A trace has been found.

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(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))

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(HMAC\_SHA256(p224(gen,pri\_P\_1),

~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))

a 1,skdm 2)),concat(a 2,ivm 2))

~X\_4 = (AES\_CCM(sdec(~M\_12,AES\_CMAC(AES

(AES CCM(p224(gen,s2 1),AES CMAC(AES CMAC(AES CMAC(

~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

(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(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)))

**Honest Process** Attacker Beginning of process step1p Beginning of process step1c Beginning of process user Beginning of process step2c Beginning of process step2p {60} new pri\_P\_1 {1}new pri\_C\_1  $\sim$ M = p224(gen,pri C 1|) gen {8}new na\_2  $HMAC_SHA256(a,concat(concat(gen,\sim M),zero)) = HMAC_SHA256(a,concat(gen,p224(gen,pri_C_1)),zero))$  $\sim$ M 1 = na 2  $\sim$ M\_2 = #MAC\_SHA256(p224(gen,pri\_C\\_1),concat(concat( concat(concat(na\_2,a),zero),iodap\_A),addr\_A),
addr\_B)) ~X 1 {37} new skdm\_2 {38} **new** ivm 2  $(\sim M_3, \sim M_4) = (skdm_2, ivm_2)$  $(a_1,a_2)$ gen  $\sim M_5 = 1224(gen, pri_P_1)$ {67} new nb\_2  $\sim$  M\_6 = HMAC\_SHA25\( \text{f(nb\_2,concat(concat(p224(gen,  $pri_P_1),gen),zero))$ a 3  $\sim M 7 = nb 2$ ~X 2  $\sim$ M\_8 = HMAC\_SHA256(p224(gen,pri\_P\_1),concat(concat( concat(concat(concat(nb\_2,a\_3),zero),iocap\_B), addr\_B),addr\_A)) {97} new skds 2 {98} new ivs 2 (a\_4,a\_5)  $(\sim M_9, \sim M_10) = (skds_2, ivs_2)$ {104}new s1\_2 {105}new r1\_6 ~M 11 ~X 3 {46} new s2\_1 {47} new r2\_7  $(\sim M 12, \sim M 13)$ ~X 4  $(\sim M 14, \sim M 15)$ {116}insert p1p(addr\_A,get\_id(add\_G(p224(gen,s1\_2), p224(gen,s2\_1)),concat(r1\_6,r2\_7))) ~X 5 {59} insert p1c(addr\_B,get\_id(add\_G(p224(gen,s1\_2), p224(gen,s2\_1)),concat(r1\_6,r2\_7))) {122}get p1c(addr\_B,get\_id(add\_G(p224(gen,s1\_2), p224(gen,s2\_1)),concat(r1\_6,r2\_7)))  $\begin{array}{l} \{127\} \textcolor{red}{\texttt{get}} \ p1p(addr\_A, \textcolor{red}{\texttt{get}\_id}(add\_G(p224(\textcolor{red}{\texttt{gen,s1}\_2}), \\ p224(\textcolor{red}{\texttt{gen,s2}\_1})), \textcolor{red}{\texttt{concat}(r1\_6, r2\_7))) \end{array}$  $get_id(add_G(p|224(gen,s1_2),p224(gen,s2_1)),concat(gen,s2_1))$ r1\_6,r2\_7))  $|get_id(add_G(p224(gen,s1_2),p224(gen,s2_1)),concat(gen,s2_1))|$ r1 6, r2 7)) yes\_confirm {119}new tmp\_2  $(\sim M_16, \sim M_17) = (tmp_2, AES_CCM(s, get_id(add_G(p224(gen, s1_2), p224(gen, s2_1)), concat(r1_6, r2_7)),$ tmp 2))

The attacker has the message sdec(~M\_17,get\_id(add\_G(p224(gen,sdec(~M\_14,AES\_CMAC(AE

concat(~M 10,a 5)),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(

 $a_1, \sim M_3)$ ,  $concat(a_2, \sim M_4))), \sim M_16) = s$