Advanced Cryptography: Lightweight Cryptography

Michael Nüsken, Daniel Loebenberger

10. Exercise sheet
Hand in solutions until Monday, 23 January 2012, 23:59:59.

If you find any errors in the sheets, do not hesitate to write an email to the mailing list `11ws-ac@lists.bit.uni-bonn.de`.

Exercise 10.1 (Zero-Knowledge). (10 points)

Read

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`

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. $\boxed{4}$

(ii) Prove for this protocol the following three properties. $\boxed{6}$

Completeness/correctness If the prover's claim is true, the verification always returns true.

Soundness If the prover's claim is false, the verification fails with high probability.

Zero-knowledge The verifier does not learn anything about the private information. In other words, whatever a malicious verifier can compute after a conversation he could also compute without a conversation. The latter may be based on a simulated conversation.

Mind that all algorithms and entities are considered to be polynomial-time bounded.

Exercise 10.2 (Key sizes). (5 points)

On the website `http://www.keylength.com/` you find various methods for extrapolating the security level for public key sizes. Select two of them and throughly compare the two estimates. Decide which one you would follow. Why are all recommendations time-dependent? $\boxed{5}$

Exercise 10.3 (Symmetric vs. asymmetric ciphers). (10+5 points)

$\boxed{10+5}$ We will now compare PRESENT-80 with ElGamal encryption over the multiplicative group of a finite field $\mathbb{F}_p$ with prime p, using the security parameters that you decided on in the last exercise.

(i) Estimate how many runs of PRESENT-80 encryptions you can do within one ElGamal encryption.

(ii) Verify your estimate experimentally! Implement ElGamal in the same programming language as your PRESENT-80 code and perform precise runtime estimates for PRESENT-80 and ElGamal. What do you observe?

Exercise 10.4 (Gate equivalence). (5 points)

$\boxed{5}$ Try to figure out how many ASIC gates roughly correspond to one FPGA gate. Note that this question is somewhat ill stated. Why?