Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

9. Exercise sheet
Hand in solutions until Sunday, 27 June 2010, 23.59 h

Exercise 9.1 (Kiayias and Yung). (11 points)

You already encountered voting schemes introduced by Chaum (1981) and by Clarkson, Chong, and Myers (2008). In this exercise you will encounter a third one, introduced by Kiayas & Yung (2002). Read

Aggelos Kiayias and Moti Yung, *Self-tallying elections and perfect ballot secrecy*, PKC '02, p. 141–158, Springer-Verlag, 2002.

(i) Classify the scheme (hidden vote/hidden voter/both). $\boxed{1}$

(ii) Summarize the four steps $\boxed{4}$

- Registration,
- Pre-voting,
- Voting, and
- Tallying

each with one sentence.

(iii) Check the scheme for the familiar points $\boxed{6}$

- Eligibility,
- Anonymity,
- Individual verifiability,
- Global verifiability,
- Receipts, and
- Robustness.

Comment quickly on your decision.

Exercise 9.2 (ElGamal Encryption). (6 points)

Consider ElGamal encryption in a cyclic additive group G of order q with generator P. Let (P, X) denote the public key and (T, Y) the ciphertext. Prove that BREAKING ELGAMAL, in the sense of recovering the plaintext from the ciphertext, is equivalent to the COMPUTATIONAL DIFFIE-HELLMAN problem. $\boxed{6}$

Exercise 9.3 (dudle). (13 points)

Having public polls and scheduling parties are processed similar to elections. A common tool for this is `http://www.doodle.com/`. A project at TU Dresden aims at generating a "privacy-enhanced" version of doodle, see `http://dudle.inf.tu-dresden.de/`.

$\boxed{3}$ (i) Find the documentation and name the problems they addressing.

$\boxed{6}$ (ii) There are four steps in the scheme. Name them and present their content in pseudo-code.

$\boxed{4}$ (iii) Comment on the designer's claims concerning

- verifiability,
- privacy,
- usability, and
- computational complexity.