Esecurity: secure internet & e-voting, summer 2013

MICHAEL NÜSKEN

13. Exercise sheet
Hand in solutions until Monday, 15 July 2013, 08:00

Exercise 13.1 (KnowDlog). (3 points)

Write down the proofs that the KNOWDLOG argument, as presented in the lecture, satisfies 3

- *completeness*,
- *soundness*,
- *zero-knowledge*.

Exercise 13.2 (Distributed key generation). (4 points)

Consider DISTRIBUTED KEY GENERATION and DISTRIBUTED DECRYPTION as presented in the lecture. Show that a malicious key holder can not learn the keys of his fellows. 4

Hint: Use the fact that KNOWDLOG and EQDLOGS are *zero-knowledge*.

Exercise 13.3 (DDH and CDH for EqDlogs). (12 points)

In the light of the Decisional Diffie-Hellmann Problem (DDH) and the computational Diffie-Hellmann-Problem (CDH) we distinguish three different types of groups:

Hard: Groups where DDH and CDH are hard.

Gap-DH: Groups where DDH is easy, but CDH is hard.

Easy: Groups where DDH and CDH are easy.

(i) Show that every group belongs to one of the three named classes. 2

(ii) Investigate the three properties of zero-knowledge protocols for EqDlogs on groups from the three classes. 6

Let us take a look at elliptic curves. A pairing on an elliptic curve E into a field F is a map $e(\cdot,\cdot)\colon E \times E \to F^\times$ satisfying the two properties:

bilinearity $e(aP, bQ) = e(P, Q)^{ab}$ for all points $P, Q \in E$ and integers $a, b \in \mathbb{Z}$.

non-degeneracy $e(P, P) \neq 1$ for all points $P \in E$.

4 (iii) To which of the three mentioned classes belong elliptic curves with an efficiently computable pairing?

Exercise 13.4 (dudle). (0+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/`.

+3 (i) Find the documentation and name the problems they addressing.

+6 (ii) There are four steps in the scheme. Name them and present their content in pseudo-code.

+4 (iii) Comment on the designer's claims concerning

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