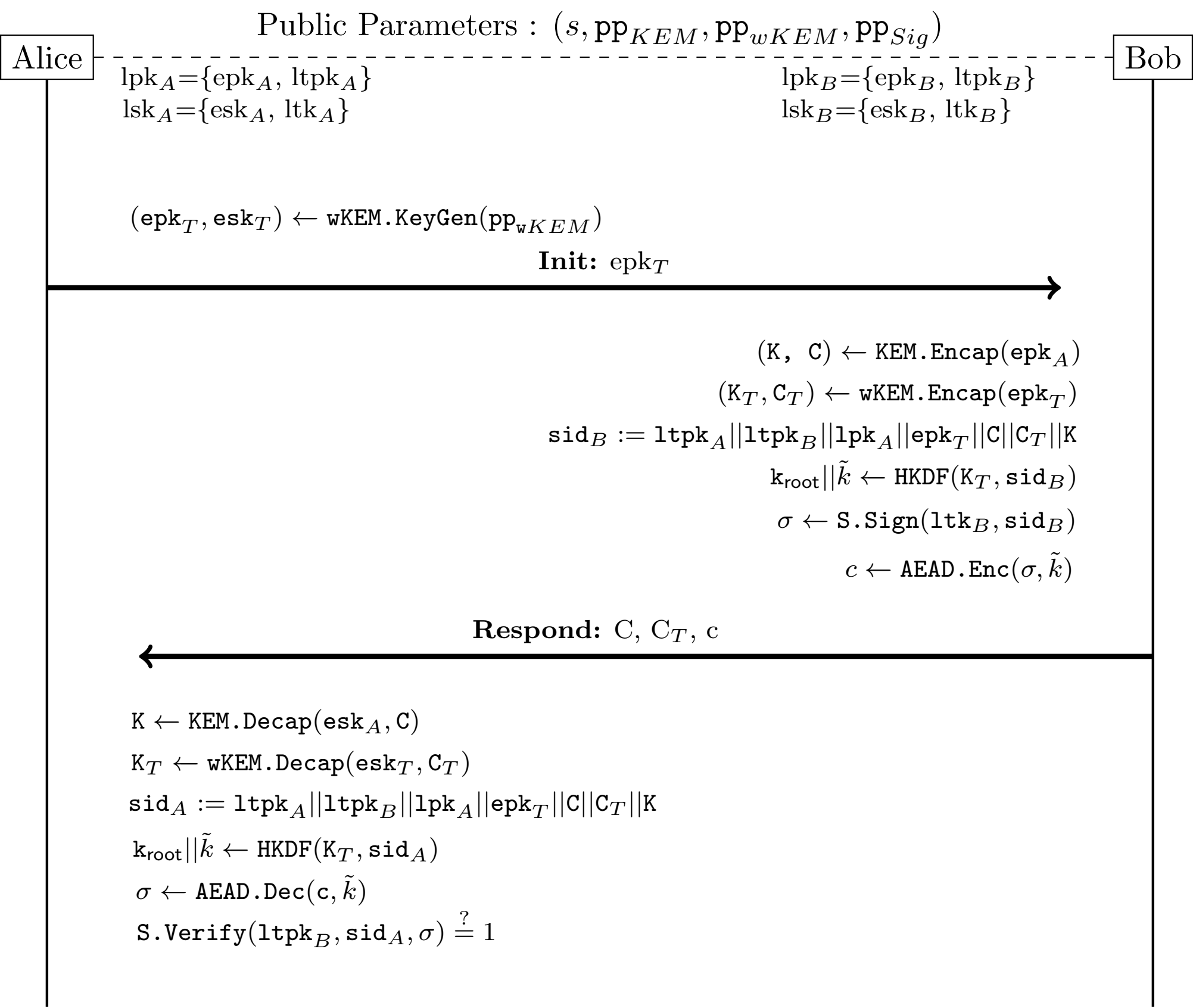
Public Parameters : $(s, \mathtt{pp}_{KEM}, \mathtt{pp}_{wKEM}, \mathtt{pp}_{Sig})$
Alice
Bob
lpk_A={epk_A, ltpk_A}
lsk_A={esk_A, ltk_A}
lpk_B={epk_B, ltpk_B}
lsk_B={esk_B, ltk_B}
$(\mathtt{epk}_T, \mathtt{esk}_T) \leftarrow \mathtt{wKEM.KeyGen}(\mathtt{pp}_{wKEM})$
Init: epk_T
$(\mathtt{K},\ \mathtt{C}) \leftarrow \mathtt{KEM.Encap}(\mathtt{epk}_A)$
$(\mathtt{K}_T, \mathtt{C}_T) \leftarrow \mathtt{wKEM.Encap}(\mathtt{epk}_T)$
$\mathtt{sid}_B := \mathtt{ltpk}_A||\mathtt{ltpk}_B||\mathtt{lpk}_A||\mathtt{epk}_T||\mathtt{C}||\mathtt{C}_T||\mathtt{K}$
$\mathtt{k}_{\mathsf{root}}||\tilde{k} \leftarrow \mathtt{HKDF}(\mathtt{K}_T, \mathtt{sid}_B)$
$\sigma \leftarrow \mathtt{S.Sign}(\mathtt{ltk}_B, \mathtt{sid}_B)$
$c \leftarrow \mathtt{AEAD.Enc}(\sigma, \tilde{k})$
Respond: C, C_T, c
$\mathtt{K} \leftarrow \mathtt{KEM.Decap}(\mathtt{esk}_A, \mathtt{C})$
$\mathtt{K}_T \leftarrow \mathtt{wKEM.Decap}(\mathtt{esk}_T, \mathtt{C}_T)$
$\mathtt{sid}_A := \mathtt{ltpk}_A||\mathtt{ltpk}_B||\mathtt{lpk}_A||\mathtt{epk}_T||\mathtt{C}||\mathtt{C}_T||\mathtt{K}$
$\mathtt{k}_{\mathsf{root}}||\tilde{k} \leftarrow \mathtt{HKDF}(\mathtt{K}_T, \mathtt{sid}_A)$
$\sigma \leftarrow \mathtt{AEAD.Dec}(\mathtt{c}, \tilde{k})$
$\mathtt{S.Verify}(\mathtt{ltpk}_B, \mathtt{sid}_A, \sigma) \stackrel{?}{=} 1$