
~M\_7 = AES\_CCM(keys,AES\_CMAC(AES\_CMAC(AES\_CMAC( ZERO,concat(concat(AES\_CMAC(ZERO,concat(concat( A trace has been found.

PS),p256(gen,exp\_P\_1)),gen)),rand\_prov\_2),rand\_prov\_2)), p256(gen,exp\_P\_1)),prsn))



The attacker tests whether concat(AES CMAC(ZERO,concat(concat(concat(concat(