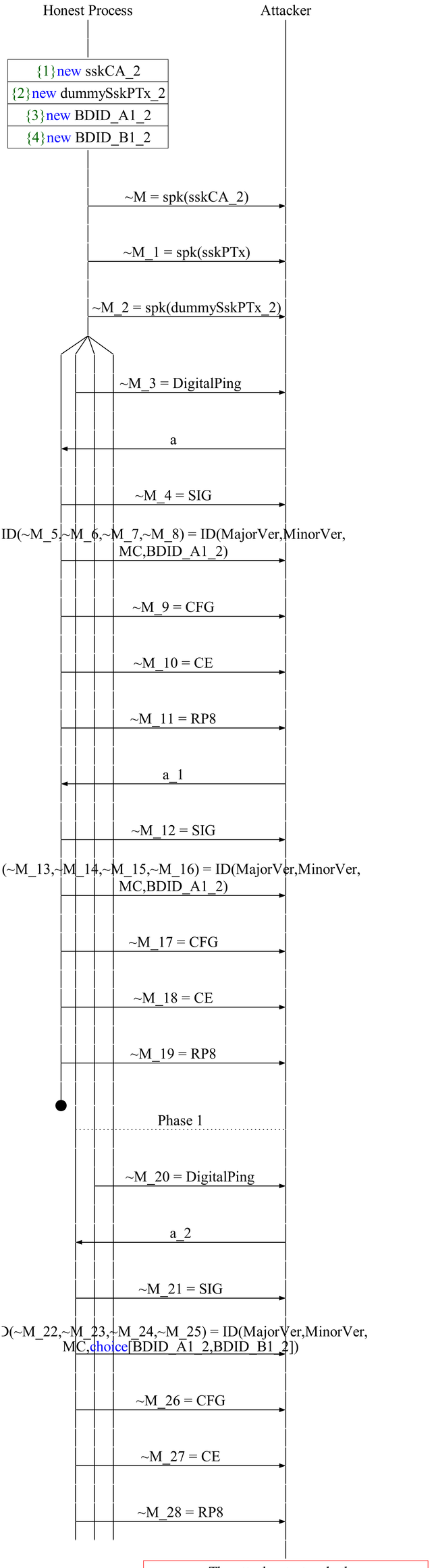
A trace has been found.



The attacker tests whether
~M_8 = BDID_A1_2
is equal to
~M_25 = choice[BDID_A1_2,BDID_B1_2].
The result in the left-hand side is different from the result in the right-hand side.