Abbreviations

~M\_4 = AES\_CMAC(AES\_CMAC(AES\_CMAC(ZERO, concat(concat(concat(PI,PCap),PS),p256(gen,exp\_P\_1)),gen)),p256(gen,exp\_P\_1)),prck),concat(rand\_prov\_2,zero))

~M\_6 = AES\_CCM(koys\_AES\_CMAC(AES\_CM

~M\_6 = AES\_CCM(keys,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)), prsk),AES\_CMAC(AES\_CMAC(AES\_CMAC(ZERO,concat(concat( AES\_CMAC(ZERO,concat(concat(concat(PI,PCap), PS),p256(gen,exp\_P\_1)),gen)),rand\_prov\_2),rand\_prov\_2)), p256(gen,exp\_P\_1)),prsn))

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 auth\_staticoob\_prov Begin  $\sim$ 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(Concat(AES\_CMAC(ZERO,concat(Concat(AES\_CMAC(ZERO,concat(Concat(AES\_CMAC(ZERO,concat(Concat(AES\_CMAC(ZERO,concat(Concat(Concat(AES\_CMAC(ZERO,concat(Co 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(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\_CMAC(AES\_CMAC(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(ZERO,concat(AES\_CMAC(A concat(concat(PI,PCap),PS),p256(gen,exp\_P\_1)), gen)),rand\_prov\_2),rand\_prov\_2)),p256(gen,exp\_P\_1)),  $\sim$ M\_6