$\sim X_1 = (dummyVotePair(commitValue(dummyRandomNumber1_1,$ rand1rand1_1),commitValue(candidate0,rand1Candidate1_1)), dummyVotePair(commitValue(dummyRandomNumber2_1, rand2rand2_1),commitValue(candidate1,rand2Candidate2_1)), pzk1(candidate0,candidate1,rand1Candidate1_1,rand2Candidate2_1, commitValue(candidate0,rand1Candidate1_1),commitValue(candidate1,rand2Candidate2_1)),sessionidv_3) A trace has been found. ~M_5 = dummyVotePair(commitValue(dummyRandomNumber1_1, rand1rand1_1),commitValue(candidate0,rand1Candidate1_1)) \sim M_6 = dummyVotePair(commitValue(dummyRandomNumber2_1, rand2rand2_1),commitValue(candidate1,rand2Candidate2_1)) \sim M_7 = pzk1(candidate0,candidate1,rand1Candidate1_1, rand2Candidate2_1,commitValue(candidate0,rand1Candidate1_1), commitValue(candidate1,rand2Candidate2_1)) \sim M_8 = sessionidv_3 **Honest Process** Attacker {2}new vmsecretkey_1 ~M = signedPublicKey(vmsecretkey_1) {5}new trgsecretkey_1 \sim M_1 = signedPublicKey(trgsecretkey_1) {8}new bbsecretkey_1 \sim M_2 = signedPublicKey(bbsecretkey_1) {11}new vsecretkey_1 \sim M_3 = signedPublicKey(vsecretkey_1) {14}new channelvoterandva_1 {15}new channelvoterandtrg_1 {16}new channeltrgandmachine_1 {17}new channelvaprep_1 {18}new channelvareceipts_1 {19}new channeltrgandtest_1 {20}new channelvoterandtest_1 {21}new channelBBandTest_1 {22}new channelVAandTest_2 {24}new sessionidv_3 \sim M_4 = sessionidv_3 Beginning of process VotingAuthority {33}new rand1rand1_1 {34}new rand1Candidate1_1 Beginning of process TRG Beginning of process Voter Beginning of process Bulletin Beginning of process test {35}new rand2rand2_1 [91] event VoterChoice(candidate0,sessionidv_3) {80}new freshRandomNumber_4 {36}new rand2Candidate2_1 {37}new dummyRandomNumber1_1 {38}new dummyRandomNumber2_1 $(a_2,a_3,a_4,\sim M_4) = (a_2,a_3,a_4,sessionidv_3)$ ~X_1 $(\sim M_5, \sim M_6, \sim M_7, + M_8)$ sign((candidate0,sessionidv_3),vsecretkey_1) sign((freshRandomNumber_4,sessionidv_3),trgsecretkey_1) freshRandomNumber_4 {53}new barCode_1 sign((freshRandomNumber_4,sessionidv_3),trgsecretkey_1) \sim M_9 = freshRandomNumber_4 sign((candidate0,candidate1,freshRandomNumber_4, dummyRandomNumber2_1,barCode_1,sessionidv_3),vmsecretkey_1) {101}event OKv(freshRandomNumber_4,candidate0, sessionidv_3)

Abbreviations