Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

10. Exercise sheet
Hand in solutions until Sunday, 4 July 2010, 23.59 h

Exercise 10.1 (Fiat-Shamir protocol). (9 points)

We investigate a popular zero-knowledge protocol in a simplified form, where the challenge consists of only a single bit. $\boxed{9}$

Let n be an RSA integer, $s \in \mathbb{Z}_n^\times$ the secret of P and $v = s^2 \mod n$.

Protocol. Interactive zero-knowledge proof for squareness modulo a composite.
Principals: Prover P and Verifier V
Public input: n, v
Private input to the prover: s

1. Commitment: P chooses a random $r \in \mathbb{Z}_n$ and sends $x = r^2$ to V. $\xrightarrow{\quad x \quad}$
2. Challenge: V selects randomly $e \in \{0, 1\}$ and sends it to P. $\xleftarrow{\quad e \quad}$
3. Response: P sends $y = r \cdot s^e$ to V. $\xrightarrow{\quad y \quad}$
4. Verification: V verifies $y^2 = x \cdot v^e$.

Investigate the three properties completeness, soundness, and zero-knowledge for this protocol.

Exercise 10.2 (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. $\boxed{2}$

(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?