Esecurity: secure internet & e-voting, summer 2013

MICHAEL NÜSKEN

11. Exercise sheet
Hand in solutions until Monday, 1 July 2013, 08:00

Exercise 11.1 (Zero-Knowledge). (10 points)

Read Quisquater, Quisquater, Quisquater, Quisquater, Guillou, Guillou, Guillou, Guillou, Guillou (1989) to one of your children. Alternatively take one of your fellow students.

(i) Write down the protocol in a form appropriate for computer science students rather than for children. [4]

(ii) Prove for this protocol the following three properties: [6]

- If the prover's claim is true, the verification returns true — always.
- If the prover's claim is false, the verification fails — with high probability.
- The verifier does not learn anything about the private information.

Exercise 11.2 (Kiayias and Yung). (11 points)

In this exercise you will encounter a further voting scheme introduced by Kiayias & Yung (2002). Read that paper.

(i) Classify the scheme (hidden vote/hidden voter/both). [1]

(ii) Summarize the four steps [4]

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

each with one sentence.

(iii) Check the scheme for the familiar points [6]

- Eligibility,

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

Comment quickly on your decision.

Exercise 11.3 (Voting). (11 points)

Two fundamental steps in voting are

election process getting the voters' opinion (assuming they have one),

tallying process transforming the voters' opinion into a final result.

The party pooper for the second point is ARROW's theorem. In this lecture we deal with the first point. The bad news here is reality. The US Presidential Election in 2000 had several problem's with the first step.

3 (i) List three of these problems as precisely as possible (give your sources).

4 (ii) Has something similar happened in Germany or in your home country (take your state, if you are German)?

4 (iii) Derive general principles for the election process.

References

AGGELOS KIAYIAS & MOTI YUNG (2002). Self-tallying elections and perfect ballot secrecy. In *Public Key Cryptography*, D. NACCACHE & P. PAILLIER, editors, volume 2274 of *Lecture Notes in Computer Science*, 141–158. Springer-Verlag, Berlin, Heidelberg. ISBN 3-540-43168-3. ISSN 0302-9743. URL http://dx.doi.org/10.1007/3-540-45664-3_10. Also available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.126.6288.

JEAN-JACQUES QUISQUATER, MYRIAM QUISQUATER, MURIEL QUISQUATER, MICHAËL QUISQUATER, LOUIS GUILLOU, MARIE ANNICK GUILLOU, GAÏD GUILLOU, ANNA GUILLOU, GWENDOLÉ GUILLOU, SOAZIG GUILLOU & TOM BERSON (1989). How to Explain Zero-Knowlegde Protocols to Your Children. In *Advances in Cryptology: Proceedings of CRYPTO '89*, Santa Barbara, CA, number 435 in Lecture Notes in Computer Science, 628–631. Springer-Verlag. ISSN 0302-9743. URL http://dx.doi.org/10.1007/0-387-34805-0_60.