A trace has been found.

Honest Process   Attacker

{1} new sskCA_2
{2} new dummyIDPTx_2
{3} new dummySskPTx_2
{4} new BDID_A1_2
{5} new BDID_B1_2

~M = spk(sskCA_2)

~M_1 = spk(sskPTx)

~M_2 = spk(dummySskPTx_2)

~M_3 = DigitalPing

a

~M_4 = SIG

ID(~M_5,~M_6,~M_7,~M_8) = ID(MajorVer,MinorVer,
MC,BDID_A1_2)

~M_9 = CFG

Phase 1

~M_10 = DigitalPing

a_1

~M_11 = SIG

)(~M_12,~M_13,~M_14,~M_15) = ID(MajorVer,MinorVer,
MC,choice[BDID_A1_2,BDID_B1_2])

~M_16 = CFG

~M_17 = CE

~M_18 = RP8
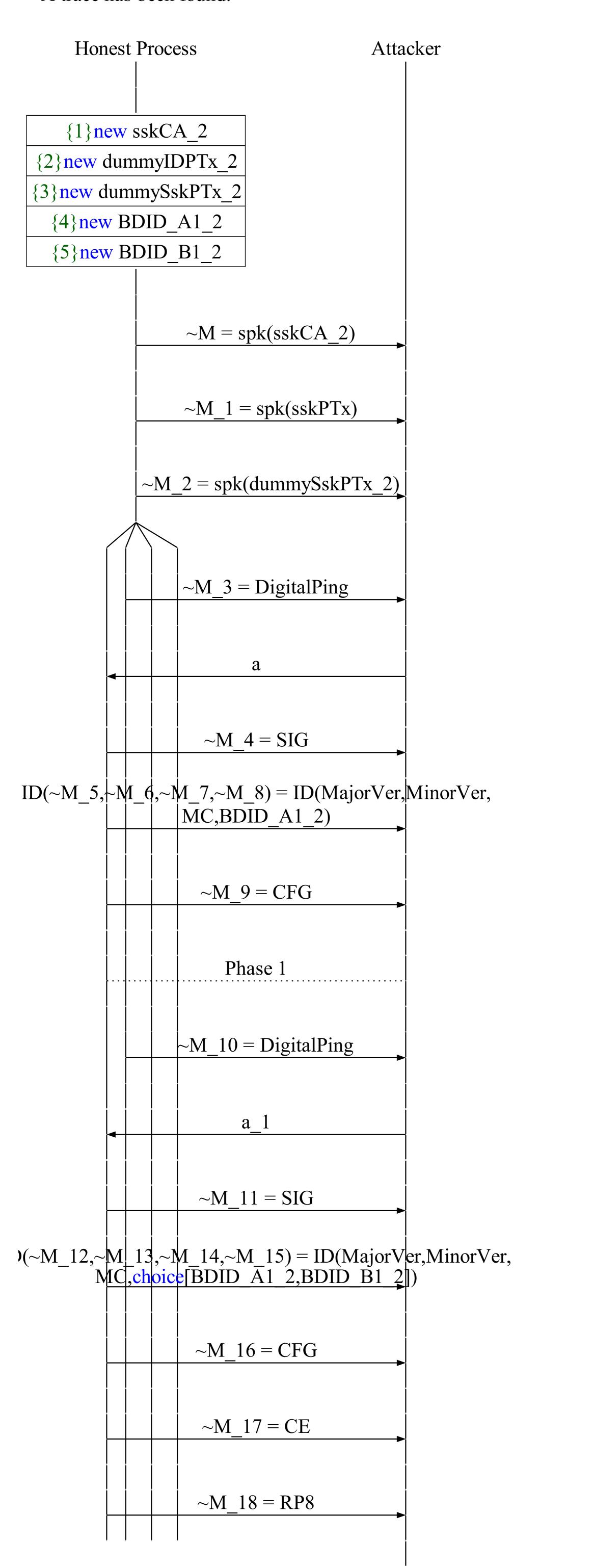
The attacker tests whether
~M_8 = BDID_A1_2
is equal to
~M_15 = choice[BDID_A1_2,BDID_B1_2].
The result in the left-hand side is different from
the result in the right-hand side.