\sim 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))), A trace has been found. concat(exp(g,a),exp(g,b),getid(exp(g,a)),getid(exp(g,b)),kCTX)),secretMsg)) \sim 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)) **Honest Process** Attacker Beginning of process processSend {5}new r_2 $\{3\}$ **let** principalA: $G = \exp(g,b)$ $\{6\}$ **let** Z: $G = \exp(g, \operatorname{emul}(r_2, b))$ $\{2\}$ **let** a_1: exponent = a $\{4\}$ let selfA: $G = \exp(g,a)$ ${7}$ **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)) {8}event termA(a,exp(g,b),hkdf(hash(exp(g,emul($r_2,b))),concat(exp(g,a),exp(g,b),getid(exp(g,a),exp(g,b),exp(g,b),getid(exp(g,a),exp(g,b),exp(g,b),getid(exp(g,a),exp(g,b),exp(g,b),exp(g,b),getid(exp(g,a),exp(g,b),exp(g,$ a)),getid(exp(g,b)),kCTX))) {12}event ASend(a,exp(g,b),secretMsg) {13}event ASendKM(a,exp(g,b),hkdf(hash(exp(g,emul(Beginning of process processRecv r_2,b))),concat(exp(g,a),exp(g,b),getid(exp(g, a)),getid(exp(g,b)),kCTX)),secretMsg) {9}**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) {10} 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)) {11}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)) $(\sim M, \sim M_1, \sim M_2)$ $(\sim M, \sim M_1, \sim M_2)$ $\{17\}$ **let** principalB: $G = \exp(g,a)$ $\{20\}$ let tPYa: $G = \exp(g, eadd(sauthtag(hkdf(hash($ $\exp(g, \operatorname{emul}(r_2, b))), \operatorname{concat}(\exp(g, a), \exp(g, b), \operatorname{getid}(a))$ exp(g,a)),getid(exp(g,b)),kCTX)),symenc(hkdf(hash($\exp(g, \operatorname{emul}(r_2, b))), \operatorname{concat}(\exp(g, a), \exp(g, b), \operatorname{getid}(a))$ $\exp(g,a)$), $getid(\exp(g,b))$, kCTX), secretMsg), a) $\{16\}$ **let** b_1: exponent = b $\{21\}$ 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($hash(exp(g,emul(r_2,b))),concat(exp(g,a),exp(g,a))$ 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)) $\{18\}$ let selfB: $G = \exp(g,b)$ {22}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)) {23}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))) {25}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)),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)) = sauthtag(hkdf(hash($\exp(g, \operatorname{emul}(r_2, b))), \operatorname{concat}(\exp(g, a), \exp(g, b), \operatorname{getid}(g, a))$ exp(g,a)),getid(exp(g,b)),kCTX)),symenc(hkdf(hash($\exp(g, \operatorname{emul}(r_2, b))), \operatorname{concat}(\exp(g, a), \exp(g, b), \operatorname{getid}(a))$ exp(g,a)),getid(exp(g,b)),kCTX)),secretMsg))) {24}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)) {26}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), (g,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 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)),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 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)),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)))

Abbreviations

 \sim 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)