~M_4 = AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO, concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)),prck),concat(rand_prov_2,zero))

A trace has been found.

Honest Process Attacker $\{1\}$ new exp_P_3 $\{2\}$ new exp_D_1 Beginning of process invite_prov Beginning of process auth_staticoob_prov Beginning of process auth_staticoob_prov Beginning of process auth_staticoob_dev Beginning of process send_data_prov Beginning of proces \sim M = PI {7}insert pi_table_prov(addr_dev,PI)
{8}insert pcap_table_prov(addr_dev,a) \sim M_1 \neq 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) \sim M_2 = PS $\sim M_3 = p256(gen, exp_P_1)$ {18} insert pubkey_table_prov(addr_prov,p256(gen, exp_P_1)) {19}insert pubkey_table_prov(addr_dev,gen)
{20}insert dhkey_table_prov(addr_prov,p256(gen, exp_P_1)) {57} get pubkey_table_prov(addr_prov,p256(gen,exp_P_1))
{56} get pubkey_table_prov(addr_dev,gen)
{55} get dhkey_table_prov(addr_prov,p256(gen,exp_P_1)) {32}new rand_prov_2 \sim M_4 ~M_4 {42}event send_prov(p256(gen,exp_P_1)) \sim M_5 = rand_prov_2 \sim M_5 = rand_prov_2 {46} event recv_prov(p256(gen,exp_P_1)) {51} insert key_table_prov(addr_dev,AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(AES_CMAC(AES_CM concat(concat(PI,PCap),PS),p256(gen,exp_P_1)), gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)), prsk)) {54} insert nonce_table_prov(addr_dev,AES_CMAC(AES_CMAC(ZERO,concat(concat(AES_CMAC(ZERO,concat(PI,PCap),PS), p256(gen,exp_P_1)),gen)),rand_prov_2),rand_prov_2)), p256(gen,exp_P_1)),prsn)) {89} get key_table_prov(addr_dev,AES_CMAC(AES_CMAC(AES_CMAC(AES_CMAC(ZERO,concat(Concat(AES_CMAC(ZERO,concat(Concat(Concat(Concat(PI,PCap),PS),p256(gen,exp_P_1)), gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)), {88} get nonce_table_prov(addr_dev,AES_CMAC(AES_ concat(concat(concat(PI,PCap),PS),p256(gen,exp_P_1)), gen)),rand_prov_2),rand_prov_2)),p256(gen,exp_P_1)), ~M 6