Solution Sheet #9

Advanced Cryptography 2020

Solution 1 Differential Cryptanalysis of a Dummy Block Cipher

- For $j = r - 1$ down to 0:
  1. Do step 4, i.e., pass groups of three bits through the Sbox (note that the SBox is it's own inverse).
  2. Do step 3, i.e., XOR the key and get the bits $m'_0, \dots m'_{62}$.
  3. Get the message $m_0, \dots, m_{62}$ in the following way:
     - $m_{61} \leftarrow m'_{62}$.
     - $m_{62} \leftarrow m'_{61} \oplus m_{61}$.
     - $m_{60} \leftarrow m'_{60} \oplus m_{62}$.
     - Starting from $i = 19$ down to $i = 0$, do $m_{3i+1} \leftarrow m'_{3i+2} \oplus m_{3i+3}$, $m_{3i+2} \leftarrow m'_{3i+1} \oplus m_{3i+1}$, and $m_{3i} \leftarrow m'_{3i} \oplus m_{3i+2}$.
- We analyze the Sbox and compute the differential distribution table (DDT) of it. Given an input difference Δ_{in} and an output difference Δ_{out}, the number in the table indicates the size of the solution set $\{v\colon \mathsf{SBox(v)} \oplus \mathsf{SBox}(v \oplus \Delta_{\mathsf{in}}) = \Delta_{\mathsf{out}}\}$

	Δ_{out}							
Δ_{in}	0	1	2	3	4	5	6	7
0	8	0	0	0	0	0	0	0
1	0	4	0	0	0	4	0	0
2	0	0	4	0	0	0	4	0
3	0	0	0	4	0	0	0	4
4	0	0	0	0	8	0	0	0
5	0	4	0	0	0	4	0	0
6	0	0	4	0	0	0	4	0
7	0	0	0	4	0	0	0	4

We note that whenever the input difference is 4, then the output difference is always 4. The same occurs (obviously) for 0. Hence, our goal will be to get an input difference of 4 (or 0) at the entrence of the Sboxes. For this, note that we can ignore the second step of the scheme, since the XOR with the key doesn't change the differences. It remains to invert the first step. One can easily check that any input difference of the form $100, 000, \dots, 000$ will lead to a difference of $100, 000, \dots, 000$ at the entrance of the Sboxes. Then, with probability one, we will get the same output difference.

- An exemple of message pair that verify this deviant property is $m_1 = 000, \ldots, 000$ and $m_2 = 100, 000, \ldots, 000$.
- Since the difference is preserved at the output of the round, this can be extended to any number of rounds!

  Note that, while this shows a huge vulnerability in the cipher, it does not allow to mount a differential attack like shown in class since all key candidates will be equaly likely.
- The DDT of the new Sbox shows that when the input difference is 100, the possible output differences are 010,011,100,101, all occuring with the same probability. Hence, the attacks works as follow: choose two random plaintexts with input difference $100, 000, \ldots, 000$ to obtain two ciphertexts c_1 and c_2. From the previous question, we know that the difference before the last round of Sboxes is still $100, 000, \ldots, 000$. Hence, to filter out key candidates, one has to look at the leftmost block (the three first bits) of the two ciphertexts c_1 and c_2, guess the first 3 bits of the round key (i.e., $k_{3j}, k_{3j+1}, k_{3j+2}$), xor c_1 and c_2 with this guess, pass them through the Sbox (in the reversed direction), and check if the difference is 100. If not, this means that the guess is wrong.

Solution 2 Impossible Differentials

The propagation of the $(\Delta\|0, \Delta\|0)$ differential characteristic is depicted in Figure 1. As we know that the functions f_1,f_2,f_3,f_4, and f_5 are in fact permutations, we must take into account that a non-zero difference in input will result in a (possibly identical) non-zero difference in output. Thus, we see that there is a contradiction at the output of f_3. A value Δ XORed with a non-zero β difference cannot give a Δ difference. Thus, the probability that such a differential characteristic occurs in a 5-round Feistel scheme is equal to 0, provided that the f_i's are permutations.

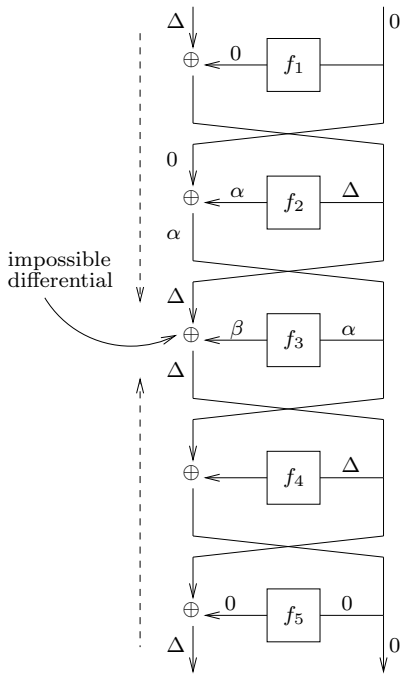

Figure 1: Propagation of a differential characteristic $(\Delta\|0, \Delta\|0)$ in a 5-round Feistel scheme

A complete security analysis of Feistel ciphers with 6 rounds or less is available in [1].

Solution 3 Differential & Linear Probabilities

1. We denote by $+$ the addition modulo 32. We have

$$\begin{aligned} \mathrm{DP}^f(\delta\|\delta,0) &= \Pr_{X,Y}[f(X\oplus\delta, Y\oplus\delta) = f(X,Y)] \\ &= \Pr_{X,Y}[(X\oplus\delta)+(Y\oplus\delta) = X+Y], \end{aligned}$$

where $X = X_{31}X_{30}\cdots X_0$ and $Y = Y_{31}Y_{30}\cdots Y_0$ are uniformly distributed random 32-bit strings. We introduce the following notations: we let S_i be the addition modulo 2^{32} of $X_iX_{i-1}\cdots X_0$ and $Y_iY_{i-1}\cdots Y_0$ and let C_i be the carry bit resulting from this addition. Note that $S_{31} = X + Y$ and that the modular addition erases the last carry bit, so that $C_{31} = 0$.

We have $X' = X\oplus\delta = \overline{X_{31}}X_{30}\cdots X_0$ and $Y' = Y\oplus\delta = \overline{Y_{31}}Y_{30}\cdots Y_0$, therefore $S_{30} = S'_{30}$ and $C_{30} = C'_{30}$. Finally,

$$X + Y = (X\oplus\delta)+(Y\oplus\delta) \Leftrightarrow X_{31}\oplus Y_{31} = \overline{X_{31}}\oplus\overline{Y_{31}},$$

and as $\overline{a}\oplus\overline{b} = a\oplus b$ for any bitstrings a and b, we conclude that

$$\mathrm{DP}^f(\delta\|\delta,0) = 1.$$

2. This time, $X' = X\oplus\delta = \overline{X_{31}X_{30}}X_{29}\cdots X_0$ and $Y' = Y\oplus\delta = \overline{Y_{31}Y_{30}}Y_{29}\cdots Y_0$. Similarly to the previous question, $S_{29} = S'_{29}$ and $C_{29} = C'_{29}$. Therefore,

$$\begin{aligned} X+Y = X'+Y' &\Leftrightarrow \begin{cases} X_{30}\oplus Y_{30} = \overline{X_{30}}\oplus\overline{Y_{30}} \\ X_{31}\oplus Y_{31}\oplus C_{30} = \overline{X_{31}}\oplus\overline{Y_{31}}\oplus C'_{30} \end{cases} \\ &\Leftrightarrow C_{30} = C'_{30}. \end{aligned}$$

Denoting $b = C_{29} = C'_{29}$, Table 1 shows the different values of the carry bits C_{30} and C'_{30} depending on the values of X_{30}, Y_{30}, and b. We deduce that $C_{30} = C'_{30}$ occurs with probability $\frac{1}{2}$. Finally,

$$\mathrm{DP}^f(\delta\|\delta,0) = \frac{1}{2}.$$

[1] L. Knudsen. The security of Feistel ciphers with six rounds or less. *Journal of Cryptology*, 15(3):207–222, 2002.

Table 1: Possible values of the carry bits C_{30} and C'_{30}, depending on X_{30}, Y_{30}, and on the previous carry bit $b = C_{29} = C'_{29}$

X_{30}	Y_{30}	$\overline{X_{30}}$	$\overline{Y_{30}}$	C_{30}	C'_{30}
0	0	1	1	0	1
0	1	1	0	b	b
1	0	0	1	b	b
1	1	0	0	1	0

3. We have

$$\begin{aligned} \mathrm{LP}^f(\delta\|\delta,\delta) &= (2\Pr[\delta\cdot X\oplus\delta\cdot Y=\delta\cdot f(X,Y)]-1)^2 \\ &= (2\Pr[\delta\cdot X\oplus\delta\cdot Y=\delta\cdot(X+Y)]-1)^2. \end{aligned}$$

As $\delta\cdot X=X_0$, $\delta\cdot Y=Y_0$, and as $\delta\cdot(X+Y)=X_0\oplus Y_0$,

$$\mathrm{LP}^f(\delta\|\delta,\delta)=1.$$

4. Here, we have $\delta\cdot X=X_1\oplus X_0$ and $\delta\cdot Y=Y_1\oplus Y_0$. As $\delta\cdot(X+Y)=X_0\oplus Y_0\oplus X_1\oplus Y_1\oplus C_0$ (using the notations of the previous questions), we have

$$\mathrm{LP}^f(\delta\|\delta,\delta)=(2\Pr[C_0=0]-1)^2.$$

As $C_0=0$ with probability $\frac{3}{4}$, we conclude that

$$\mathrm{LP}^f(\delta\|\delta,\delta)=\frac{1}{4}.$$

The reference papers on differential and linear cryptanalysis are [2] and [3] respectively.

[2] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems (extended abstract). In A. Menezes and S. Vanstone, editors, *Advances in Cryptology – Crypto'90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990. Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer-Verlag, 1990.

[3] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology – Eurocrypt'93: Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 1993. Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, 1993.