$\sim X_1 = \text{encrypt(nonce_to_bitstring(1-proj-nonce_to_bitstring())}$ decrypt(~M_14006,a_13534))),~M_13674) nonce_to_bitstring(Nb_13546),pk(skB_13544)) **Honest Process** Attacker {1}new skA_13545 \sim M_13619 = pk(skA_13545) {4} insert keys(A,pk(skA_13545)) {5}new skB_13544 \sim M_13674 = pk(skB_13544) {8} insert keys(B,pk(skB_13544)) {9}new skS_13542 \sim M_13728 = spk(skS_13542) Beginning of process processInitiator(spk(skS_13542), skA_13545, skB_13544) Beginning of process processResponder(spk(skS_13542), skA_13545, skB_13544) Beginning of process processS(skS_13542) Beginning of process processS(skS_13542) Beginning of process processK $(B,a_1|3535)$ {36} event beginBparam(B,a_13535) $(\sim M_13847, \sim M_13848) = (B,a_13535)$ (a_13537,B) {130} get keys(B,pk(skB_13544)) \sim M_13930 = sign((pk(skB_13544),B),skS_13542) (a_13540,a_13535) (a_13535,pk(a_13534)) [{134} insert keys(a_13535,pk(a_13534)) {130} get keys(a_13535,pk(a_13534)) \sim M_13957 = sign((pk(a_13534),a_13535),skS_13542) \sim M_13957 = sign((pk(a_13534),a_13535),skS_13542) {40} new Na_13543 \sim M_13968 = encrypt((Na_13543,B),pk(a_13534)) encrypt((1-proj-nonce-host-tuple(decrypt(~M_13968, a_13534)),B),~M_13619) = encrypt((Na_13543,B), pk(skA_13545)) [77] event beginAparam(B,A) $(\sim M_13986, \sim M_13987) = (A,B)$ \sim M_13930 = sign((pk(skB_13544),B),skS_13542) {81}new Nb_13546 {82} event beginAfull(B,A,pk(skA_13545),pk(skB_13544), Na_13543,Nb_13546) \sim M_13999 = encrypt((Na_13543,Nb_13546),pk(skB_13544)) \sim M_13999 = encrypt((Na_13543,Nb_13546),pk(skB_13544)) {44} event beginBfull(B,a_13535,pk(a_13534),pk(skB_13544),Na_13543,Nb_13546) ~M_14006 = encrypt(nonce_to_bitstring(Nb_13546), pk(a_13534)) ~X 1 {87} event endBparam(B,A)

Abbreviations

A trace has been found.