Daniel Loebenberger and Konstantin Ziegler Summer 2014

The art of cryptography: cryptanalytic world records

12. Assignment: Permutation-based cryptography

(Due: Sunday, 6 July 2014, 23^{59} CEST)

Exercise 1 (The dual of $\mathbb{F}_{2^n}$)**.** (3 points) Show that every linear Boolean function on $\mathbb{F}_{2^n}$ is of the form $x \mapsto a \star x$ for some $a \in \mathbb{F}_{2^n}$. (The vector space of these functions is called the *dual* of $\mathbb{F}_{2^n}$ and denoted ${\mathbb{F}_{2^n}}^*$.)

Exercise 2 (Independent random variables)**.** (3+2 points) Let $a, b, c \in \mathbb{F}_2^4$. What can you derive about $\mathrm{corr}_S(a+b, c)$ from $\mathrm{corr}_S(a, c)$ and $\mathrm{corr}_S(b, c)$?

[Bonus points for finding a necessary and sufficient condition for

$$\mathrm{corr}_S(a+b, c) = \mathrm{corr}_S(a, c)\,\mathrm{corr}_S(b, c).]$$

Exercise 3 (Linear cryptanalysis)**.** For this exercise, the S-box of baby-AES is replaced with the following new 4-bit S-box S'.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S'(x)$	8	4	2	1	C	6	3	D	A	5	E	7	F	B	9	0

We call the resulting cipher new baby-AES'.

(a) (2 points) Compute the correlation of the input/output-mask 0001 ‖ 1110 on S'.

(b) (4 points) The correlation table of S' is displayed below, but the first two rows are missing. Complete the table.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2	0	4	0	4	-4	0	-4	0	-4	0	4	-8	-8	-4	0	4
3	0	0	4	4	0	8	4	-4	-4	-4	0	0	4	-4	8	0
4	0	4	0	-4	0	4	0	-4	4	-8	4	0	-4	0	-4	-8
5	0	8	-4	-4	4	4	0	8	-4	4	0	0	0	0	4	-4
6	0	0	8	0	4	4	-4	4	0	0	0	8	-4	-4	-4	4
7	0	-4	-4	0	8	-4	4	0	0	-4	-4	0	-8	-4	4	0
8	0	4	4	0	0	-4	-4	0	4	0	-8	-4	4	-8	0	-4
9	0	0	0	8	4	4	-4	4	4	-4	-4	-4	0	8	0	0
A	0	8	4	4	-4	-4	8	0	0	0	-4	4	-4	4	0	0
B	0	-4	8	-4	0	-4	0	4	-8	-4	0	-4	0	4	0	-4
C	0	0	4	4	8	0	4	-4	0	8	4	-4	0	0	-4	-4
D	0	-4	0	-4	-4	8	4	0	0	4	-8	-4	-4	0	-4	0
E	0	-4	-4	8	-4	0	0	4	-4	0	0	4	0	-4	-4	-8
F	0	0	0	0	0	0	8	8	4	-4	4	-4	4	-4	-4	4

(c) (1 point) What is the maximal magnitude of correlation?

Exercise 4 (The average S-box, continued)**.** (5+3 points) For the following S-boxes on $\mathbb{F}_{16} = \mathbb{F}_2[t]/(t^4 + t + 1)$ determine the maximal magnitude of correlation.

(a) identity id,

(b) affine linear transformation $x \mapsto (t^3 + t^2 + 1) \cdot x + (t^2 + t)$,

(c) patched inverse

$$\mathrm{inv}(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} & \text{else,} \end{cases}$$

(d) baby-AES S-box,

(e) inverse of the baby-AES S-box,

(f) Pick 1 000 S-boxes at random. Draw the distribution of the maximal magnitude of correlation.