A trace has been found.

Honest Process {1}new exp_C_1 {2}new exp_P_1 Beginning of process step1c Beginning of process step2cpein Be \sim M = p256(gen,exp_C \downarrow 1) gen {9}insert p1c(addr_B,p256(gen,exp_C_1),gen,p256(gen,exp_C_1)) $\sim M_1 = p256(gen, exp_P_1)$ {14}insert p1p(addr_A,a,p256(gen,exp_P_1),p256(a,exp_P_1)) {43}get p1p(addr_A,a,p256(gen,exp_P_1),p256(a,exp_P_1)) exp_P_1)) {29}new nb_8 \sim M_2 = HMAC_SHA256(nb_8,concat(concat(p256(gen, exp_P_1),a),zero)) \sim M_3 = nb_8 {55} get p1c(addr_B,p256(gen,exp_C_1),gen,p256(gen,exp_C_1)) $SHA256(concat(concat(concat(a,p256(gen,exp_P_1)), a_1), nb_8))$ yes_confirm {42}insert p2p(addr_A,a_1,nb_8,zero,zero,p256(a,exp_P_1)) SHA256(concat(concat(a,p256(gen,exp_P_1)), a_1),nb_8))
$$\label{eq:mass_section} \begin{split} \sim & M_4 = HMAC_SHA256(na_8,concat(concat(p256(gen, exp_C_1),gen),SHA256(concat(concat(concat(a,p256(gen, exp_P_1)),a_1),nb_8)))) \end{split}$$
 \sim M_5 = na_8 {54}insert p2c(addr_B,na_8,a_2,SHA256(concat(concat(concat(a,p256(gen,exp_P_1)),a_1),nb_8)),SHA256(concat(concat(a,p256(gen,exp_P_1)),a_1),nb_8)),p256(gen,exp_C_1)) {86} get p2c(addr_B,na_8,a_2,SHA256(concat(concat(concat(a,p256(gen,exp_P_1)),a_1),nb_8)),SHA256(concat(concat(a,p256(gen,exp_P_1)),a_1),nb_8)),p256(gen,exp_C_1))

{77} event send_central(p256(gen,exp_C_1)) {84} event recv_central(p256(gen,exp_C_1))

Abbreviations a_2,concat(concat(gen,p256(gen,exp_C_1)),SHA256(concat(concat(a,p256(gen,exp_P_1)),a_1),

 $\sim M_6 = HMAC_SHA256(p256(gen,exp_C_1),concat(concat(concat(concat(na_8,a_2),SHA256(concat(concat(concat(concat(a,p256(gen,exp_P_1)),a_1),nb_8))),iocap_A), \\ addr_A),addr_B))$ ~X_2 = HMAC_SHA256(~M,concat(concat(concat(concat(concat(concat(a,~M_1), a_1),~M_3))),iocap_B),addr_B),addr_A))
= HMAC_SHA256(

p256(gen,exp_C_1),concat(concat(concat(concat(concat(a_2,na_8),SHA256(concat(concat(concat(a,p256(gen,exp_P_1)),a_1),nb_8))),iocap_B),addr_B), addr_A))

Attacker