

| Abbreviations |
|--|
| $\sim X_1 = (\text{dummyVotePair}(\text{commitValue}(\text{dummyRandomNumber1_1}, \text{rand1rand1_1}), \text{commitValue}(\text{candidate0}, \text{rand1Candidate1_1})), \text{dummyVotePair}(\text{commitValue}(\text{dummyRandomNumber2_1}, \text{rand2rand2_1}), \text{commitValue}(\text{candidate1}, \text{rand2Candidate2_1})), \text{pzk1}(\text{candidate0}, \text{candidate1}, \text{rand1Candidate1_1}, \text{rand2Candidate2_1}), \text{commitValue}(\text{candidate0}, \text{rand1Candidate1_1}), \text{commitValue}(\text{candidate1}, \text{rand2Candidate2_1})), \text{sessionidv_3})$ |
| $\sim M_5 = \text{dummyVotePair}(\text{commitValue}(\text{dummyRandomNumber1_1}, \text{rand1rand1_1}), \text{commitValue}(\text{candidate0}, \text{rand1Candidate1_1}))$ |
| $\sim M_6 = \text{dummyVotePair}(\text{commitValue}(\text{dummyRandomNumber2_1}, \text{rand2rand2_1}), \text{commitValue}(\text{candidate1}, \text{rand2Candidate2_1}))$ |
| $\sim M_7 = \text{pzk1}(\text{candidate0}, \text{candidate1}, \text{rand1Candidate1_1}, \text{rand2Candidate2_1}, \text{commitValue}(\text{candidate0}, \text{rand1Candidate1_1}), \text{commitValue}(\text{candidate1}, \text{rand2Candidate2_1}))$ |
| $\sim M_8 = \text{sessionidv_3}$ |
| $\sim X_2 = (\text{candidate0}, \text{sign}((\text{candidate0}, \text{candidate1}, \text{freshRandomNumber_4}, \text{dummyRandomNumber2_1}, \text{barCode_1}, \text{sessionidv_3}), \text{vmsecretkey_1}), \text{sessionidv_3})$ |

A trace has been found.

