

Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

6. Exercise sheet

Hand in solutions until Monday, 12 December 2011, 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 6.1 (Experimental cryptography: Chasing S-boxes). (20+20 points)

On the course webpage you find a ANSIC program that supplies you with data structures and helper routines for searching S-boxes that fulfill Coppersmith's and Poschmann's conditions. There are, however, three algorithms missing. Your task is to implement them and do some further experiments.

- (i) Implement the routines that incrementally update differential tables and bias tables. 3

- (ii) Realize the backtracker and find an S-box mapping 4 input bits to 4 output bits that fulfills Poschmann's conditions (which are implicitly specified by the functions `maxdiffstab` and `maxlintab`). To debug your backtracker it might be of big help to start with an example S-box having all the desired properties, throwing away some assignments the S-box makes and look whether your backtracker can reconstruct the S-box.
Hint: Once you have a fully specified S-box, do not forget to check whether the requirements on the bias are fulfilled. 15

- (iii) Modify the `maxdiffstab` procedure such that only S-boxes that are permutations are returned. 2
Hint: Express the property of being a permutation in terms of upper bounds on entries in the differential table.

- (iv) Find a 6-bit to 4-bit S-box that fulfills the Coppersmith and the Poschmann conditions (there were two mails to the course discussion list containing necessary changes). +10
Warning: Your program will run several hours before it finds an S-box.

- (v) Experiment with the `computepenalty` function. Can you find one that returns good S-boxes considerably faster? +10