Abbreviations
~M_4 = symenc(hkdf(hash(exp(g,emul(r_2,b))),concat(exp(g,a),exp(g,b),getid(exp(g,a)),getid(exp(g,b)),kCTX)),secretMsg)
~M_5 = sauthtag(hkdf(hash(exp(g,emul(r_2,b))),concat(exp(g,a),exp(g,b),getid(exp(g,a)),getid(exp(g,b)),kCTX)),symenc(hkdf(hash(exp(g,emul(r_2,b))),concat(exp(g,a),exp(g,b),getid(exp(g,a)),getid(exp(g,b)),kCTX)),secretMsg))
~M_6 = ediv(r_2,eadd(sauthtag(hkdf(hash(exp(g,emul(r_2,b))),concat(exp(g,a),exp(g,b),getid(exp(g,a)),getid(exp(g,b)),kCTX)),symenc(hkdf(hash(exp(g,emul(r_2,b))),concat(exp(g,a),exp(g,b),getid(exp(g,a)),getid(exp(g,b)),kCTX)),secretMsg)),a))

A trace has been found.

Honest Process

Attacker

(~M,~M_1,~M_2,~M_3) = (b,kCTX,exp(g,a),exp(g,b))

!

!

Beginning of process processSend

{6}new r_2

{4}let principalA: G = exp(g,b)

{7}let Z: G = exp(g,emul(r_2,b))

{3}let a_1: exponent = a

{5}let selfA: G = exp(g,a)

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

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

{13}event ASend(a,exp(g,b),secretMsg)

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

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

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

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

Beginning of process processRecv

(~M_4,~M_5,~M_6)

(~M_4,~M_5,~M_6)

{18}let principalB: G = exp(g,a)

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

{17}let b_1: exponent = b

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

{19}let selfB: G = exp(g,b)

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

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

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

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

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

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

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