Daniel Loebenberger and Konstantin Ziegler Summer 2014

The art of cryptography: cryptanalytic world records

13. Assignment: Algebraic Cryptanalysis

(Due: Sunday, 13 July 2014, 23^{59} CEST)

Exercise 1 (Independent random variables). (3+2 points) Let $a, b, c \in \mathbb{F}_2^4$. What can you derive about $\operatorname{corr}_S(a+b, c)$ from $\operatorname{corr}_S(a, c)$ and $\operatorname{corr}_S(b, c)$?

[Bonus points for finding a necessary and sufficient condition for

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

Exercise 2 (Linear cryptanalysis). In the lecture, we found a linear approximation through the first two rounds of baby-AES with correlation of magnitude 1/8. For the corresponding linear attack, we requested 2^9 randomly chosen plaintext-ciphertext pairs.

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'.

The correlation table of S' is displayed below.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	-4	0	4	0	0	-4	-8	-4	-4	0	4	0	-8	4
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

(a) (4 points) The maximal magnitude of correlation for a nonzero input/output mask in the correlation table is 8. Give an upper bound for the absolute value of the correlation of a linear approximation through the first two rounds of our new baby-AES.

(b) Find a linear approximation through the first two rounds of our new baby-AES whose magnitude of correlation achieves the upper bound of (a).

(c) (2 points) How many plaintext-ciphertext pairs will you request for a linear attack against our new baby-AES using a linear approximation whose bias matches the upper bound obtained in (a). Use the same implicit constant as we used for the attack on the original baby-AES described above.

(d) (3 points) Compare the amount and the type of encrypted information an attacker requires for differential and linear attacks, respectively.

(e) (4 points) The differential and linear attack presented in the lecture do not recover the complete secret key. State precisely their actual output and argue why this is in many situations still considered a "break". [Hint: The key schedule of (baby-)AES is invertible.]

Exercise 3 (Matching pennies over the phone)**.** The following protocol lets you play "Matching Pennies" over the phone when you have access to a hash function h.

1. Randomly choose a number r
2. Choose your a bit b corresponding to heads/tails and append it to r
3. Compute commitment $x = h(r \mid b)$ and send it to your fellow player.
4. Receive her commitment y
5. Both players reveal their choices and determine the winner.

(a) (3 points) Assume h is not collision resistant/2nd-preimage-resistant/preimage-resistant. What consequences does it have for the game?

(b) (2 points) Why is it necessary to prepend your chosen bit b with a random number?

Exercise 4. Let H_1 and H_2 be two hash functions. Let $H = H_1|H_2$ be the concatenation of them.

(a) (2 points) Is H collision resistant if *at least one* of H_1 and H_2 is collision resistant?

(b) (2 points) Analogously for second pre-image resistance and pre-image resistance, respectively.

Exercise 5. (2 points) Let H be a collision resistant hash function. Is the composition $H \circ H$ collision resistant?