LELEC2770 – Practical Sessions

Practical Session 3: Verifiable Voting

1. Consider a yes/no election with 5 candidates. The elector must select 3 candidates among the 5. Design the ballot and a sigma protocol that makes the ballot verifiable.

2. Prove the completeness, the soundness and the honest verifier zero-knowledge properties of the previous sigma protocol (apart from the disjunctive proofs).

3. Follow the link `https://lelec2770.pythonanywhere.com/elections1#`.

   Your goal is

   (a) to find the result of the election and,

   (b) to unveil the choice of the first voter.

   The file `votes1.json` represents the public bulletin board. You have access to a decryption oracle but you cannot query it on the ciphertexts of `votes1.json`.

4. Follow the link `https://lelec2770.pythonanywhere.com/elections2#`.

   You are in charge of the elections where 1000 electors must choose between three candidates. As before, you have access to a decryption oracle but you cannot query it on the ciphertexts of `votes2.json`. Announce the result of the election in the appropriate field. Hint: use the file `utils.py` to help you.

5. Turn the interactive proof of the sigma protocol of exercise 1 into its non-interactive version by using the Fiat-Shamir heuristic.