Abbreviations
~M = 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_1 = 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_2 = 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

{1}new session_id_3

!

!

Beginning of process processSend

{7}new r_2

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

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

{3}let a_1: exponent = a

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

{9}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))

{10}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)))

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

{15}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)

{11}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)

{12}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))

{13}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,~M_1,~M_2)

(~M,~M_1,~M_2)

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

{23}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))

{18}let b_1: exponent = b

{24}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))

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

{25}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))

{26}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)))

{28}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))) = 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))

{27}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))

{29}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))

{30}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)))

{31}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)))