Abbreviations

~X\_1 = HMAC\_SHA256(~M\_1,concat(concat(concat(concat(concat(concat(concat(concat(concat(concat(concat(concat(concat(concat(concat(concat(p.256(gen,exp\_P\_1),concat(concat(concat(concat(concat(concat(concat(concat(concat(a,nb\_8),zero),iocap\_A),addr\_A),addr\_B)) A trace has been found.

**Honest Process** Attacker {1}new exp\_C\_1 {2}new exp\_P\_1 Beginning of process step2peout Beginning of process step2peou  $\sim$ M = p256(gen,exp\_C $\downarrow$ 1)  $\sim M_1 = p256(gen, exp_P_1)$ {14}insert p1p(addr\_A,gen,p256(gen,exp\_P\_1),p256(gen,exp\_P\_1)) {43}get p1p(addr\_A,gen,p256(gen,exp\_P\_1),p256(gen,exp\_P\_1)) gen,exp\_P\_1)) {29}new nb\_8  $\sim$  M\_2 = HMAC\_SHA256(nb\_8,concat(concat(p256(gen, exp\_P\_1),gen),zero))  $\sim$  M\_3 = nb\_8 SHA256(concat(concat(concat(gen,p256(gen,exp\_P\_1)), a),nb\_8)) yes\_confirm {42}insert p2p(addr\_A,a,nb\_8,zero,zero,p256(gen, exp\_P\_1))  $\begin{array}{c} \{100\} \\ \text{get p2p(addr\_A,a,nb\_8,zero,zero,p256(gen,exp\_P\_1))} \end{array} \\$ ~X\_1