Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

8. Exercise sheet
Hand in solutions until Monday, 09 December 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 8.1 (Chasing s-boxes, cont.). (0+20 points)

Pursue s-box finding further! We want complete Poschmann conditions (incl. most of Coppersmith's). Try to optimize the heuristic used in the traversal of the backtrack-tree by using new definitions for the penalty-function used in the backtracker. We supplied you with the up-to-date sources for the finder on our webpage. Document thoroughly what we have done so far and which optimizations you propose in the style of a research paper. +20

Exercise 8.2 (Algebraic attacks on PRESENT). (0+20 points)

Set-up a system of equations that represent whole PRESENT-80. Reduce your system of equations to obtain a (larger) system with degree-two equations only. Perform experiments! Can you break in this way reduced variants of PRESENT? Hint: You need a powerful computer algebra-system for this task and some knowledge on so-called Gröbner-bases. +20

Exercise 8.3 (Attacks on eStream ciphers). (0+20 points)

On the web-page `http://www.ecrypt.eu.org/stream/finallist.html` you find four Profile 2 ciphers that can be implemented in hardware. Do research on either F-FCSR v2, Grain v1, or MICKEY v2! Find out which kind of attacks exists and report your findings. +20