concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)),secretMsg)) \sim M_6 = ediv(r_2,eadd(symtag(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)) **Honest Process** Attacker $(\sim M, \sim M_1, \sim M_2, \sim M_3) = (b, kCTX, exp(P,a), exp(P,b))$ Beginning of process processSend {6}new r_2 $\{4\}$ **let** principalA: $G = \exp(P,b)$ ${7}$ let Z: G = exp(P,emul(r_2,b)) $\{3\}$ **let** a_1: exponent = a $\{5\}$ **let** selfA: $G = \exp(P,a)$ $\{8\}$ **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)) {9}event termA(a,exp(P,b),hkdf(hash(exp(P,emul($r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp(P,b),getid(exp(P,a),exp$ a)),getid(exp(P,b)),kCTX))) {13}event ASend(a,exp(P,b),secretMsg) {14}event ASendKM(a,exp(P,b),hkdf(hash(exp(P,emul(Beginning of process processRecv r_2,b))),concat(exp(P,a),exp(P,b),getid(exp(P, a)),getid(exp(P,b)),kCTX)),secretMsg) {10} 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) {11}let tag: exponent = symtag(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)) {12}let sig: exponent = ediv(r_2,eadd(symtag(hkdf($hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,a))$ 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)) $(\sim M_4, \sim M_5, \sim M_6)$ $(\sim M_4, \sim M_5, \sim M_6)$ $\{18\}$ let principalB: $G = \exp(P,a)$ {21}let tPYa: G = exp(P,eadd(symtag(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)) $\{17\}$ **let** b_1: exponent = b $\{22\}$ let Z_1: G = exp(P,emul(emul(eadd(symtag(hkdf($hash(exp(P,emul(r_2,b))),concat(exp(P,a),exp(P,a))$ 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(symtag(hkdf(hash($\exp(P, \operatorname{emul}(r_2, b))), \operatorname{concat}(\exp(P, a), \exp(P, b), \operatorname{getid}(a))$ exp(P,a)),getid(exp(P,b)),kCTX)),symenc(hkdf(hash($\exp(P, \operatorname{emul}(r_2, b))), \operatorname{concat}(\exp(P, a), \exp(P, b), \operatorname{getid}(a))$ $\exp(P,a)$), $\gcd(\exp(P,b))$, kCTX), $\gcd(Span(P,a))$, $\gcd(Span(P,a)$ $\{19\}$ let selfB: $G = \exp(P,b)$ {23}let k_1: key = hkdf(hash(exp(P,emul(emul(eadd(symtag(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($\exp(P,a), \exp(P,b), \gcd(\exp(P,a)), \gcd(\exp(P,a))$ b)),kCTX)),secretMsg)),a),ediv(r_2,eadd(symtag(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))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P,b)),kCTX)) {24}event termB(b,exp(P,a),hkdf(hash(exp(P,emul(emul(eadd(symtag(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(symtag(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))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P, b)),kCTX))) {26}if (symtag(hkdf(hash(exp(P,emul(emul(eadd(symtag(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(symtag(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))),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)) = symtag(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))) {25}let msg: bitstring = symdec(hkdf(hash(exp(P,emul(emul(eadd(symtag(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(symtag(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))),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 BRecv(b,exp(P,a),symdec(hkdf(hash(exp(P,emul(emul(eadd(symtag(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(symtag(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))),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 BRecvKM(b,exp(P,a),hkdf(hash(exp(P,emul(emul(eadd(symtag(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(symtag(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))),concat(exp(P,a),exp(P,b),getid(exp(P,a)),getid(exp(P, b)),kCTX)),symdec(hkdf(hash(exp(P,emul(emul(eadd(symtag(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(symtag(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))),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))) {29}event BRecvMsg(symdec(hkdf(hash(exp(P,emul(emul(eadd(symtag(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(symtag(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))),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)))

Abbreviations

 \sim M_4 = 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)

 \sim M_5 = symtag(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))),

A trace has been found.