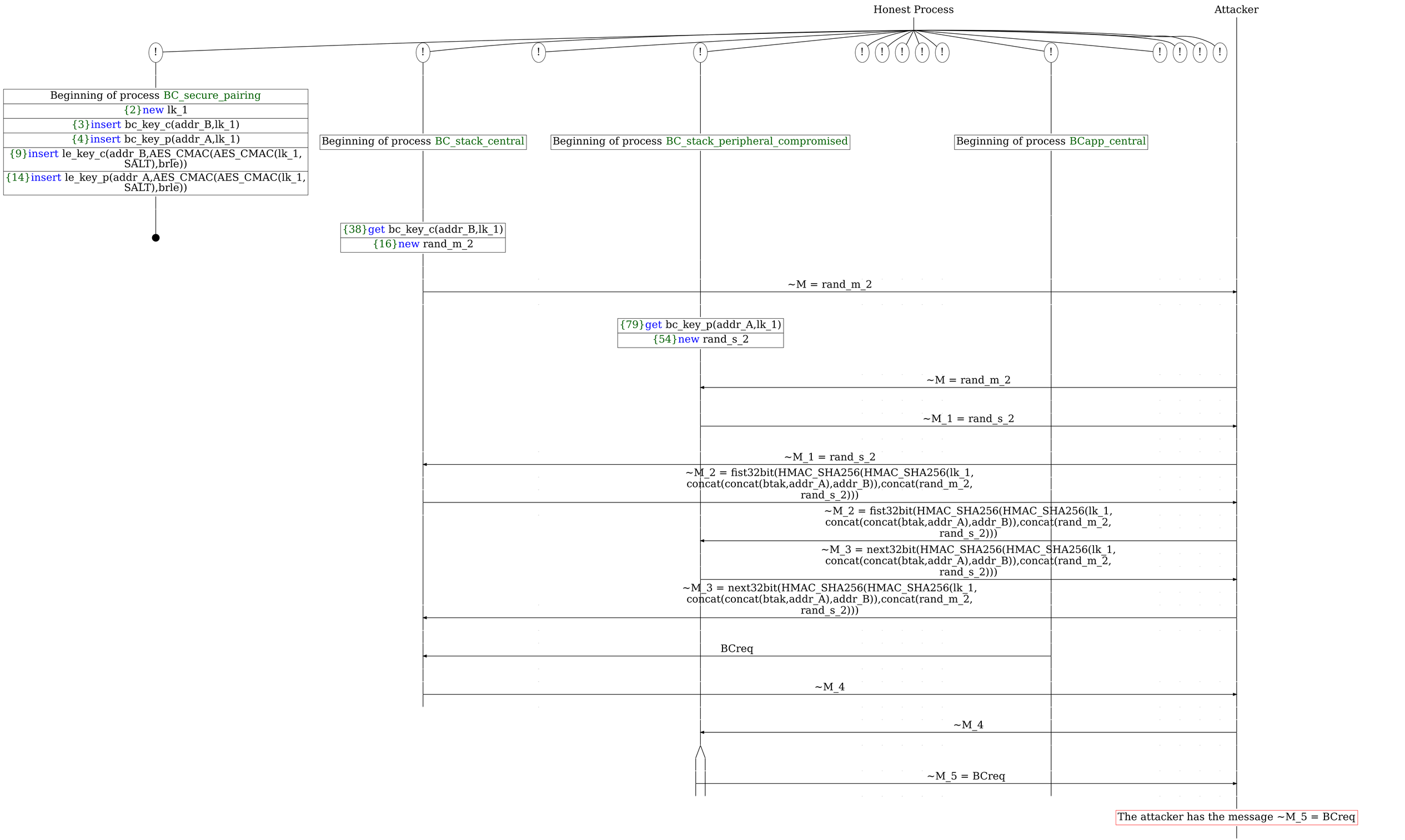
Abbreviations
~M_4 = AES_CCM(BCreq,HMAC_SHA256(lk_1,concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(lk_1,concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))))),last64bit(HMAC_SHA256(HMAC_SHA256(lk_1,concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))))

A trace has been found.



The attacker has the message ~M_5 = BCreq