Abbreviations
~M = symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)
~M_1 = sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg))
~M_2 = ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a))

A trace has been found.

Honest Process

Attacker

!

!

Beginning of process processSend

{5}new r_2

{3}let principalA: G = exp(P,b)

{6}let Z: G = exp(P,emul(r_2,b))

{2}let a_1: exponent = a

{4}let selfA: G = exp(P,a)

{7}let k: key = hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX))

{8}event termA(a,exp(P,b),hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)))

{12}event ASend(a,exp(P,b),secretMsg)

{13}event ASendKM(a,exp(P,b),hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)

{9}let ciphertext: bitstring = symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)

{10}let tag: exponent = sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg))

{11}let sig: exponent = ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a))

Beginning of process processRecv

(~M,~M_1,~M_2)

(~M,~M_1,~M_2)

{17}let principalB: G = exp(P,a)

{20}let tPYa: G = exp(P,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a))

{16}let b_1: exponent = b

{21}let Z_1: G = exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b))

{18}let selfB: G = exp(P,b)

{22}let k_1: key = hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX))

{23}event termB(exp(P,a),hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)))

{25}if (sauthtag(hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)) = sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)) then

{24}let msg: bitstring = symdec(hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg))

{26}event BRecv(b,exp(P,a),symdec(hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg))

{27}event BRecvKM(b,exp(P,a),hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symdec(hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)))

{28}event BRecvMsg(symdec(hkdf(hash(exp(P,emul(emul(eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(sauthtag(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)),a)),b)),b)),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg))