# Heads and tails, summer 2015

PROF. DR. JOACHIM VON ZUR GATHEN AND DR. DANIEL LOEBENBERGER

## 7. Exercise sheet
## Hand in solutions until Sunday, 07 June 2015, 23:59:59

**Exercise 7.1** (Small Blum-Blum-Shub generator). (7 points)

(i) Determine $\square_7, \boxtimes_7, \square_{11}, \boxtimes_{11}, \square_{77}$, and $\boxtimes_{77}$. [4]

(ii) Draw a graph of the squaring map in $\mathbb{Z}_{77}$ for the arguments in $\square_{77} \cup \boxtimes_{77}$ as done in the lecture. [3]

The following tasks does not have a strict deadline.

**Exercise 7.2** (Analyzing the generators discussed, contd.). (15 points)

Continue with your comparative analysis of the different pseudorandom generators from Exercise 6.1. In particular, perform a thorough quality check of your implementations: [15]

- Are the algorithms implemented efficiently?
- Are they correct?
- Do they run properly?

Furthermore, check the follwoing:

- Are the timings reasonable?
- Are the results comparable?
- Which further results would you like to see?

**Exercise 7.3** (Creating a (short) research article). *As communicated on the mailing list, there is the Crypto-Day on July 9 & 10 at Infineon Technologies AG in Munich approaching. The idea of this "exercise" is to submit your findings from Exercise 6.1 and 7.2 to this event. Deadline for submission is 15 June 2015 and you would have to create a one DIN A4 paged abstract until then to do so.*

*For details see*

`http://goo.gl/NuKc5B`

*Of course, there would be some more work to do afterwards:*

- *Your results have to be assembled in a (short, but nice and error-free) LaTeX-document. This technical report will then be published in the proceedings of Crypto-Day.*
- *There is a twenty minute talk to be created until July.*
- *Someone of you has to travel to Munich, stay one night and give the talk there.*

*For active participation in this adventure, an arbitrary number of bonus point is awarded.*