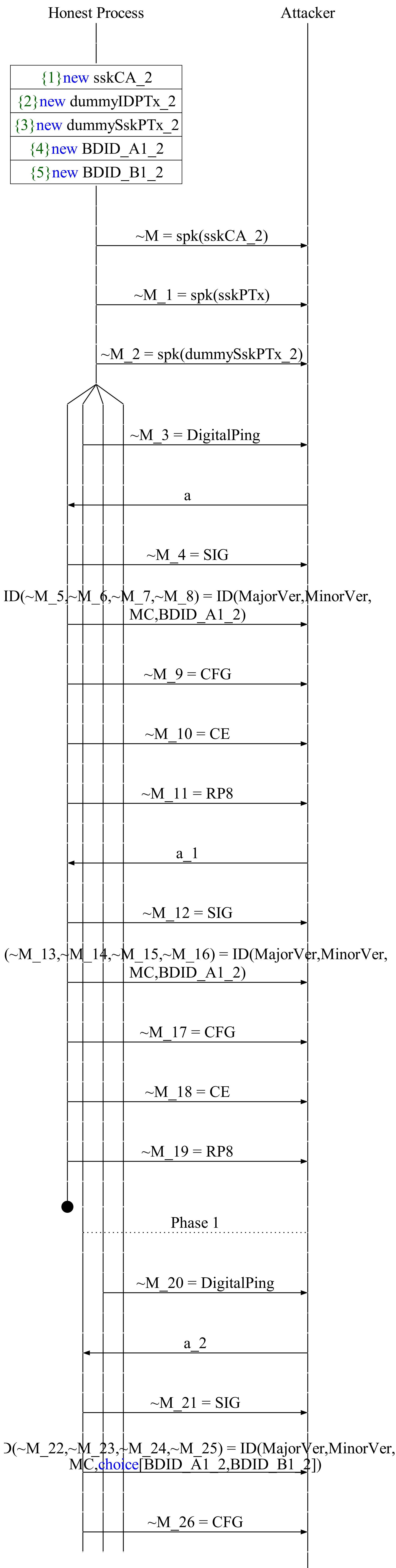


A trace has been found.



The attacker tests whether  
 $\sim M\_8 = \text{BDID\_A1\_2}$   
 is equal to  
 $\sim M\_25 = \text{choice}[\text{BDID\_A1\_2}, \text{BDID\_B1\_2}]$ .  
 The result in the left-hand side is different from  
 the result in the right-hand side.