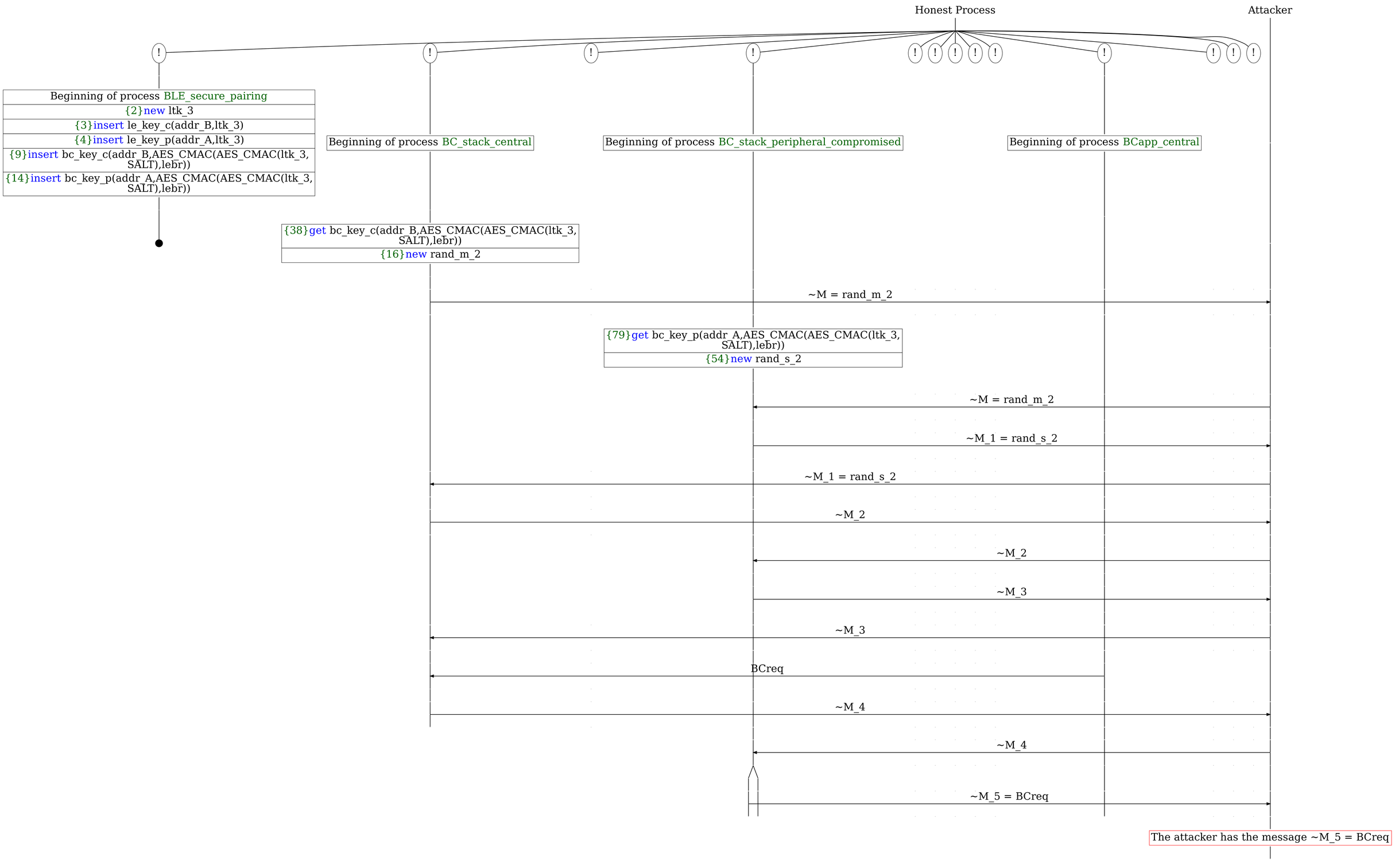
| Abbreviations |
| --- |
| ~M_2 = fist32bit(HMAC_SHA256(HMAC_SHA256(AES_CMAC(AES_CMAC(ltk_3,SALT),lebr),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))) |
| ~M_3 = next32bit(HMAC_SHA256(HMAC_SHA256(AES_CMAC(AES_CMAC(ltk_3,SALT),lebr),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))) |
| ~M_4 = AES_CCM(BCreq,HMAC_SHA256(AES_CMAC(AES_CMAC(ltk_3,SALT),lebr),concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(AES_CMAC(AES_CMAC(ltk_3,SALT),lebr),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2))))),last64bit(HMAC_SHA256(HMAC_SHA256(AES_CMAC(AES_CMAC(ltk_3,SALT),lebr),concat(concat(btak,addr_A),addr_B)),concat(rand_m_2,rand_s_2)))) |

A trace has been found.