Daniel Loebenberger and Konstantin Ziegler Summer 2014

The art of cryptography: cryptanalytic world records

11. Assignment: Permutation-based cryptography

(Due: Sunday, 29 June 2014, 23^{59} CEST)

Exercise 1 (Differential cryptanalysis)**.** In the lecture, we found a differential trail through the first two rounds of baby-AES with propagation ratio 1/64. For the corresponding differential attack, we required 192 pairs of plaintext-ciphertext pairs with corresponding input difference.

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

We call the resulting cipher baby-AES'.

(a) (3 points) Compute the output difference distribution of S' for input difference $\Delta x = 0001$. [Hint: Eight xors suffice.]

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

$\Delta x \backslash \Delta y$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0																
1																
2																
3	0	2	0	4	0	2	0	0	0	2	0	4	0	2	0	0
4	0	4	2	2	0	2	0	2	2	0	0	2	0	0	0	0
5	0	0	0	4	0	0	0	4	0	0	0	0	2	2	2	2
6	0	0	0	0	2	0	2	0	2	0	2	0	2	2	2	2
7	0	0	4	2	2	0	0	0	4	2	0	0	0	0	2	0
8	0	2	0	0	2	4	2	2	0	2	0	0	0	2	0	0
9	0	6	0	0	0	0	2	0	0	0	2	4	0	2	0	0
A	0	0	2	0	0	0	0	2	4	0	4	2	0	0	2	0
B	0	0	0	0	2	2	2	2	0	0	0	0	4	0	4	0
C	0	0	2	0	0	2	4	0	2	0	0	0	2	2	2	0
D	0	0	2	2	2	0	2	0	0	2	6	0	0	0	0	0
E	0	0	2	2	0	0	0	0	2	6	0	0	0	0	0	4
F	0	0	0	0	2	4	0	2	0	2	0	2	2	2	0	0

(c) (2 points) Use a computer algebra system of your choice (for example Sage) to compute the difference distribution table for S' and check your answers for (a) and (b).

(d) (1 point) What is the maximal propagation ratio for a nonzero differential in S'?

(e) (3 points) A "differential attacker" will search for a differential trail with large propagation ratio. Use (d) to derive an upper bound for the propagation ratio of a any nonzero differential trail through the first two rounds of baby-AES'.

(f) (+2 points) Find a differential trail through the first two rounds of baby-AES' whose propagation ratio achieves the upper bound of (e).

(g) (2 points) How many pairs of plaintext-ciphertext pairs will you request for a differential attack against of baby-AES' using a trail whose propagation ratio matches the upper bound obtained in (e). [Use the same implicit constant as we used for the attack on the original baby-AES described at the beginning.]

Exercise 2 (How many samples?)**.** You visit a casino with 2^k lotteries which have a probability of winning of $1/2^\ell$ each. One of them is broken though and has a probability of winning of $p + 1/2^\ell$ with $p > 0$.

We run the following experiment to find the "lucky" machine

1. Run each lottery N times and record the number of "wins".
2. We call the set of machines with the most wins W
3. The experiment is *successful* if the "lucky" machine is an element of W, and *uniquely successful* if the "lucky" machine is the unique element of W.

Determine by experiment the answer to the following questions for $k = \ell = 8$ and $p = 1/64$.

(a) (5 points) For which size of N do you expect the experiment to be successful.

(b) (+5 points) For which size of N do you expect the experiment to be uniquely successful.

Exercise 3 (the average S-box)**.** (5 points)

For the following S-boxes on $\mathbb{F}_{16} = \mathbb{F}_2[t]/(t^4 + t + 1)$ draw the difference distribution matrix and find the maximal difference probability.

(a) identity id,

```
S = mq.SBox(0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15)    # identity
S.difference_distribution_matrix()
S.maximal_difference_probability()
```

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

(c) patched inverse

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

(d) baby-AES S-box.

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

(f) Plot the distribution of the maximal difference probability of 1 000 randomly chosen S-boxes.