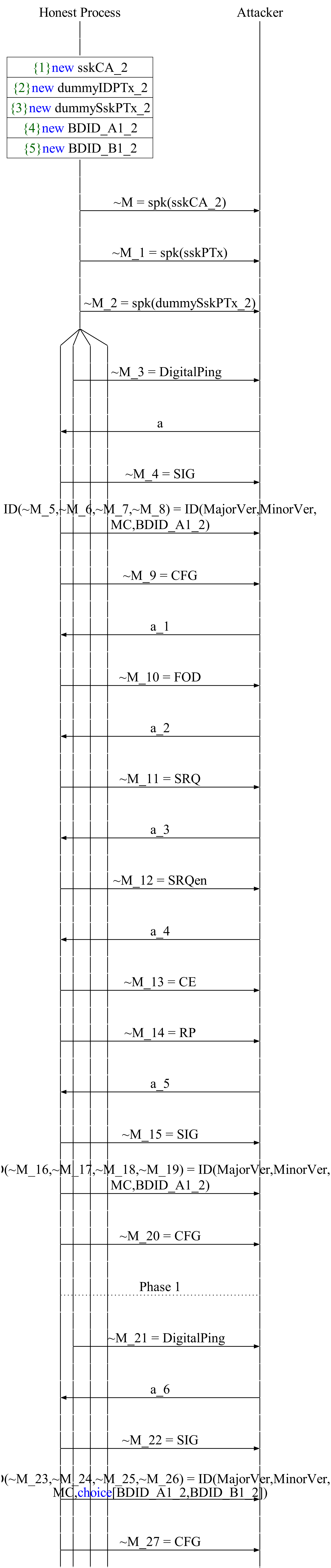


A trace has been found



The attacker tests whether $\sim M_8 = \text{BDID_A1_2}$ is equal to $\sim M_26 = \text{choice}[\text{BDID_A1_2}, \text{BDID_B1_2}]$. The result in the left-hand side is different from the result in the right-hand side.