~X_2 = HMAC_SHA256(~M_1,concat(concat(concat(concat(concat(concat(a_2,~M_4),SHA256(concat(concat(concat(~M,a),~M_2), a_1))),iocap_A),addr_A),addr_B))
= HMAC_SHA256(
p256(gen,exp_P_1),concat(c concat(a_2,nb_8),SHA256(concat(concat(concat(p256(gen,exp_C_1),a),na_8),a_1))),iocap_A),addr_A),
addr_B)) **Honest Process** Attacker {1}new exp_C_ {2}new exp_P_1 Beginning of process step2pein Beginning Beginning Beginning Beginning Beginning Beginning Beginning Beginning Beginning Beg \sim M = p256(gen,exp_C \downarrow 1) {9}insert p1c(addr_B,p256(gen,exp_C_1),a,p256(a,exp_C_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)) $HMAC_SHA256(a_1,concat(concat(a,\sim M),zero)) = HMAC_SHA256(a_1,concat(concat(a,p256(gen,exp_C_1)),zero))$ \sim M_2 = na_8 {72}get p1p(addr_A,gen,p256(gen,exp_P_1),p256(gen,exp_P_1)) SHA256(concat(concat(p256(gen,exp_C_1), a),na_8),a_1)) yes_confirm {27} insert p2c(addr_B,na_8,a_1,zero,zero,p256(a,exp_C_1)) SHA256(concat(concat(concat(p256(gen,exp_C_1), a),na_8),a_1)) {62} new nb_8 \sim M_4 = nb_8 {71}insert p2p(addr_A,a_2,nb_8,SHA256(concat(concat(concat(p256(gen,exp_C_1),a),na_8),a_1)),SHA256(concat(p256(gen,exp_C_1),a),na_8), a_1)),p256(gen,exp_P_1))

Abbreviations

a_2,concat(concat(gen,p256(gen,exp_P_1)),SHA256(concat(concat(concat(p256(gen,exp_C_1),a),na_8),