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 = (a 5, discoveredParticipant, participant data( $\sim$ M 7, ~M 4,~M 10,discoveryRegister)) = (a 5, discovered Participant, participant\_data(GUIDA\_4,Topic\_bd\_4,QoSA\_2,discoveryRegister)) ~M\_34 = sign\_cert(GUIDA\_4,pk(PrivKA\_1),SN\_CI,SK\_CI) ~M 35 = sign perm(GUIDA 4,DGA 1,PPA 1,SK Perm) A trace  $\sim$ M 36 = GUIDA 4 has been found.  $\sim$ M 37 = Topic bd 4  $\sim$ M 38 = QoSA\_2  $\sim$ M 39 = discoveryRegister  $\sim$ M 40 = ID G  $\sim$ M 41 = DH RSA  $\sim$ M 42 = SHA256 ~M 43 = 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 44 = ChallengeA 6  $\sim$ M\_45 = dh\_pub(ID\_G,dh\_k(s\_6))  $\sim$ X\_3 = (make\_C\_list( $\sim$ M\_22, $\sim$ M\_23,participant\_data( $\sim$ M\_7, ~M\_4,~M\_10,discoveryRegister),make\_algo(ID\_G,DH\_RSA), SHA256),hash(SHA256,Clist2bit(make C list(~M 22, ~M 23,participant\_data(~M\_7,~M\_4,~M\_10,discoveryRegister), make algo(ID G,DH RSA),SHA256))),~M 44,~M 45) (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),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))),ChallengeA 6, dh pub(ID G,dh k(s 6))) **Honest Process** Attacker  $\sim$ M = pk(SK CI)  $\sim$ M 1 = pk(SK Perm) {5}new GUIDA\_4 {6}new PrivKA\_1 {10}new DGA\_1 {11}new PPA\_1 {12}new QoSA\_2 {18}new GUIDB\_4 {19}new PrivKB 1 {23}new DGB\_2 {24}new PPB\_2 {25}new QosB\_3 {31}new Topic\_bd\_4 Beginning of process ParticipantB {94} event B\_discover(participant\_data(GUIDB\_4, Topic\_bd\_4,QosB\_3,discoveryRegister))  $(\sim M_2, participant_data(\sim M_3, \sim M_4, \sim M_5, \sim M_6)) =$ (GUIDB\_4,participant\_data(GUIDB\_4,Topic\_bd\_4,QosB\_3, discoveryRegister)) Beginning of process ParticipantA Beginning of process ParticipantA Beginning of process ParticipantA (~M\_7,participant\_data(~M\_8,~M\_9,~M\_10,~M\_11)) = (GUIDA\_4,participant\_data(GUIDA\_4,Topic\_bd\_4, QoSA 2, discoveryRegister))  $(\sim M_12, participant_data(\sim M_13, \sim M_14, \sim M_15, \sim M_16))$ = (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 {42} event A\_discover(a\_4) {44}new ChallengeA 5 {45}new s 5 {50} 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, discovery Register), 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 {42} event A\_discover(a\_5) {44}new ChallengeA 6  $\{45\}$  new s 6 {50} 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, discovery Register), make algo (ID G, DH RSA), SHA256), Challenge A 6, dh pub (ID G, dh k(s 6)), a 5) (make\_C\_list(~M\_34,~M\_35,participant\_data(~M\_36, ~M\_37,~M\_38,~M\_39),make\_algo(~M\_40,~M\_41),~M\_42),  $\sim$ M 4 $\beta$ , $\sim$ M 44, $\sim$ M 45) ~X 3 {101}new ChallengeB 3 {102}new s 7 {108} event beginAtoB(GUIDB\_4, sign\_cert(GUIDB\_4, pk(PrivKB 1),SN CI,SK CI),ChallengeA 6) {109} event B\_0(GUIDB\_4,make\_C\_list(sign\_cert(GUIDB\_4, pk(PrivKB\_1),SN\_CI,SK\_CI),sign\_perm(ĞUIDB\_4,DGB\_2, PPB\_2,SK\_Perm),participant\_data(GUIDB\_4,Topic\_bd\_4, QosB 3, discovery Register), make algo (ID G, DH RSA), SHA256), ChallengeB \_3, dh \_pub(ID \_G, dh \_k(s \_7)), 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, discovery Register), make\_algo(ID\_G,DH\_RSA),SHA256),ChallengeA\_6,dh\_pub(  $\overline{ID}$  G,dh k(s 6)))

Abbreviations

 $\sim X_1 = (a_4, discoveredParticipant, participant_data(\sim M_7,$ 

~M\_4,~M\_10,discoveryRegister))

= (a 4,discoveredParticipant,