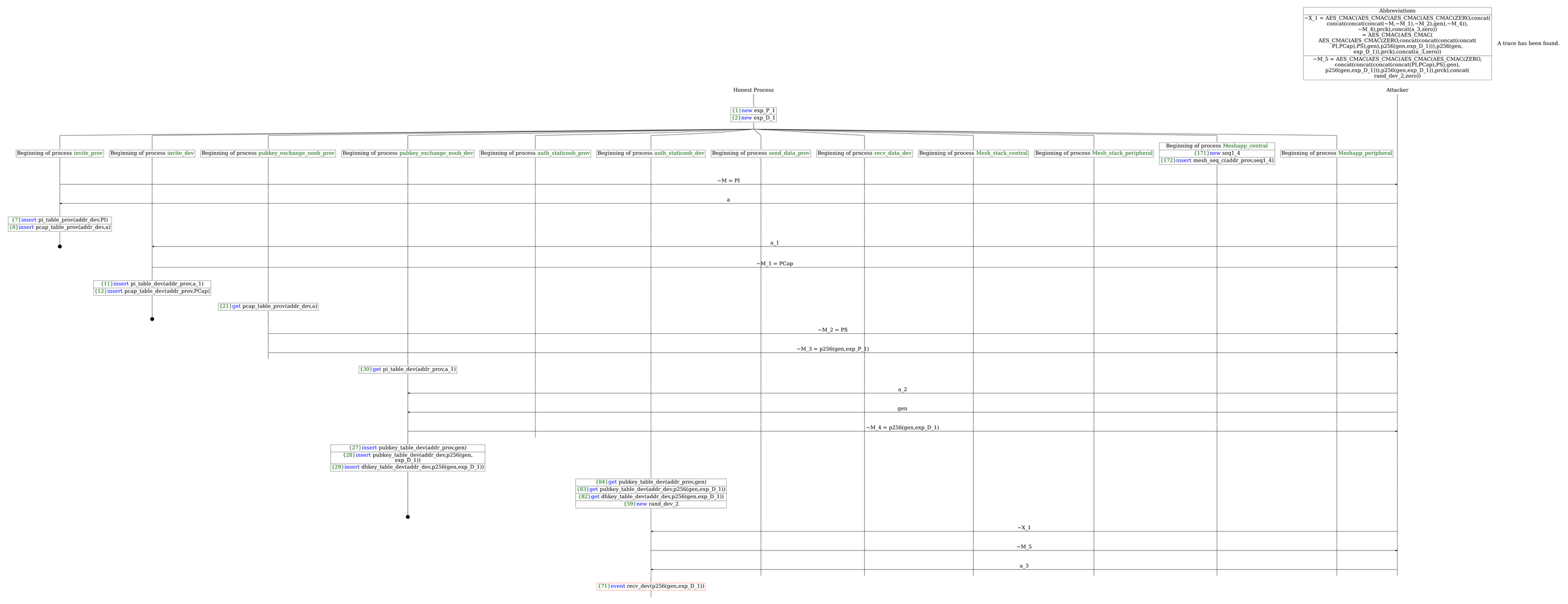
Abbreviations
~X_1 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(concat(~M_1),~M_2),gen),~M_4)),~M_4),prck),concat(a_3,zero)) = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1)),p256(gen,exp_D_1)),prck),concat(a_3,zero))
~M_5 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(concat(concat(concat(PI,PCap),PS),gen),p256(gen,exp_D_1))),p256(gen,exp_D_1)),prck),concat(rand_dev_2,zero))
A trace has been found.
Honest Process
Attacker
{1}new exp_P_1
{2}new exp_D_1
Beginning of process invite_prov
Beginning of process invite_dev
Beginning of process pubkey_exchange_noob_prov
Beginning of process pubkey_exchange_noob_dev
Beginning of process auth_staticoob_prov
Beginning of process auth_staticoob_dev
Beginning of process send_data_prov
Beginning of process recv_data_dev
Beginning of process Mesh_stack_central
Beginning of process Mesh_stack_peripheral
Beginning of process Meshapp_central
{171}new seq1_4
{172}insert mesh_seq_c(addr_prov,seq1_4)
Beginning of process Meshapp_peripheral
~M = PI
a
{7}insert pi_table_prov(addr_dev,PI)
{8}insert pcap_table_prov(addr_dev,a)
a_1
~M_1 = PCap
{11}insert pi_table_dev(addr_prov,a_1)
{12}insert pcap_table_dev(addr_prov,PCap)
{21}get pcap_table_prov(addr_dev,a)
~M_2 = PS
~M_3 = p256(gen,exp_P_1)
{30}get pi_table_dev(addr_prov,a_1)
a_2
gen
~M_4 = p256(gen,exp_D_1)
{27}insert pubkey_table_dev(addr_prov,gen)
{28}insert pubkey_table_dev(addr_dev,p256(gen,exp_D_1))
{29}insert dhkey_table_dev(addr_dev,p256(gen,exp_D_1))
{84}get pubkey_table_dev(addr_prov,gen)
{83}get pubkey_table_dev(addr_dev,p256(gen,exp_D_1))
{82}get dhkey_table_dev(addr_dev,p256(gen,exp_D_1))
{59}new rand_dev_2
~X_1
~M_5
a_3
{71}event recv_dev(p256(gen,exp_D_1))