A trace has been found. Attacker **Honest Process** {1}new sskCA_2 {2}new dummyIDPTx_2 {3}new dummySskPTx_2 {4}new BDID_A1_2 {5}new BDID B1 2 \sim M = spk(sskCA_2) \sim M_1 = spk(sskPTx) \sim M_2 = spk(dummySskPTx_2) \sim M_3 = DigitalPing a \sim M 4 = SIG $ID(\sim M_5, \sim M_6, \sim M_7, \sim M_8) = ID(MajorVer, MinorVer,$ MC,BDID A1 2) \sim M 9 = CFG a 1 \sim M 10 = FOD a 2 \sim M_11 = SRQ a 3 \sim M 12 = SRQen a 4 \sim M 13 = CE \sim M 14 = RP a 5 \sim M 15 = SIG $(\sim M_16, \sim M_17, \sim M_18, \sim M_19) = ID(MajorVer, MinorVer,$ MC,BDID_A1_2) \sim M 20 = CFG Phase 1 \sim M_21 = DigitalPing

The attacker tests whether

~M_8 = BDID_A1_2

is equal to

~M_26 = choice[BDID_A1_2,BDID_B1_2].

The result in the left-hand side is different from the result in the right-hand side.

a 6

 \sim M 22 = SIG

)(~M_23,~M_24,~M_25,~M_26) = ID(MajorVer,MinorVer, MC,choice[BDID A1 2,BDID B1 2])

 \sim M 27 = CFG