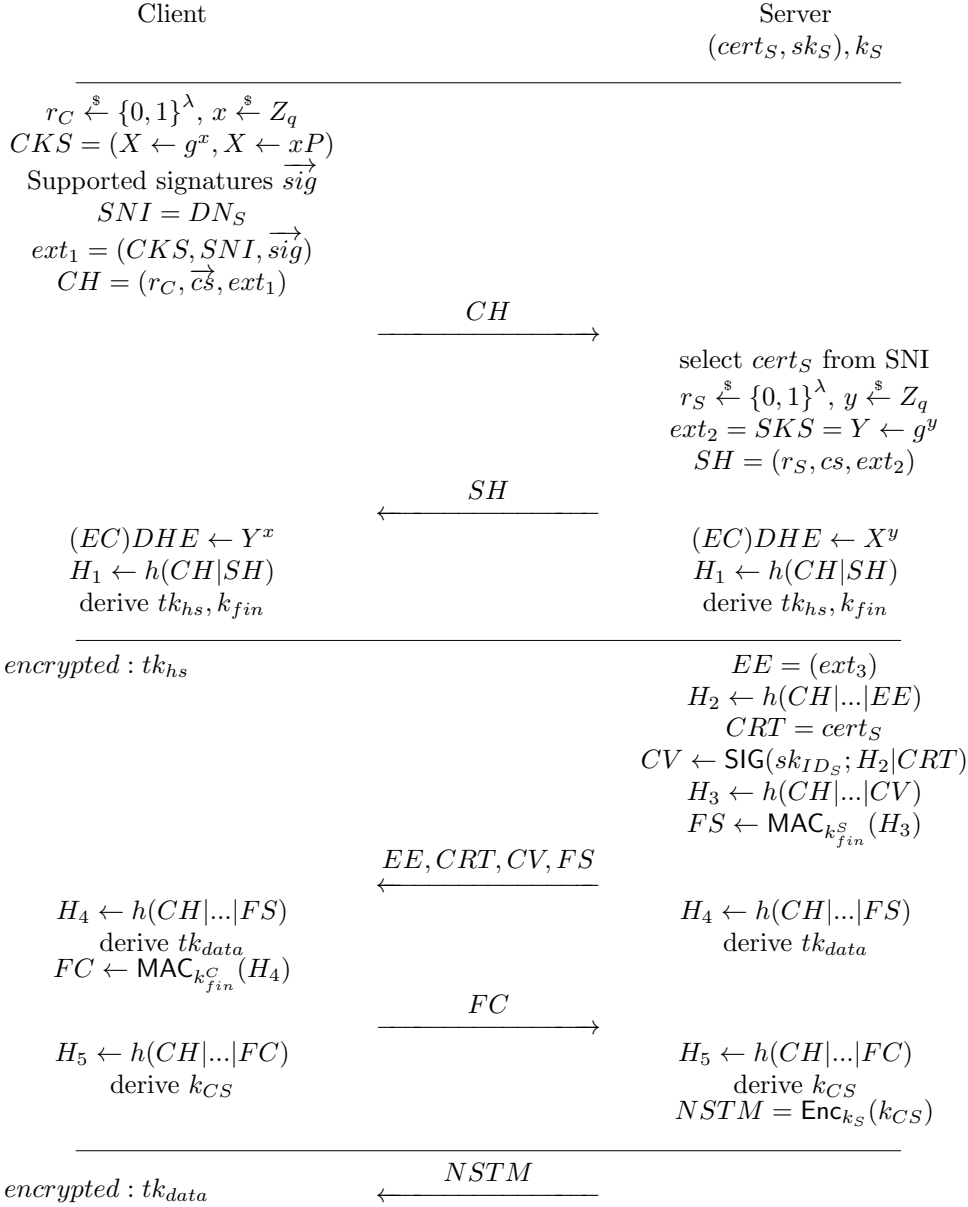
Client
Server
$(cert_S, sk_S), k_S$
$r_C \xleftarrow{\$} \{0,1\}^\lambda$, $x \xleftarrow{\$} Z_q$
$CKS = (X \leftarrow g^x, X \leftarrow xP)$
Supported signatures $\overrightarrow{sig}$
$SNI = DN_S$
$ext_1 = (CKS, SNI, \overrightarrow{sig})$
$CH = (r_C, \overrightarrow{cs}, ext_1)$
CH
select $cert_S$ from SNI
$r_S \xleftarrow{\$} \{0,1\}^\lambda$, $y \xleftarrow{\$} Z_q$
$ext_2 = SKS = Y \leftarrow g^y$
$SH = (r_S, cs, ext_2)$
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}
$encrypted : tk_{hs}$
$EE = (ext_3)$
$H_2 \leftarrow h(CH|...|EE)$
$CRT = cert_S$
$CV \leftarrow \mathsf{SIG}(sk_{ID_S}; H_2|CRT)$
$H_3 \leftarrow h(CH|...|CV)$
$FS \leftarrow \mathsf{MAC}_{k^S_{fin}}(H_3)$
EE, CRT, CV, FS
$H_4 \leftarrow h(CH|...|FS)$
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_{CS}
$H_5 \leftarrow h(CH|...|FC)$
derive k_{CS}
$NSTM = \mathsf{Enc}_{k_S}(k_{CS})$
$NSTM$
$encrypted : tk_{data}$