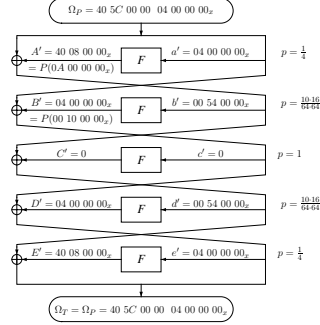


Tutorial on Differential Cryptanalysis

An Example of a 0R-Attack on 5-Round DES

We use a 5-round characteristic with probability $p = \frac{1}{10485.76}$:



An Example of a 0R-Attack on 5-Round DES (cont.)

The algorithm:

- We choose $m = \frac{2}{p} \approx 20000$ random pairs P, P^* such that $P' = \Omega_P$, and request the corresponding ciphertexts T and T^* under the unknown key K .
- We keep only the pairs satisfying $T' = \Omega_T$, and discard the others. About $m(p + 2^{-64})$ pairs remain (from the m pairs): $mp \approx 2$ right pairs and $2^{-64}m$ wrong pairs.
- The differences of the inputs and the outputs of the S boxes of the last round are known from $T' = T \oplus T^*$ (and from the characteristic):

The two inputs of F in the 5th round differ only in the 6th bit. Thus, the two inputs of S2 in the 5th round differ by $0S_x$ in the input. From T^* we know that the outputs of S2 differ by A_x .

An Example of a 0R-Attack on 5-Round DES (cont.)

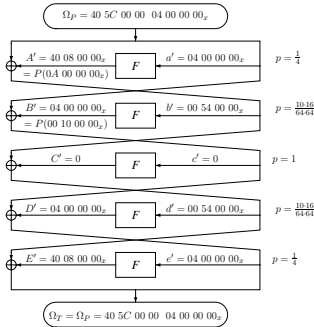
- When looking at the difference distribution table of S2, we find 16 possible pairs for this combination, thus we reduce the number of possible keys by a factor of $\frac{16}{2^6} = \frac{1}{4}$.
- Other pairs further reduce the number of possible keys.

The Difference Distribution Table of S2:

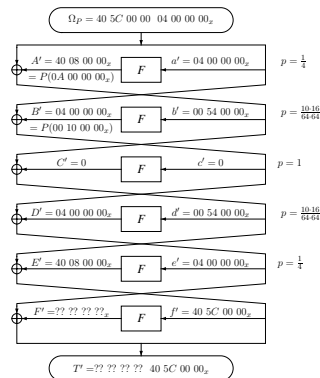
Input XOR Ω_P	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
S_x	0	0	0	4	0	4	0	8	0	10	16	6	6	0	6	4
$3F_x$	4	0	0	2	0	8	2	4	0	2	4	4	4	14	10	6

An Example of a 1R-Attack on 6-Round DES

We use the previous 5-round characteristic:



An Example of a 1R-Attack on 6-Round DES (cont.)



An Example of a 1R-Attack on 6-Round DES (cont.)

The algorithm:

- We choose $m = \frac{2}{p} \approx 20000$ random pairs P, P^* such that $P' = \Omega_P$, and request the corresponding ciphertexts T and T^* under the unknown key K .
- We keep only the pairs satisfying $T'_R = (\Omega_T)_L$, and discard the others. About $m(p + 2^{-32})$ pairs remain (from the m pairs) of which about $mp \approx 2$ are right pairs and $2^{-32}m$ are wrong pairs.
- The differences of the inputs of the S boxes of the last round are known from T'_R (and from the characteristic). The differences of the outputs of the S boxes of the last round are known from $T'_L \oplus (\Omega_T)_R$.
- As $T'_R = (\Omega_T)_L = 40\ 5C\ 00\ 00_x$, we attack only 3 S-boxes in the last round: S1, S3 and S4.

An Example of a 1R-Attack on 6-Round DES (cont.)

- For each of the above S-boxes: By using the difference distribution table we find several possible 6-bit keys for every pair of inputs and outputs. If we have sufficiently many pairs then only two possible 6-bit keys remain.

Note:

Let K be a 6-bit key and:

$$Si(\alpha \oplus K) \oplus Si(\beta \oplus K) = \Delta$$

Then for $K' = K \oplus \alpha \oplus \beta$ we have:

$$Si(\alpha \oplus K') \oplus Si(\beta \oplus K') = Si(\beta \oplus K) \oplus Si(\alpha \oplus K) = \Delta$$

$\alpha \oplus \beta$ is determined by the characteristic, thus keys come in pairs K, K' .

- We have $2^3 = 8$ possibilities for 18 key bits. Thus, we reduce the number of possible keys by a factor of $\frac{2^3}{2^6} = 2^{-15}$.

S-Boxes

In order to find characteristics with high probabilities we would like to find out which input differences of F can cause zero output difference.

In particular we want to find out which input differences of S1 cause zero output difference:

- 0_x input difference to S1 causes 0_x output difference.
- Furthermore, S1 is designed in such a way that in order to receive 0_x output difference from a non zero input difference at least one of four bits must be non zero. Those four bits are the first two bits and the last two bits (bits 1, 2, 5 and 6).

S-Boxes (cont.)

- By the expansion E those exact bits are used for other S-boxes. The first 2 are used for S8 and the last 2 are used for S2. Thus, when seeking non zero input and zero output differences for S1 we must involve another S-box.

Input XOR	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2

S-Boxes (cont.)

Other S-boxes are designed by the same criteria, i.e.,

$$\begin{aligned} 04_x &\not\rightarrow 0_x \\ 08_x &\not\rightarrow 0_x \\ 0C_x &\not\rightarrow 0_x \end{aligned}$$

Conclusion: In DES, in order to receive the same output of the F -function, two different inputs must differ in the input of at least **two** S boxes.

S-Boxes (cont.)

From the difference distribution table of S1 the possibilities for bits 1, 2, 5 and 6 which can produce zero output difference are:

12	56	12	56
00	00	00	00
01	10	10	01
11	00	01	11
01	01	01	11
11	10	10	01
10	00	11	10
01	10	10	11
10	11	11	00
11	00	11	01
11	01	01	10
10	10	10	11

S-Boxes (cont.)

From the difference distribution table of S2 the possibilities for bits 1, 2, 5 and 6 which can produce zero output difference are:

12	56	12	56
00	00	00	00
01	10	10	01
11	00	01	11
01	01	01	11
11	10	10	01
10	00	10	10
01	11	11	00
10	00	11	01
11	01	01	10
11	10	10	11
11	11	11	11

Note: All S-boxes are designed similarly.

S-Boxes (cont.)

We focus on the following possibilities:

00	01	10	00
11	11	10	01

We can conclude from these possibilities that when the input difference of S_i is non zero then the only way not to influence S_{i+1} is to use 10 as the first two bits. Furthermore, we have to use 01 or 11 as the last two bits in order not to involve S_{i-1} .

On the other hand:

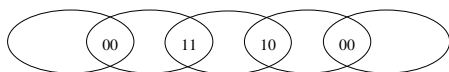
- If we use 10 as the first two bits then the input difference of S_{i-2} must be non zero.
- If we use 01 or 11 as the last two bits the input difference of S_{i+2} must be non zero.

S-Boxes (cont.)

Conclusion: In DES, in order to receive the same output of the F -function, two different inputs must differ in the input of at least **three** S boxes.

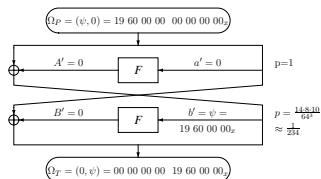
Previously we have seen characteristics which involve three S-boxes (Iterative characteristics).

The way to do this:



Iterative Characteristics

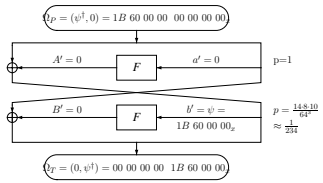
The first iterative characteristic:



uses S1, S2 and S3. The input differences are 03_x , 32_x and $2C_x$ respectively.

Iterative Characteristics (cont.)

The second iterative characteristic:



uses S1,S2 and S3 as well. The input differences are 03_x , 36_x and $2C_x$ respectively.