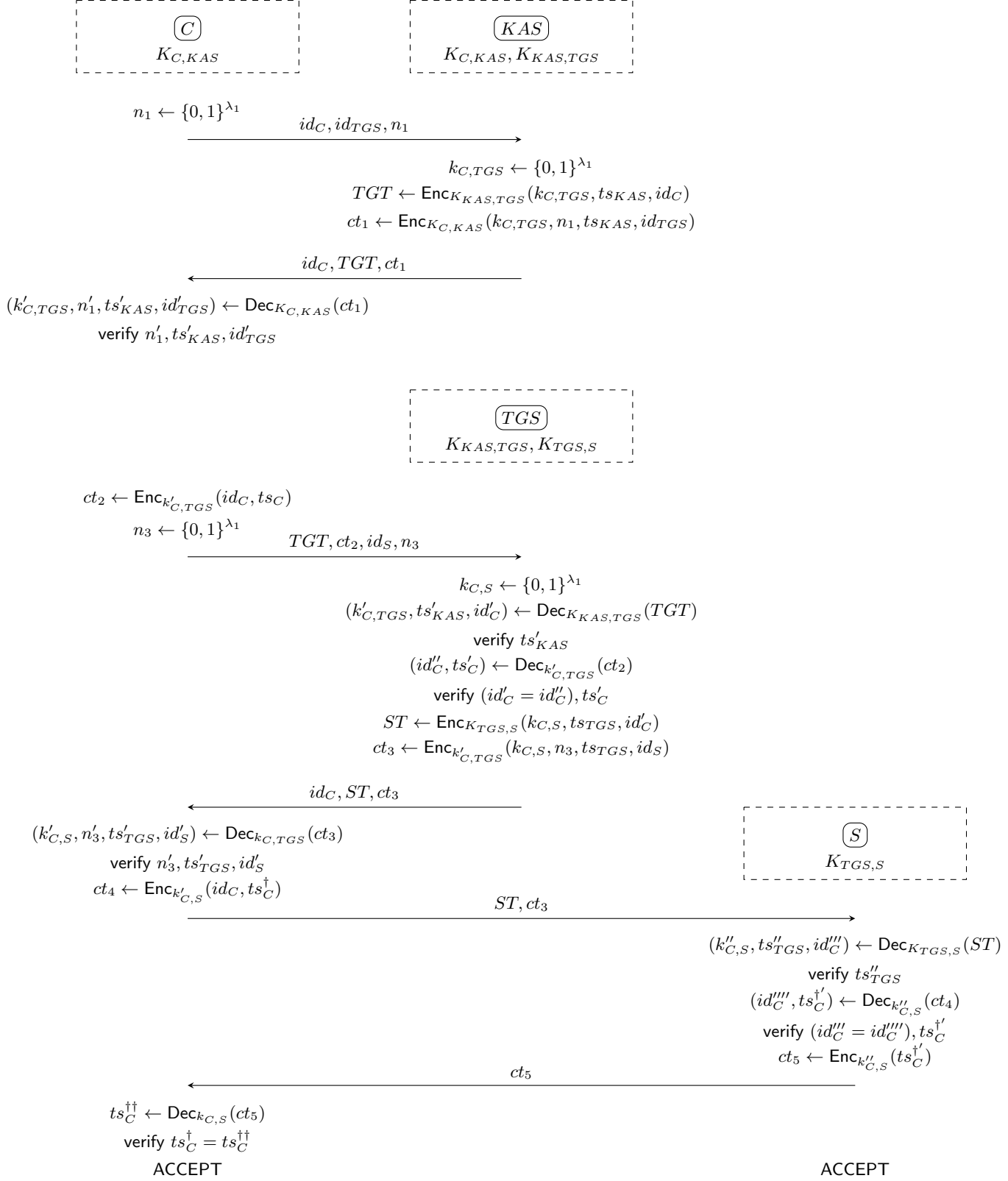
C
$K_{C,KAS}$
KAS
$K_{C,KAS}, K_{KAS,TGS}$
$n_1 \leftarrow \{0,1\}^{\lambda_1}$
id_C, id_{TGS}, n_1
$k_{C,TGS} \leftarrow \{0,1\}^{\lambda_1}$
$TGT \leftarrow \mathsf{Enc}_{K_{KAS,TGS}}(k_{C,TGS}, ts_{KAS}, id_C)$
$ct_1 \leftarrow \mathsf{Enc}_{K_{C,KAS}}(k_{C,TGS}, n_1, ts_{KAS}, id_{TGS})$
id_C, TGT, ct_1
$(k'_{C,TGS}, n'_1, ts'_{KAS}, id'_{TGS}) \leftarrow \mathsf{Dec}_{K_{C,KAS}}(ct_1)$
verify $n'_1, ts'_{KAS}, id'_{TGS}$
TGS
$K_{KAS,TGS}, K_{TGS,S}$
$ct_2 \leftarrow \mathsf{Enc}_{k'_{C,TGS}}(id_C, ts_C)$
$n_3 \leftarrow \{0,1\}^{\lambda_1}$
TGT, ct_2, id_S, n_3
$k_{C,S} \leftarrow \{0,1\}^{\lambda_1}$
$(k'_{C,TGS}, ts'_{KAS}, id'_C) \leftarrow \mathsf{Dec}_{K_{KAS,TGS}}(TGT)$
verify ts'_{KAS}
$(id''_C, ts'_C) \leftarrow \mathsf{Dec}_{k'_{C,TGS}}(ct_2)$
verify $(id'_C = id''_C), ts'_C$
$ST \leftarrow \mathsf{Enc}_{K_{TGS,S}}(k_{C,S}, ts_{TGS}, id'_C)$
$ct_3 \leftarrow \mathsf{Enc}_{k'_{C,TGS}}(k_{C,S}, n_3, ts_{TGS}, id_S)$
id_C, ST, ct_3
$(k'_{C,S}, n'_3, ts'_{TGS}, id'_S) \leftarrow \mathsf{Dec}_{k_{C,TGS}}(ct_3)$
verify n'_3, ts'_{TGS}, id'_S
$ct_4 \leftarrow \mathsf{Enc}_{k'_{C,S}}(id_C, ts^{\dagger}_C)$
S
$K_{TGS,S}$
ST, ct_3
$(k''_{C,S}, ts''_{TGS}, id'''_C) \leftarrow \mathsf{Dec}_{K_{TGS,S}}(ST)$
verify ts''_{TGS}
$(id''''_C, ts^{\dagger'}_C) \leftarrow \mathsf{Dec}_{k''_{C,S}}(ct_4)$
verify $(id'''_C = id''''_C), ts^{\dagger'}_C$
$ct_5 \leftarrow \mathsf{Enc}_{k''_{C,S}}(ts^{\dagger'}_C)$
ct_5
$ts^{\dagger\dagger}_C \leftarrow \mathsf{Dec}_{k_{C,S}}(ct_5)$
verify $ts^{\dagger}_C = ts^{\dagger\dagger}_C$
ACCEPT
ACCEPT