Abbreviations ~X_1 = HMAC_SHA256(~M,concat(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(concat(a,na_2),zero),iocap_B),addr_B),addr_A)) \sim X_2 = HMAC_SHA256(\sim M_5,concat(concat(concat(concat(concat(a_3, \sim 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)) \sim 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(\sim X_3 = AES_CCM(sdec(\sim M_11,AES_CMAC(AES_CMAC \sim M_7),btlk),addr_A),addr_B)),SALT),brle),concat(~M_9,a_4)),concat(~M_10,a_5)),AES_CMAC($a_1, \sim M_3)$, concat($a_2, \sim M_4$)) = 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), $concat(a_1,skdm_2)$, $concat(a_2,ivm_2)$ \sim M_12 = AES_CCM(p224(gen,s2_1),AES_CMAC(AES_CMAC(ĀES_CMAC(HMAC_SHA256(p224(gen,pri_C_1),concat(concat(concat(concat(na 2,a),btlk),addr A),addr B)), SALT), brle), $concat(a_1,s\overline{k}dm_2)$), $concat(a_2,ivm_2)$) \sim M_13 = AES_CCM(r2_7,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(-p224(gen,pri_ \overline{C}_1),concat(concat(concat(concat)) na_2,a),btlk),addr_A),addr_B)),SALT),brle),concat(a_1 ,skdm $^-$ 2)),con $cat(a_2$,ivm $^-$ 2)) $\sim X_4 = (AES_CCM(sdec(\sim M_12,AES_CMAC(AES_CMAC$ HMAC_SHA256(~M,concat(concat(concat(concat(concat(~M_1, a),btlk),addr_A),addr_B)),SALT),brle),concat(a_1, \sim M_3)),concat(a_2, \sim M_4)),AES_CMAC(HMAC SHA256(~M 5,concat(concat(concat(concat(a 3, \sim M_7),btlk),addr_A),addr_B)),SALT),brle),concat(\sim M_9,a_4)),concat(\sim M_10,a_5)),AES_CCM(sdec(\sim M_13, AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256)~M,concat($-concat(concat(concat(\sim M 1,a),btlk),addr A),addr B)),$ SALT), brle), concat(a $1,\sim M$ 3)), concat(a $2,\sim M$ 4)), AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M_5,concat($-concat(concat(concat(a^3, \sim M^7), btlk), addr A), addr B)),$ SALT), brle), concat($\sim \overline{M}_9$, a=4)), concat($\sim \overline{M}_10$, a=5))) (AES CCM(p224(gen,s2 1),AES CMAC(AES CMAC(AES CMAC($\overline{HMAC}_{SHA256}(p22\overline{4}(gen,pri_P_1),concat(conc$ 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(a 3,nb 2), btlk),addr_A),addr_B)),SALT),brle),concat(skds_2, $a_4)$),concat(ivs_2,a_5))) \sim M_14 = AES_CCM(s1_2,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256($p224(gen,pri_{-}P_{1}),concat(conca$ a_3,nb_2),btlk),addr_A),addr_B)),SALT),brle),concat($skds_2,a_4)$), $concat(ivs_2,a_5)$) \sim M_15 = AES_CCM(r1_6,AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256($p224(gen,pri_{-}P_{1}),concat(conca$ a_3,nb_2),btlk),addr_A),addr_B)),SALT),brle),concat($skds_2,a_4)$), $concat(ivs_2,a_5)$) $\sim X_5 = (AES_CCM(sdec(\sim M_14,AES_CMAC(AES_CMAC$ HMAC_SHA256(~M_5,concat(concat(concat(concat(a_3, \sim M 7), btlk), addr A), addr B)), SALT), brle), concat(~M $9,a^{-}4)$), concat(~ \overline{M} 10, a $\overline{5}$)), AES CMAC(AES CMAC(AES $\overline{CMAC}(HMAC\ SHA2\overline{5}6(\sim\overline{M},concat(c$ \sim M_1,a),btlk),addr_A),addr_B)),SALT),brle),concat(a $1, \sim \overline{M}$ 3)), concat(a $\overline{2}, \sim M_4)$), AES_CCM(sdec($\sim M_15$), 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($\sim \overline{M}_9$, a=\frac{4}{4}), concat($\sim \overline{M}_1$ 10, a=\frac{5}{9}), AES_CMAC(AES_CMAC(AES_CMAC(HMAC_SHA256(~M,concat(- concat(concat($\sim \overline{M}_1$,a),btlk),a \overline{d} dr_A),addr_B)), SALT), brle), concat(a_1, $\overline{}$ M_3)), concat(a_2, $\overline{}$ 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 , skd m_2)), concat(a_2 , ivm $_2$), AES_CCM(r1_6, AES_CMAC(ĀES_CMĀC(AES_CMĀC(HMĀC_SHA256(p224(gen,pri_C_1), concat(concat(concat(na 2,a),btlk),addr A), addr_B)),SALT),brle),concat(a_1̄,skdm_2)),concat($a_2,ivm_2)$ $\sim X_6 = SHA256(concat(get_id(add_G(p224(gen,sdec(\sim M_14, M_2)))))$ 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($\sim \overline{M}$ 9, a $\overline{4}$)), concat($\sim \overline{M}$ 10, a $\overline{5}$)), sdec(~M 12,AES CMAC(AES CMAC(AES CMAC(HMAC SHA256(\sim M,concat(concat(concat(concat(\sim M 1,a),btlk),addr A), addr B)), SALT), brle), concat(a $1, \overline{\sim} M$ 3)), concat(a_2,~M_4))),sdec(~M_15,AES_CMAC(AES_CMA ~M 7),btlk),addr A),addr B)),SALT),brle),concat(\sim M 9,a 4)),concat(\sim M 10,a 5)),sdec(\sim 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), $concat(a_1, \sim M_3)$, $concat(a_2, \sim M_4)), \sim M_17)$

A trace has been found.

SHA256(concat(get_id(add_G(p224(gen,s1_2),p224(gen,s2_1)),r1_6,r2_7),salt2_2)) **Honest Process** Attacker Beginning of process step1p Beginning of process step1c Beginning of process step2c Beginning of process step2p Beginning of process user Beginning of process step3c Beginning of process step3p {59} new pri_P_1 {1}new pri_C_1 \sim M = p224(gen,pri_C_1) {8}new na_2 HMAC_SHA256(a,concat(concat(gen,~M),zero)) = HMAC_SHA256(a,concat(concat(gen,p224(gen,pri_C_1)),zero)) \sim M_1 = na_2 ~X 1 {37} new skdm_2 $(\sim M_3, \sim M_4) = (skdm_2, ivm_2)$ (a_1,a_2) gen $\sim M_5 = p224(gen, pri_P_1)$ {66} new nb_2 \sim M_6 = HMAC_SHA256(nb_2,concat(concat(p224(gen, pri_P_1),gen),zero)) a_3 \sim M 7 = nb 2 ~X 2 ~M_8 = HMAC_SHA256(p224(gen,pri_P_1),concat(concat(concat(nb_2,a_3),zero),iocap_B), addr_B),addr_A)) {96} new skds_2 (a_4,a_5) $(\sim M_9, \sim M_10) = (skds_2, ivs_2)$ {103}new s1_2 ~M 11 ~X 3 {46} new s2_1 {47} new r2_7 $(\sim M_12, \sim M_13)$ ~X 4 $(\sim M_114, \sim M_15)$ {114}insert p1p(addr_A,get_id(add_G(p224(gen,s1_2), p224(gen,s2_1)),r1_6,r2_7)) ~X 5 {58} insert p1c(addr_B,get_id(add_G(p224(gen,s1_2), p224(gen,s2_1)),r1_6,r2_7)) {119}get p1c(addr_B,get_id(add_G(p224(gen,s1_2), p224(gen,s2_1)),r1_6,r2_7)) {124} get p1p(addr_A,get_id(add_G(p224(gen,s1_2), p224(gen,s2_1)),r1_6,r2_7)) $get_id(add_G(p224(gen,s1_2),p224(gen,s2_1)),r1_6,$ get_id(add_G(p224(gen,s1_2),p224(gen,s2_1)),r1_6, yes_confirm {118}insert p2c(addr_B,get_id(add_G(p224(gen,s1_2), p224(gen,s2_1)),r1_6,r2_7)) {140}get p2c(addr_B,get_id(add_G(p224(gen,s1_2), p224(gen,s2_1)),r1_6,r2_7)) $\begin{array}{c} \{133\} \textcolor{red}{event} \ send \ central(get \ id(add \ G(p224(gen, s1_2), p224(gen, s2_1)), r1_6, r2_7)) \end{array}$ \sim M_16 = SHA256(concat(get_id(add_G(p224(gen,s1_2), p224(gen,s2_1)),r1_6,r2_7),a_6)) {135}new salt2_2 \sim M 17 = salt2 | 2 ~X 6