Abbreviations \sim X_1 = (a_4,discoveredParticipant,participant_data(\sim M_12, ~M_4,~M_15,discoveryRegister)) = (a 4,discoveredParticipant, participant_data(GUIDA_4,Topic_bd_4,QoSA_2,discoveryRegister)) ~M_22 = sign_cert(GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI) ~M 23 = sign perm(GUIDA 4,DGA 1,PPA 1,SK Perm) \sim M 24 = GUIDA 4 \sim M_25 = Topic_bd_4 \sim M 26 = QoSA 2 \sim M 27 = discoveryRegister \sim M 28 = ID G \sim M 29 = DH RSA \sim M 30 = SHA256 ~M_31 = hash(SHA256,Clist2bit(make_C_list(sign_cert(GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI),sign_perm(GUIDA_4, DGA_1,PPA_1,SK_Perm),participant_data(GUIDA_4, Topic_bd_4,QoSA_2,discoveryRegister),make_algo(ID G,DH RSA),SHA256))) \sim M 32 = ChallengeA 5 \sim M_33 = dh_pub(ID_G,dh_k(s_5)) \sim X 2 = (make C list(\sim M 22,a 5,a 6,make algo(ID G,DH RSA), SHA256),hash(SHA256,Clist2bit(make C list(~M 22, a 5,a 6,make algo(ID G,DH RSA),SHA256))),a 7,a 8) (make C list(sign cert(GUIDA 4,pk(PrivKA 1), SN_CI,SK_CI),a_5,a_6,make_algo(ID_G,DH_RSA),SHA256), hash(SHA256,Clist2bit(make C list(sign cert(GUIDA 4, pk(PrivKA_1),SN_CI,SK_CI),a_5,a_6,make_algo(ID_G, DH RSA),SHA256))),a 7,a 8) \sim X_3 = (make_C_list(\sim M_34, \sim M_35,participant_data(\sim M_36, ~M 37,~M 38,~M 39),make algo(~M 40,~M 41),~M 42), \sim M_43, \sim M_44, \sim M_45, \sim M_46, \sim M_47, \sim M_48, \sim M_49) make C list(sign cert(GUIDB 4,pk(PrivKB 1),SN CI, SK_CI),sign_perm(GUIDB_4,DGB_2,PPB_2,SK_Perm), participant_data(GUIDB_4,Topic_bd_4,QosB_3,discoveryRegister), make algo(ID G,DH RSA),SHA256),hash(SHA256,Clist2bit(make_C_list(sign_cert(GUIDB_4,pk(PrivKB_1),SN_CI, SK CI), sign perm(GUIDB 4,DGB 2,PPB 2,SK Perm), participant_data(GUIDB_4,Topic_bd_4,QosB_3,discoveryRegister), make algo(ID G,DH RSA),SHA256))),a 7,ChallengeB 4, dh pub(ID G,dh k(s 6)),hash(SHA256,Clist2bit(make C list(sign_cert(GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI),a_5, a 6,make algo(ID G,DH RSA),SHA256))),a 8,sign(PrivKB 1,(hash(SHA256,Clist2bit(make C list(sign cert(GUIDB_4,pk(PrivKB_1),SN_CI,SK_CI),sign_perm(GUIDB_4, DGB_2,PPB_2,SK_Perm),participant_data(GUIDB_4, Topic bd 4,QosB 3,discoveryRegister),make algo(ID_G,DH_RSA),SHA256))),ChallengeB_4,dh_pub(ID_G, dh k(s 6)),a 7,a 8,hash(SHA256,Clist2bit(make C list(sign_cert(GUIDA_4,pk(PrivKA_1),SN_CI,SK_CI),a_5, a 6,make algo(ID G,DH RSA),SHA256)))))) $\sim X_4 = (make_C_list(\sim M_34,a_9,a_10,make_algo(ID_G,DH_RSA),$ SHA256),hash(SHA256,Clist2bit(make C list(~M 34, a_9,a_10,make_algo(ID_G,DH_RSA),SHA256))),a_11, a_12)

= (make_C_list(sign_cert(GUIDB_4,pk(PrivKB_1), SN CI,SK CI),a 9,a 10,make algo(ID G,DH RSA),SHA256), hash(SHA256,Clist2bit(make_C_list(sign_cert(GUIDB_4, pk(PrivKB 1),SN CI,SK CI),a 9,a 10,make algo(ID G, DH RSA),SHA256))),a 11,a 12) Honest Process Attacker \sim M = pk(SK CI) \sim M 1 = pk(SK Perm) {5}new Topic_bd_4 {6}new GUIDA_4 {73}new GUIDB_4 {7}new PrivKA_1 {74}new PrivKB_1 {78}new DGB_2 {11}new DGA_1 {12}new PPA_1 {79}new PPB_2 {13}new QoSA_2 {80}new QosB_3 Beginning of process ParticipantB Beginning of process ParticipantB {94} event B_discover(participant_data(GUIDB_4, Topic_bd_4,QosB_3,discoveryRegister)) {94} event B_discover(participant_data(GUIDB_4, Topic_bd_4,QosB_3,discoveryRegister)) (~M_2,participant_data(~M_3,~M_4,~M_5,~M_6)) = (GUIDB_4,participant_data(GUIDB_4,Topic_bd_4,QosB_3, discoveryRegister)) $(\sim M_7, participant_data(\sim M_8, \sim M_9, \sim M_10, \sim M_11))$ = (GUIDB_4,participant_data(GUIDB_4,Topic_bd_4, QosB 3, discoveryRegister)) Beginning of process ParticipantA Beginning of process ParticipantA $(\M_12, participant_data(\M_13,\M_14,\M_15,\M_16))$ = (GUIDA_4,participant_data(GUIDA_4,Topic_bd_4), QoSA 2, discoveryRegister)) (~M_17,participant_data(~M_18,~M_19,~M_20,~M_21)) = (GUIDA_4,participant_data(GUIDA_4,Topic_bd_4, QoSA 2, discoveryRegister)) ~X 1 {29} event A_discover(a_4) {31}new ChallengeA 5 {32}new s_5 {37} event A_0(GUIDA_4,make_C_list(sign_cert(GUIDA_4, pk(PrivKA_1),SN_CI,SK_CI),sign_perm(GUIDA_4,DGA_1,PPA_1,SK_Perm),participant_data(GUIDA_4,Topic_bd_4, QoSA_2,discoveryRegister),make_algo(ID_G,DH_RSA), SHA256), Challenge A_5, dh_pub (ID_G, dh_k(s_5)), a_4) (make_C_list(~M_22,~M_23,participant_data(~M_24, ~M 25,~M 26,~M 27),make algo(~M 28,~M 29),~M 30), ~M 31,~M 32,~M 33) ~X 2 {101}new ChallengeB 4 {102}new s 6 {108} event beginAtoB(GUIDB_4, sign_cert(GUIDB_4, pk(PrivKB 1),SN CI,SK CI),a 7) {109}event B_0(GUIDB_4,make_C_list(sign_cert(GUIDB_4, pk(PrivKB_1),SN_CI,SK_CI),sign_perm(GUIDB_4,DGB_2, PPB 2,SK Perm), participant data (GUIDB 4, Topic bd 4, QosB_3,discoveryRegister),make_algo(ID_G,DH_RSA), SHA256), ChallengeB_4, dh_pub(ID_G, dh_k(s_6)), GUIDA_4, make C list(sign cert(GUIDA 4,pk(PrivKA 1),SN CI, SK_CI),a_5,a_6,make_algo(ID_G,DH_RSA),SHA256), a 7,a 8) ~X 3 {101}new ChallengeB 5 {102}**new** s_7 {108} event beginAtoB(GUIDB_4, sign_cert(GUIDB_4, pk(PrivKB 1),SN CI,SK CI),a 11)

{109} event B_0(GUIDB_4, make_C_list(sign_cert(GUIDB_4,

pk(PrivKB_1),SN_CI,SK_CI),sign_perm(GUIDB_4,DGB_2, PPB_2,SK_Perm),participant_data(GUIDB_4,Topic_bd_4,

QosB_3,discoveryRegister),make_algo(ID_G,DH_RSA), SHA256),ChallengeB_5,dh_pub(ID_G,dh_k(s_7)),GUIDB_4, make_C_list(sign_cert(GUIDB_4,pk(PrivKB_1),SN_CI,

SK_CI),a_9,a_10,make_algo(ID_G,DH_RSA),SHA256),

a 11,a 12)

A trace has been found.