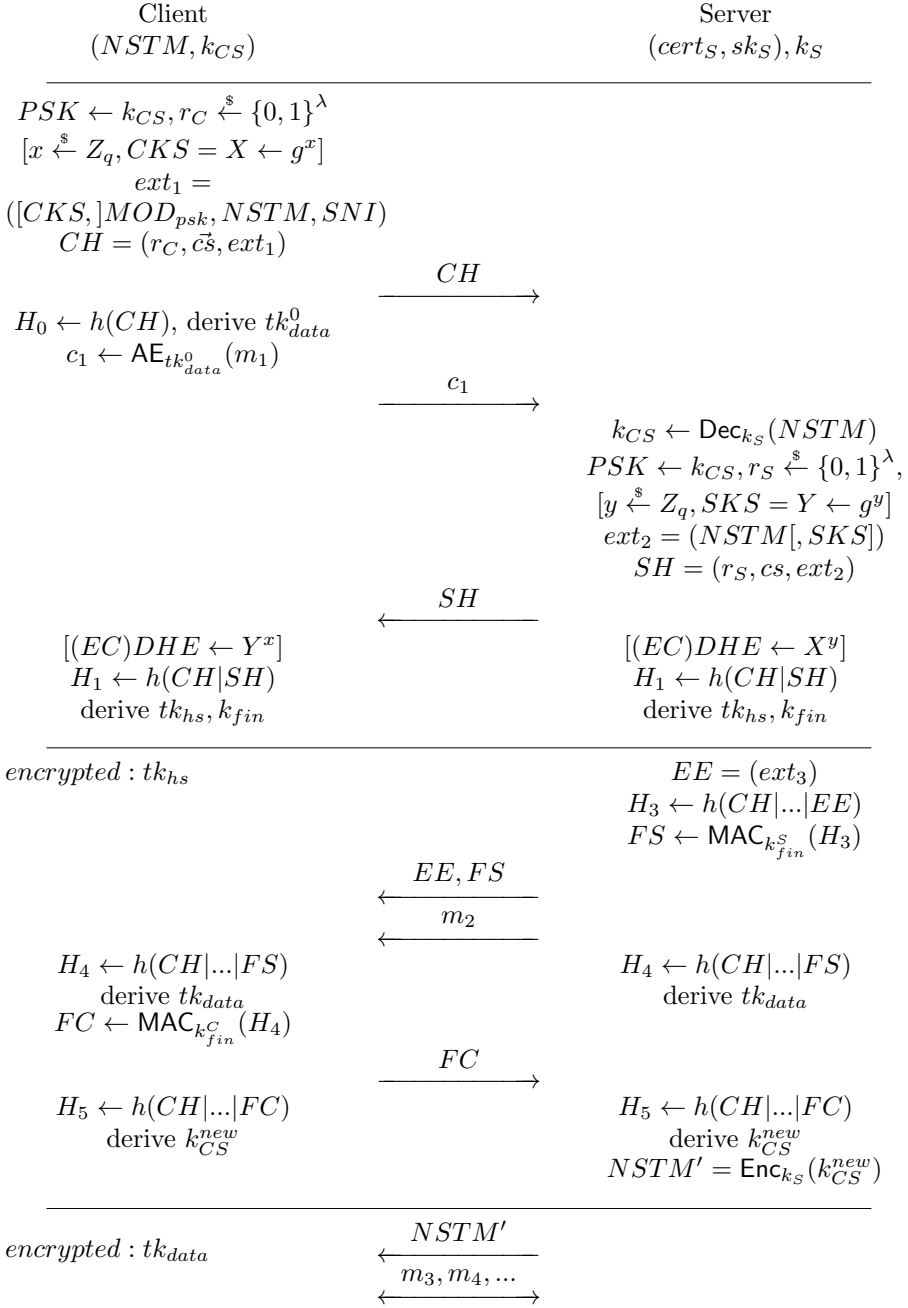
Client
$(NSTM, k_{CS})$
Server
$(cert_S, sk_S), k_S$
$PSK \leftarrow k_{CS}, r_C \xleftarrow{\$} \{0,1\}^\lambda$
$[x \xleftarrow{\$} Z_q, CKS = X \leftarrow g^x]$
$ext_1 =$
$([CKS,]MOD_{psk}, NSTM, SNI)$
$CH = (r_C, \vec{cs}, ext_1)$
CH
$H_0 \leftarrow h(CH)$, derive tk^0_{data}
$c_1 \leftarrow \mathsf{AE}_{tk^0_{data}}(m_1)$
c_1
$k_{CS} \leftarrow \mathsf{Dec}_{k_S}(NSTM)$
$PSK \leftarrow k_{CS}, r_S \xleftarrow{\$} \{0,1\}^\lambda,$
$[y \xleftarrow{\$} Z_q, SKS = Y \leftarrow g^y]$
$ext_2 = (NSTM[, SKS])$
$SH = (r_S, cs, ext_2)$
SH
$[(EC)DHE \leftarrow Y^x]$
$H_1 \leftarrow h(CH|SH)$
derive tk_{hs}, k_{fin}
$[(EC)DHE \leftarrow X^y]$
$H_1 \leftarrow h(CH|SH)$
derive tk_{hs}, k_{fin}
$encrypted : tk_{hs}$
$EE = (ext_3)$
$H_3 \leftarrow h(CH|...|EE)$
$FS \leftarrow \mathsf{MAC}_{k^S_{fin}}(H_3)$
EE, FS
m_2
$H_4 \leftarrow h(CH|...|FS)$
derive tk_{data}
$FC \leftarrow \mathsf{MAC}_{k^C_{fin}}(H_4)$
$H_4 \leftarrow h(CH|...|FS)$
derive tk_{data}
FC
$H_5 \leftarrow h(CH|...|FC)$
derive k^{new}_{CS}
$H_5 \leftarrow h(CH|...|FC)$
derive k^{new}_{CS}
$NSTM' = \mathsf{Enc}_{k_S}(k^{new}_{CS})$
$encrypted : tk_{data}$
$NSTM'$
$m_3, m_4, ...$