Exercise Sheet #9

Advanced Cryptography 2022

Exercise 1 Differential Cryptanalysis of a Dummy Block Cipher

Consider the following block cipher having 63-bit inputs and 63-bit keys. Let the bits of the message be denoted by $m_0, \ldots, m_{62}$ and the bits of the key $k_0, \ldots, k_{62}$. To encrypt, we do the following three operations for r rounds:

1. For round j, do:
2. Let $m'_{3i} \leftarrow m_{3i} \oplus m_{3i+2}$, $m'_{3i+1} \leftarrow m_{3i+1} \oplus m_{3i+2}$, and $m'_{3i+2} \leftarrow m_{3i+1} \oplus m_{3i+3}$ for $i \in \{0, \ldots, 19\}$. Let also $m'_{60} \leftarrow m_{60} \oplus m_{62}$, $m'_{61} \leftarrow m_{61} \oplus m_{62}$, and $m'_{62} \leftarrow m_{61}$.
3. Then, let $m''_i \leftarrow m'_i \oplus k_{i+3j \bmod 63}$.
4. For the last step, for every $i \in \{0, \ldots, 20\}$, we take the bits m''_{3i},m''_{3i+1}, and m''_{3i+2} and pass them through the following 3×3 Sbox (where m''_{3i} is the most significant bit):

input	output
0	0
1	1
2	2
3	7
4	4
5	5
6	6
7	3

E.g, if $m''_0, m''_1, m''_2, m''_3, m''_4, m''_5 = 0, 1, 1, 1, 1, 0$, we get as an output $1, 1, 1, 1, 1, 0$.

- How do you decrypt a ciphertext?
- For $r = 1$, find a differential deviant property that has a probability of 1 to occur.
- Provide message pairs that will verify this property.
- Can you extend this property for more rounds (i.e., for $r > 1$)?
- Unfortunately, this path doesn't allow to mount a differential attack to recover part of the key the same way as shown in class. Suppose now that in the last round (and only in the last round), we put the xoring with the key layer after the Sboxes (i.e., we switch the order between step 3 and 4) and we replace the Sboxes of *the last round* with

input	output
0	1
1	4
2	3
3	5
4	2
5	6
6	7
7	0

Explain how you would use the previous diffential path to recover part of the key.

Exercise 2 Impossible Differentials

We consider a classical Feistel scheme (with two balanced branches, with the usual $\oplus$ operation). Following standard notations, $\Psi(f_1, \ldots, f_r)$ denotes an r-round Feistel scheme in which the ith round function is f_i. Note that we omit the branch swap in the last round. Let $C = \Psi(f_1, f_2, f_3, f_4, f_5)$ where the f_i's are *permutations* (note that usually, the f_i's are simple functions) over $\{0,1\}^{\frac{m}{2}}$. Let $\Delta \in \{0,1\}^{\frac{m}{2}}$ such that $\Delta \neq 0$. We let $a = \Delta \| 0 \in \{0,1\}^m$ be the concatenation of Δ followed by $\frac{m}{2}$ zero bits. Show that $\mathrm{DP}^C(a, a) = 0$ for any choice of the permutations and any $\Delta \neq 0$.

Exercise 3 Differential Probabilities

We consider a block cipher using the following function f as a building block

$$\begin{array}{rccl} f: & \{0,1\}^{32} \times \{0,1\}^{32} & \to & \{0,1\}^{32} \\ & (x, y) & \mapsto & f(x, y) = x + y \bmod 2^{32}. \end{array}$$

1. Compute $\mathrm{DP}^f(\delta \| \delta, 0)$, where $\delta =$ `0x80000000`, where $\|$ denotes the concatenation operation and $(x, y) \oplus (\delta \| \delta) = (x \oplus \delta, y \oplus \delta)$.
2. Compute $\mathrm{DP}^f(\delta \| \delta, 0)$, where $\delta =$ `0xC0000000`.
3. Compute $\mathrm{LP}^f(\delta \| \delta, \delta)$, where $\delta =$ `0x00000001`.
4. Compute $\mathrm{LP}^f(\delta \| \delta, \delta)$, where $\delta =$ `0x00000003`.

Reminder: The differential probabilities of a function f are defined by

$$\begin{array}{rcl} \mathrm{DP}^f(a, b) & = & \Pr[f(X \oplus a) = f(X) \oplus b] \quad \text{and} \\ \mathrm{LP}^f(a, b) & = & (2 \Pr[a \cdot X = b \cdot f(X)] - 1)^2, \end{array}$$

where X is a uniformly distributed random variable over the plaintext space.