eadd(rB_1,emul(s_1,h1(idB,exp(g,rB_1)))))),eadd(eadd(rA_1,emul(h1(idA,exp(g,rA_1)),s_1)),x_1)), exp(exp(g,a_10),x_1))) A trace has been found. **Honest Process** Attacker {1}new a_3 \sim M = exp(g,a_3) {4}new b_3 $\sim M_1 = \exp(g,b_3)$ {7}new s_1 \sim M_2 = exp(g,s_1) {10} new rA_1 {14}new rB_1 Beginning of process principalA Beginning of process principalB Beginning of process principalA Beginning of process principalB $(\sim M, \sim M_1) = (\exp(g, a_3), \exp(g, b_3))$ {22}new x_1 $(\sim M_3, \sim M_4, \sim M_5) = (idA, exp(g, rA_1), exp(g, x_1))$ $(\sim M, a_5) = (\exp(g, a_3), a_5)$ {22} new x_2 $(\sim M_6, \sim M_7, \sim M_8) = (idA, exp(g, rA_1), exp(g, x_2))$ $(\sim M_1, a_7) = (\exp(g,b_3), a_7)$ $(idA,\sim M \downarrow 4,a_9) = (idA,exp(g,rA_1),a_9)$ {49} new y_1 $(\sim M_9, \sim M_10, \sim M_11) = (idB, exp(g, rB_1), exp(g, y_1))$ $(idB, \sim M_10, \exp(g, a_10)) = (idB, \exp(g, rB_1), \exp(g, a_10))$ g,a_10)) {33} event acceptsA(exp(g,a_3),exp(g,b_3),(idA, exp(g,rA_1),exp(g,x_1))) {35} event termA(exp(g,a_3),exp(g,b_3),(idB,exp(g,rB_1),exp(g,a_10)),h2_con(exp(exp(g,eadd(a_10,eadd(rB_1,emul(s_1,h1(idB,exp(g,rB_1)))))),eadd(eadd(rA_1,emul(h1(idA,exp(g,rA_1)),s_1)),x_1)), exp(exp(g,a_10),x_1))) ~M 12 {37} event Send(exp(g,a_3),exp(g,b_3),secretA) $(\sim M_1, \sim M) = (\exp(g,b_3), \exp(g,a_3))$ $(idA, \sim M_4, exp(g, a_12)) = (idA, exp(g, rA_1), exp(g, rA_1)) = (idA, exp(g, rA_1), exp(g, rA_1)) = (idA, exp(g, rA_1), exp(g, rA_1), exp(g, rA_1)) = (idA, exp(g, rA_1), exp(g, rA_1$ g,a_12)) [{49} new y_2 $(\sim M_13, \sim M_14, \sim M_15) = (idB, exp(g, rB_1), exp(g, y_2))$ {57} event acceptsB(exp(g,a_3),exp(g,b_3),(idB, exp(g,rB_1),exp(g,y_2)),h2_con(exp(exp(g,eadd(a_12,eadd(rA_1,emul(s_1,h1(idA,exp(g,rA_1))))), eadd(eadd(rB_1,emul(h1(idB,exp(g,rB_1)),s_1)), y_2)),exp(exp(g,a_12),y_2)))

Abbreviations

 \sim M_12 = senc(secretA,h2_con(exp(exp(g,eadd(a_10,