Heads and tails, summer 2015

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

10. Exercise sheet
Hand in solutions until Sunday, 28 June 2015, 23:59:59

Exercise 10.1 (Digging into the proof). (6 points)

In the lecture we omitted the proofs of several smallish facts. Your task is to fill those gaps.

(i) Prove that if $w_{t,i} \neq w'_{t,i}$ then $((2i+1)[a_t x]_N + [bx]_N)/N$ has distance at most $|\Delta_{t,i}|$ from an integer. Conclude that $\frac{1}{N}[c_{t,i}x]_N \leq |\Delta_{t,i}|$. 3

(ii) Prove that the values $c_{t,i}$ are pairwise independent if a_t and b are independent. 3

The following Exercise does not have the strict deadline on 26 June 2015.

Exercise 10.2 (Assembling the results). (15 points)

Goal of this exercise is now to finish the research article on the comparative analysis of cryptographic pseudorandom generators. 15

(i) Write a short piece of text describing the parameter choices of the generator you implemented.

(ii) Put the results of Exercise 9.2 in context of each other.

(iii) Compare with your previous results from Exercise 6.1 and 7.2.

The whole task should result in a (short, but self-contained) article, which is going to be published in the proceedings of Crypto-Day 2015 in Munich.