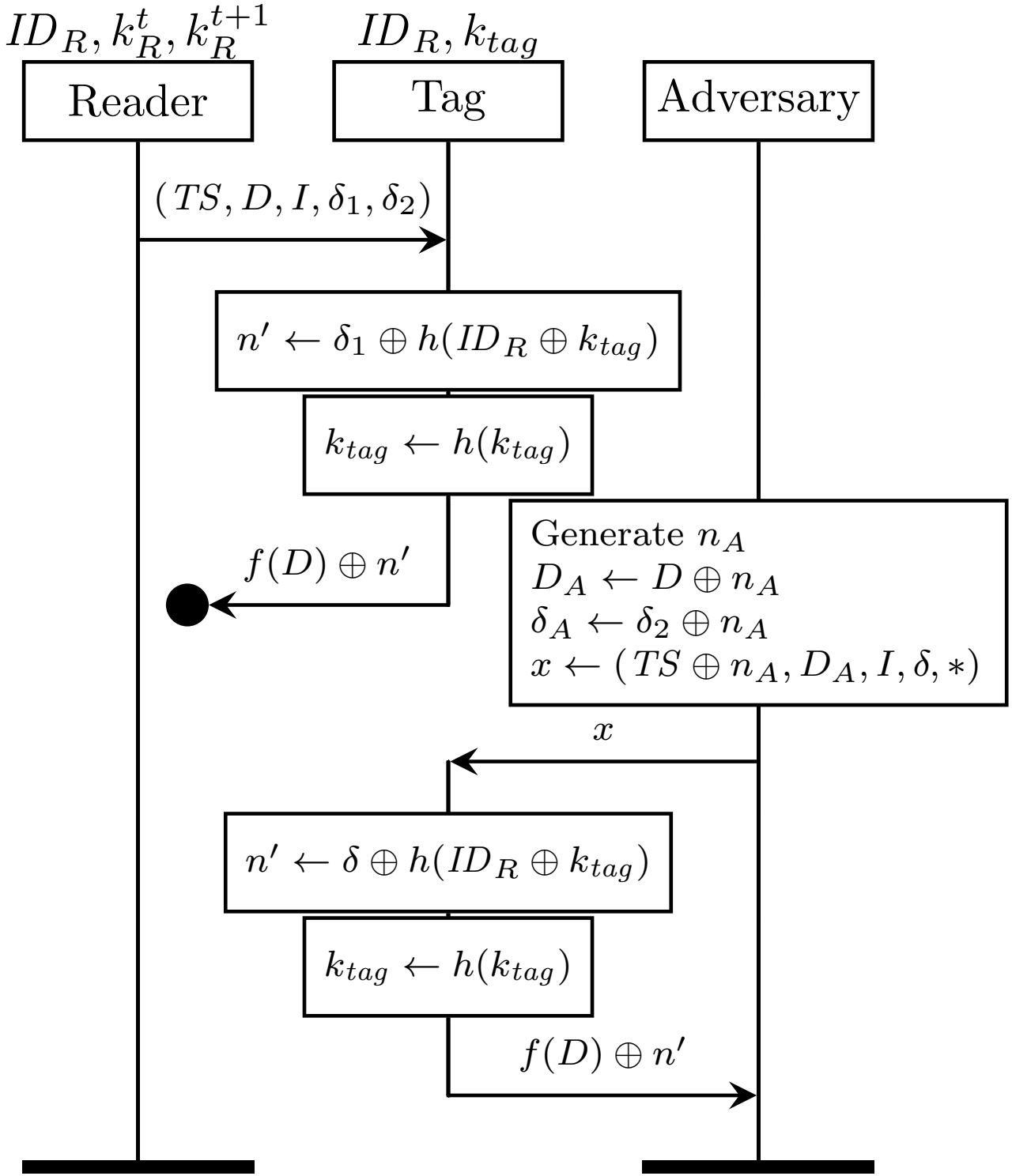
ID_R, k_R^t, k_R^{t+1}
ID_R, k_{tag}
Reader
Tag
Adversary
$(TS, D, I, \delta_1, \delta_2)$
$n' \leftarrow \delta_1 \oplus h(ID_R \oplus k_{tag})$
$k_{tag} \leftarrow h(k_{tag})$
$f(D) \oplus n'$
Generate n_A
$D_A \leftarrow D \oplus n_A$
$\delta_A \leftarrow \delta_2 \oplus n_A$
$x \leftarrow (TS \oplus n_A, D_A, I, \delta, *)$
x
$n' \leftarrow \delta \oplus h(ID_R \oplus k_{tag})$
$k_{tag} \leftarrow h(k_{tag})$
$f(D) \oplus n'$