

static $(KEM_C) : pk_C, sk_C$

static $(KEM_S) : pk_S, sk_S$

Knows: pk_S

Knows: pk_C

$(pk_e, sk_e) \leftarrow KEM_e.Keygen()$

$(ss_S, ct_S) \leftarrow KEM_S.Encap(pk_S)$

$K_s \leftarrow KDF(ss_S)$
 $ct_S, AEAD_{K_s}.Enc(pk_e)$

$ss_S \leftarrow KEM_S.Decap(ct_S, sk_S)$

$pk_e \leftarrow AEAD_{K_s}.Dec(ct_{pk_e})$

$(ss_e, ct_e) \leftarrow KEM_e.Encap(pk_e)$

$(ss_C, ct_C) \leftarrow KEM_C.Encap(pk_C)$

$K_1 \leftarrow KDF(ss_S || ss_e)$
 $ct_C, AEAD_{K_1}.Enc(ct_e)$

$ss_C \leftarrow KEM_C.Decap(ct_C, sk_C)$

$ct_e \leftarrow AEAD_{K_1}.Dec(ct_{ct_e})$

$ss_C \leftarrow KEM_C.Decap(ct_C, sk_C)$

$K_2, K_2', K_2'', K_2''' \leftarrow KDF(ss_S || ss_e || ss_C)$
 $AEAD_{K_2}.Enc(\text{key confirmation})$

$AEAD_{K_2'}.Enc(\text{application data})$

$AEAD_{K_2''}.Enc(\text{key confirmation})$

$AEAD_{K_2'''}Enc(\text{application data})$

KEM.Ephemeral: Kyber

KEM.Client: Classic McEliece

KEM.Server: Classic McEliece