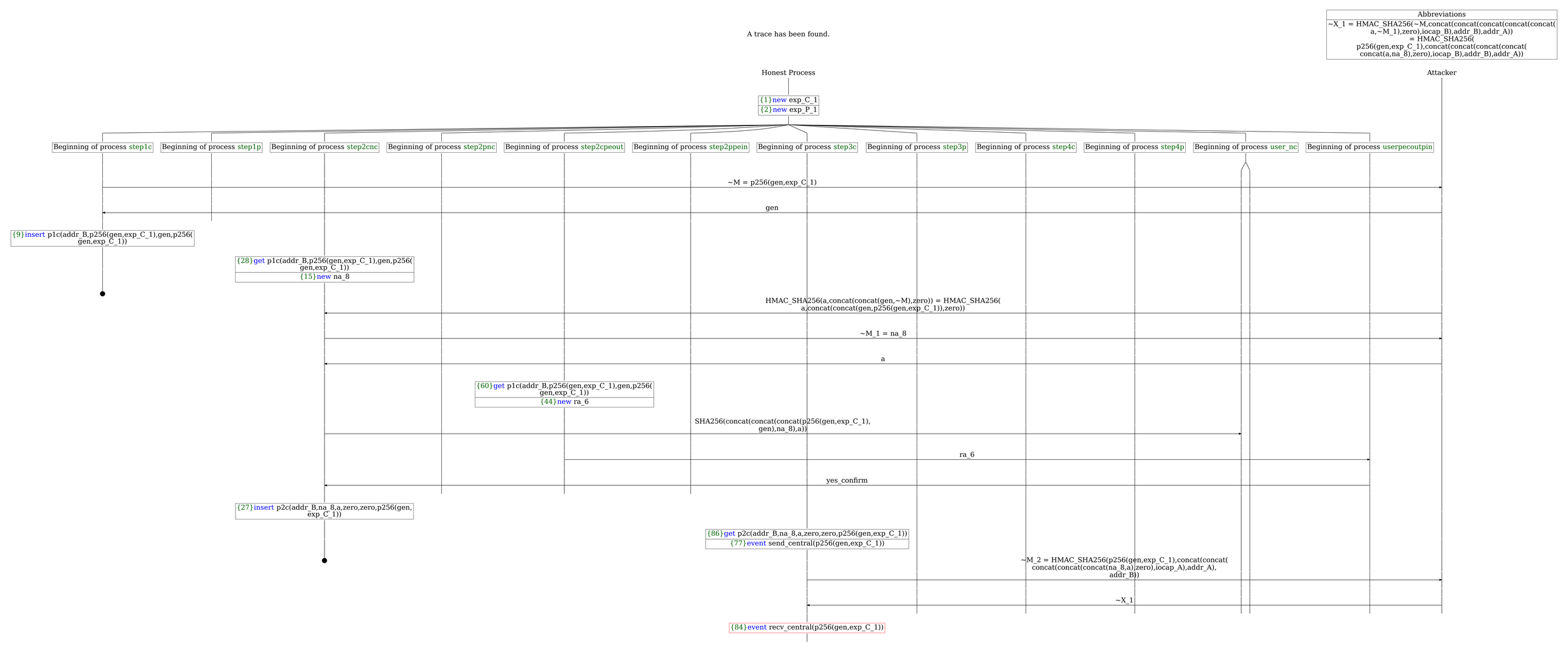
Abbreviations
~X_1 = HMAC_SHA256(~M,concat(concat(concat(concat(concat(
a,~M_1),zero),iocap_B),addr_B),addr_A))
= HMAC_SHA256(
p256(gen,exp_C_1),concat(concat(concat(concat(
concat(a,na_8),zero),iocap_B),addr_B),addr_A))
A trace has been found.
Honest Process
Attacker
{1}new exp_C_1
{2}new exp_P_1
Beginning of process step1c
Beginning of process step1p
Beginning of process step2cnc
Beginning of process step2pnc
Beginning of process step2cpeout
Beginning of process step2ppein
Beginning of process step3c
Beginning of process step3p
Beginning of process step4c
Beginning of process step4p
Beginning of process user_nc
Beginning of process userpecoutpin
~M = p256(gen,exp_C_1)
gen
{9}insert p1c(addr_B,p256(gen,exp_C_1),gen,p256(
gen,exp_C_1))
{28}get p1c(addr_B,p256(gen,exp_C_1),gen,p256(
gen,exp_C_1))
{15}new na_8
HMAC_SHA256(a,concat(concat(gen,~M),zero)) = HMAC_SHA256(
a,concat(concat(gen,p256(gen,exp_C_1)),zero))
~M_1 = na_8
a
{60}get p1c(addr_B,p256(gen,exp_C_1),gen,p256(
gen,exp_C_1))
{44}new ra_6
SHA256(concat(concat(concat(p256(gen,exp_C_1),
gen),na_8),a))
ra_6
yes_confirm
{27}insert p2c(addr_B,na_8,a,zero,zero,p256(gen,
exp_C_1))
{86}get p2c(addr_B,na_8,a,zero,zero,p256(gen,exp_C_1))
{77}event send_central(p256(gen,exp_C_1))
~M_2 = HMAC_SHA256(p256(gen,exp_C_1),concat(concat(
concat(concat(concat(na_8,a),zero),iocap_A),addr_A),
addr_B))
~X_1
{84}event recv_central(p256(gen,exp_C_1))