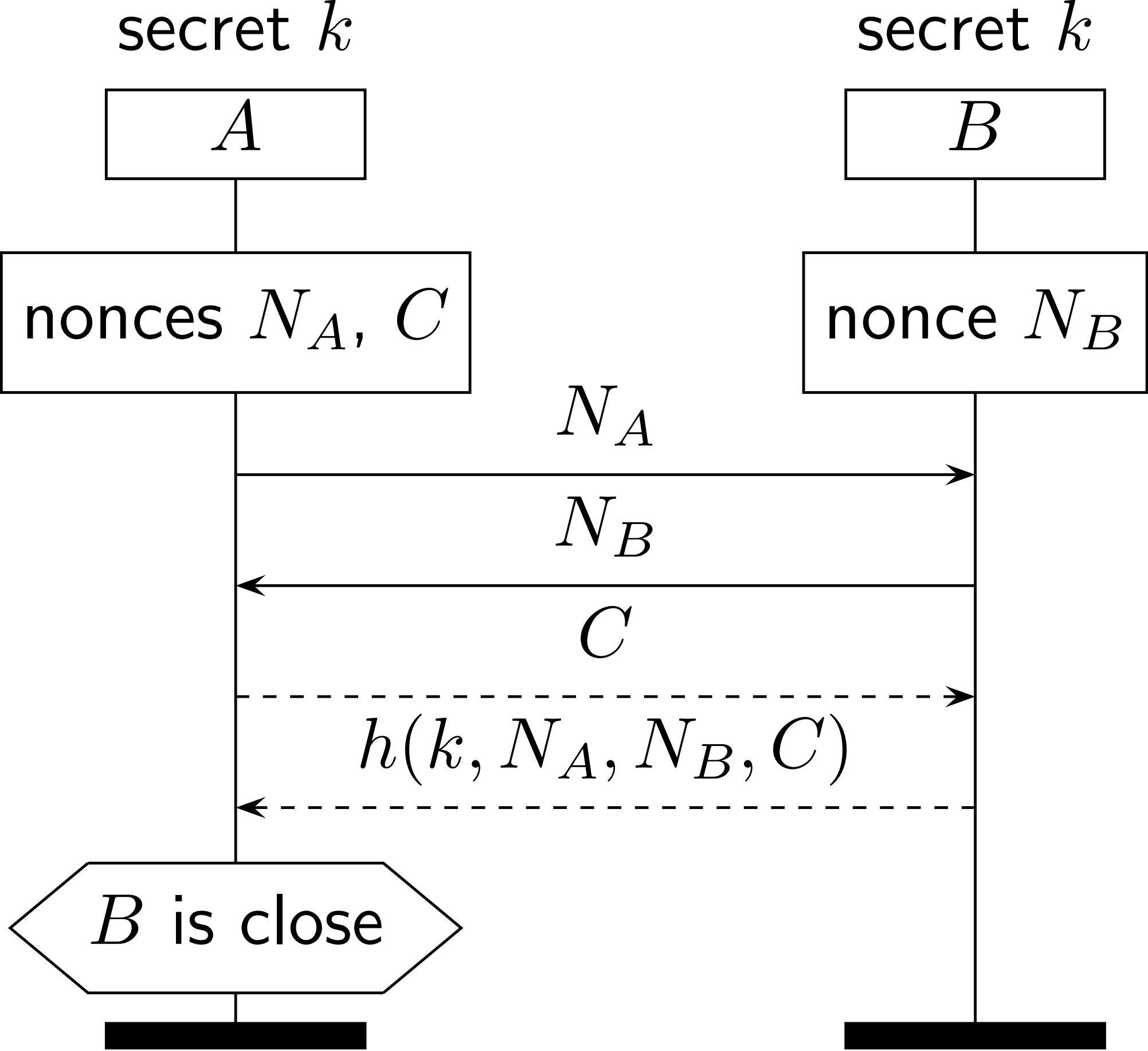
secret k
secret k
A
B
nonces N_A, C
nonce N_B
N_A
N_B
C
$h(k, N_A, N_B, C)$
B is close