{4}let sidBob_1: bitstring = session(Bob_3) [7] insert tbl_locks_handle(session(Bob_3),lock_sidBob_init) {9}new RootInit {10}new EphemeralInit
{12}insert tbl_states_handle(session(Alice_3),
stateChannelsidA) {11}let CK_1: bitstring = pars1(hkdf(RootInit, EphemeralInit)) [15] insert tbl_states_handle(session(Bob_3),stateChannelsidB) ~M = pars1(hkdf(RootInit,EphemeralInit)) Beginning of process NewSession Beginning of process NewSession Beginning of process MsgNewSession Beginning of process MsgNewSession Beginning of process NewSession Beginning of process CompromiseSession(session(Alice_3), session(Bob_3)) Beginning of process NewSession Beginning of process NewSession Beginning of process SessionCipherEncrypt Beginning of process MsgNewSession Beginning of process NewSession Beginning of process SessionCipherEncrypt Beginning of process MsgNewSession Beginning of process MsgNewSession Beginning of process SessionCipherDecrypt Beginning of process CompromiseSession(session(Alice_3), session(Bob_3)) Beginning of process MsgNewSession Beginning of process SessionCipherDecrypt Beginning of process CompromiseSession(session(Alice_3), session(Bob_3)) Beginning of process SessionCipherEncrypt $\sim M_1 + 1 = a_1 + 1$ $\sim M_2 + 1 = a_1 + 1$ ~M_3 = pars1(hkdf(RootInit,EphemeralInit)) [109] get tbl_locks_handle(session(Alice_3),lock_sidAlice_init) [108] get tbl_locks_handle(session(Bob_3),lock_sidBob_init) [107] get tbl_states_handle(session(Alice_3),stateChannelsidA) {106} get tbl_states_handle(session(Bob_3),stateChannelsidB) $\{94\}$ let MKa_1: bitstring = hash2(a_16,s1) {103}event eCompromise(session(Alice_3),session(Bob_3)) $\sim M_7 + 1 = a_15 + 1$ $\sim M_8 + 1 = a_14 + 1$ $\sim M_9 = hash2(a_16,s1)$ $\{95\}$ let MKb_1: bitstring = hash2(a_17,s1) $\sim M_10 = hash2(a_17,s1)$ {98}event eCompromise(session(Alice_3),session(Bob_3)): blocks $\sim M_11 = a_17$ [279] get tbl_locks_handle(session(Alice_3),lock_sidAlice_init) [278] get tbl_locks_handle(session(Bob_3),lock_sidBob_init)

A trace has been found.

Honest Process

{1}new Alice_3

{2}new Bob_3

{3}let sidAlice_1: bitstring = session(Alice_3)

{5} insert tbl_locks_handle(session(Alice_3),lock_sidAlice_init)

Attacker