Abbreviations
~X_1 = HMAC_SHA256(~M,concat(concat(concat(concat(concat(a,~M_1),zero),iocap_B),addr_B),addr_A)) = HMAC_SHA256(p224(gen,pri_C_1),concat(concat(concat(concat(concat(a,na_2),zero),iocap_B),addr_B),addr_A))
~X_2 = HMAC_SHA256(~M_5,concat(concat(concat(concat(concat(a_3,~M_7),zero),iocap_A),addr_A),addr_B)) = HMAC_SHA256(p224(gen,pri_P_1),concat(concat(concat(concat(concat(a_3,nb_2),zero),iocap_A),addr_A),addr_B))
~M_11 = AES_CCM(SHA256(concat(s1_2,r1_6)),AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_P_1), concat(concat(concat(concat(a_3,nb_2),btlk),addr_A), addr_B)),SALT),brle),concat(skds_2,a_4)),concat(ivs_2,a_5))
~X_3 = AES_CCM(sdec(~M_11,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M_5,concat(concat(concat(concat(a_3, ~M_7),btlk),addr_A),addr_B)),SALT),brle),concat(~M_9,a_4)),concat(~M_10,a_5)),AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M,concat(concat(concat(concat(~M_1,a),btlk),addr_A),addr_B)),SALT),brle),concat(a_1,~M_3)),concat(a_2,~M_4)) = AES_CCM(SHA256(~ concat(s1_2,r1_6)),AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_C_1),concat(concat(concat(concat(na_2,a),btlk),addr_A),addr_B)),SALT),brle), concat(a_1,skdm_2)),concat(a_2,ivm_2))
~M_12 = AES_CCM(p224(gen,s2_1),AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_C_1),concat(concat(concat(concat(na_2,a),btlk),addr_A),addr_B)), SALT),brle),concat(a_1,skdm_2)),concat(a_2,ivm_2))
~M_13 = AES_CCM(r2_7,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_C_1),concat(concat(concat(concat(na_2,a),btlk),addr_A),addr_B)),SALT),brle),concat(a_1,skdm_2)),concat(a_2,ivm_2))
~X_4 = (AES_CCM(sdec(~M_12,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M,concat(concat(concat(concat(~M_1, a),btlk),addr_A),addr_B)),SALT),brle),concat(a_1, ~M_3)),concat(a_2,~M_4)),AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M_5,concat(concat(concat(concat(a_3, ~M_7),btlk),addr_A),addr_B)),SALT),brle),concat(~M_9,a_4)),concat(~M_10,a_5)),AES_CCM(sdec(~M_13, AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M,concat(concat(concat(concat(~M_1,a),btlk),addr_A),addr_B)), SALT),brle),concat(a_1,~M_3)),concat(a_2,~M_4)), AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M_5,concat(concat(concat(concat(a_3,~M_7),btlk),addr_A),addr_B)), SALT),brle),concat(~M_9,a_4)),concat(~M_10,a_5))) = (AES_CCM(p224(gen,s2_1),AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_P_1),concat(concat(concat(concat(a_3,nb_2),btlk),addr_A),addr_B)),SALT), brle),concat(skds_2,a_4)),concat(ivs_2,a_5)),AES_CCM(r2_7,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_P_1),concat(concat(concat(concat(a_3,nb_2), btlk),addr_A),addr_B)),SALT),brle),concat(skds_2, a_4)),concat(ivs_2,a_5)))
~M_14 = AES_CCM(s1_2,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_P_1),concat(concat(concat(concat(a_3,nb_2),btlk),addr_A),addr_B)),SALT),brle),concat(skds_2,a_4)),concat(ivs_2,a_5))
~M_15 = AES_CCM(r1_6,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_P_1),concat(concat(concat(concat(a_3,nb_2),btlk),addr_A),addr_B)),SALT),brle),concat(skds_2,a_4)),concat(ivs_2,a_5))
~X_5 = (AES_CCM(sdec(~M_14,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M_5,concat(concat(concat(concat(a_3, ~M_7),btlk),addr_A),addr_B)),SALT),brle),concat(~M_9,a_4)),concat(~M_10,a_5)),AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M,concat(concat(concat(concat(~M_1,a),btlk),addr_A),addr_B)),SALT),brle),concat(a_1,~M_3)),concat(a_2,~M_4)),AES_CCM(sdec(~M_15, AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M_5,concat(concat(concat(concat(a_3,~M_7),btlk),addr_A),addr_B)), SALT),brle),concat(~M_9,a_4)),concat(~M_10,a_5)), AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M,concat(concat(concat(concat(~M_1,a),btlk),addr_A),addr_B)), SALT),brle),concat(a_1,~M_3)),concat(a_2,~M_4))) = (AES_CCM(s1_2,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_C_1),concat(concat(concat(concat(na_2,a),btlk),addr_A),addr_B)),SALT),brle),concat(a_1,skdm_2)),concat(a_2,ivm_2)),AES_CCM(r1_6,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(p224(gen,pri_C_1), concat(concat(concat(concat(na_2,a),btlk),addr_A), addr_B)),SALT),brle),concat(a_1,skdm_2)),concat(a_2,ivm_2)))

A trace has been found.