Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

11. Exercise sheet
Hand in solutions until Sunday, 11 July 2010, 23.59 h

Exercise 11.1 (Proof of Knowledge for EqDlogs). (4 points)

Prove that EQDLOGS, as used in the lecture, has the property *Proof of Knowledge*. $\boxed{4}$

Exercise 11.2 (KnowDlog). (3 points)

Write down the proofs that the KNOWDLOG argument, as presented in the lecture, satisfies $\boxed{3}$

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

Exercise 11.3 (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. $\boxed{4}$

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