Abbreviations
~X_1 = HMAC_SHA256(~M_3,concat(concat(concat(concat(a,~M_5),zero),iocap_A),addr_A),addr_B)) = HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),zero),iocap_A),addr_A),addr_B))
~X_2 = fist32bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(~M_3,concat(concat(concat(concat(a,~M_5),btlk), addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)), concat(a_1,~M_7))) = fist32bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(a_1,rand_s_2)))
~M_8 = next32bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),btlk),addr_A),addr_B)),concat(concat(btak, addr_A),addr_B)),concat(a_1,rand_s_2)))
~X_3 = AES_CCM(a_2,HMAC_SHA256(HMAC_SHA256(~M_3,concat(concat(concat(concat(a,~M_5),btlk),addr_A),addr_B)), concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(~M_3,concat(concat(concat(concat(a,~M_5),btlk),addr_A),addr_B)), concat(concat(btak,addr_A),addr_B)),concat(a_1, ~M_7)))),last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(~M_3,concat(concat(concat(a,~M_5),btlk), addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)), concat(a_1,~M_7)))) = AES_CCM(a_2,HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),btlk),addr_A),addr_B)),concat(concat(concat(btak,addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),btlk),addr_A),addr_B)), concat(concat(btak,addr_A),addr_B)),concat(a_1, rand_s_2)))),last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(a_1,rand_s_2))))
~M_9 = AES_CCM(BCrsp,HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6), btlk),addr_A),addr_B)),concat(concat(concat(btak, addr_A),addr_B),last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),btlk),addr_A),addr_B)),concat(concat(btak,addr_A),addr_B)),concat(a_1,rand_s_2)))), last64bit(HMAC_SHA256(HMAC_SHA256(HMAC_SHA256(p256(gen,exp_P_1),concat(concat(concat(concat(a,nb_6),btlk),addr_A),addr_B)),concat(concat(btak, addr_A),addr_B)),concat(a_1,rand_s_2))))

A trace has been found.