6. Exercise sheet

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

Exercise 6.1 (Experimental cryptography: Chasing S-boxes). (20+20 points)

On the course webpage you find an ANSI C 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.

(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 maxdiftab 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.

(iii) Modify the maxdiftab procedure such that only S-boxes that are permutations are returned.

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).

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?