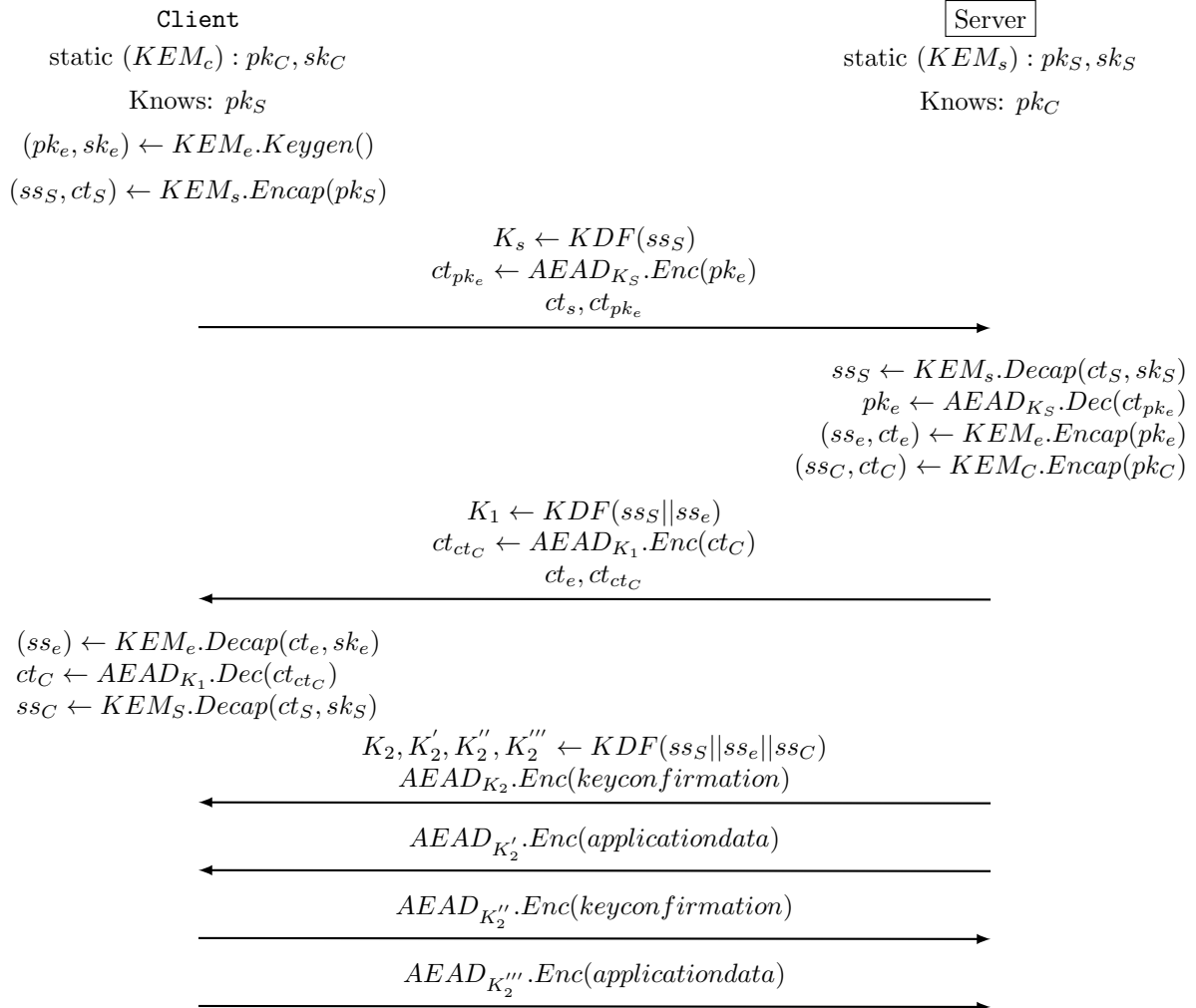
Client
Server
static $(KEM_c) : pk_C, sk_C$
static $(KEM_s) : pk_S, sk_S$
Knows: pk_S
Knows: pk_C
$(pk_e, sk_e) \leftarrow KEM_e.Keygen()$
$(ss_S, ct_S) \leftarrow KEM_s.Encap(pk_S)$
$K_s \leftarrow KDF(ss_S)$
$ct_{pk_e} \leftarrow AEAD_{K_S}.Enc(pk_e)$
ct_s, ct_{pk_e}
$ss_S \leftarrow KEM_s.Decap(ct_S, sk_S)$
$pk_e \leftarrow AEAD_{K_S}.Dec(ct_{pk_e})$
$(ss_e, ct_e) \leftarrow KEM_e.Encap(pk_e)$
$(ss_C, ct_C) \leftarrow KEM_C.Encap(pk_C)$
$K_1 \leftarrow KDF(ss_S||ss_e)$
$ct_{ct_C} \leftarrow AEAD_{K_1}.Enc(ct_C)$
ct_e, ct_{ct_C}
$(ss_e) \leftarrow KEM_e.Decap(ct_e, sk_e)$
$ct_C \leftarrow AEAD_{K_1}.Dec(ct_{ct_C})$
$ss_C \leftarrow KEM_S.Decap(ct_S, sk_S)$
$K_2, K_2^{'}, K_2^{''}, K_2^{'''} \leftarrow KDF(ss_S||ss_e||ss_C)$
$AEAD_{K_2}.Enc(keyconfirmation)$
$AEAD_{K_2^{'}}.Enc(applicationdata)$
$AEAD_{K_2^{''}}.Enc(keyconfirmation)$
$AEAD_{K_2^{'''}}.Enc(applicationdata)$