Scribe: Cryptography and Network Security

Akash Singh Sant (20CS60R40)

October 16, 2020

1 Differential Cryptanalysis

Differential cryptanalysis involves comparing the x-or (exclusive-or) of two plaintexts to the x-or of the corresponding two ciphertexts.
It is a chosen plain text attack.
In this attack we can ignore the initial permutation and its inverse (it has no effect on cryptographic significance).

1.1 Need of Differential Analysis:

To understand the need of differential analysis let us consider two plain text p_1 and p_1'.
Let the key be K. Now p_1 on XORing gives us an intermediate state

$$u_1{=}p_1 \oplus k_1$$

Now p_1' on XORing gives us an intermediate state

$$u_1'{=}p_1' \oplus k_1$$

Now if we take XOR of u_1 and u_1' we get

$$u_1 \oplus u_1'{=}p_1 \oplus p_1'.$$

From the above equation we can see the effect of key gets cancelled out.Now we have an expression whose right hand side is known to us.Now we have some information about the XOR of an internal state of cipher which can be used for some attack.

1.2 Informal Working:

In this attacker choses an input XOR ,x'. He has several tuples : (x,x*,y,y*) such that x$\oplus$x*=x'.
For each pair of y and y*, attacker guesses the key value of the last round.
Decrypts the pair, and checks the XOR at the last but one round.
Attacker checks out whether the result matches with the most probable outcome (which he has found out using some probabilistic approach, analogous to the

finding of the best differential equation).
Attacker maintains a frequency table, for each key noting the number of matches. It is expected that the candidate key will have the highest number of matches.

1.3 Differential characteristics of the S-Box

Lets suppose our s-box have m→n bit mapping S: $\{0,1\}^n \rightarrow \{0,1\}^m$.We will consider an ordered pair of bit-strings of length m, say (x,x*) for which XOR of x and x* is fixed.
We find input XOR : x $\oplus$ x*
And then for corresponding output we find y=S(x),y*=S(x*)
So the XOR of y and y* will be given by:

$$y \oplus y^* = S(x) \oplus S(x^*).$$

Let del(x') be the set of all ordered pairs, (x,x*) such that x$\oplus$x*=x'.
Now in this for every value of x we will have a corresponding x*. So for n bit x well have 2^n pairs.
for eg :del(1011)=(0000,1011),(0001,1010),. . . ,(1111,0100). Now on distribution of the S-box output XOR for the input XOR = 1011

x	x^*	y	y^*	y'
0000	1011	1110	1100	0010
0001	1010	0100	0110	0010
0010	1001	1101	1010	0111
0011	1000	0001	0011	0010
0100	1111	0010	0111	0101
0101	1110	1111	0000	1111
0110	1101	1011	1001	0010
0111	1100	1000	0101	1101
1000	0011	0011	0001	0010
1001	0010	1010	1101	0111
1010	0001	0110	0100	0010
1011	0000	1100	1110	0010
1100	0111	0101	1000	1101
1101	0110	1001	1011	0010
1110	0101	0000	1111	1111
1111	0100	0111	0010	0101

In the above table we can see that y' that is S(x) $\oplus$ S(x*) has a non uniform distribution.
Frequency Distribution of the Output XORs show that only 5 out of the 16 possible XORs occur, this is because two different plain text will map to two different Cipher text (bijective) hence S(x) $\neq$ S(x*).

It can be seen that there are some XOR in y' which occur 0 times like 0000 and there are some XOR which occur very frequently like 0010 (occurring 8 times). Attacker exploits this property,which serves as the distinguisher. This above values can be stored in the form of table where the row a' stand for input differential and column b' stand for output differential and the corresponding cell(a',b') gives the frequency of output differential b'.A table is shown below.

a' \ b'	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	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

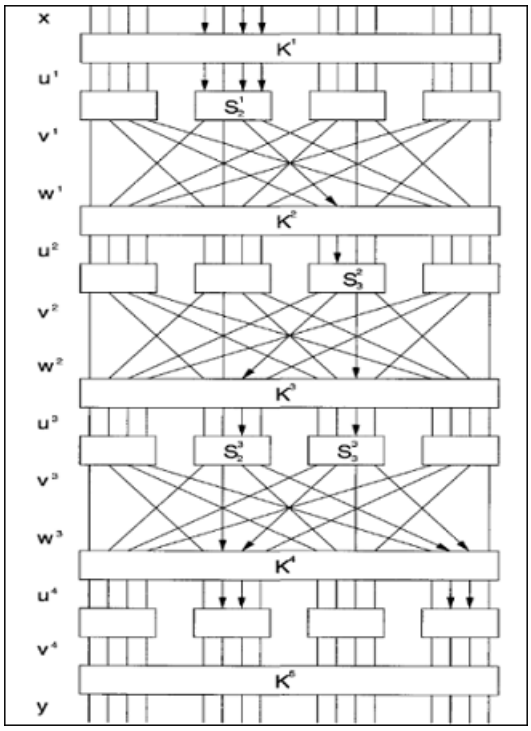
for eg: for input differential 0010(2) and output differential 0101(5) the corresponding entry is 6.

1.4 Working

In this we look a property which involve differential at x and u^4,the idea is that differential equation should hold with a very high probability. This probability is measured by propagation ratio.
Propagation ratio is the probability that an input XOR a' gives an output XOR b'. The pair (a',b') is called Differential. The propagation ratio can be measured using the equation given below :

$$R_p(\text{a'},\text{b'})=N_D(\text{a'},\text{b'})/2^m$$

where N_D(a',b') is an entry in table . 2^m is the number of input possible.
To explain let us consider working on the given plain text cipher text pair.



In the above figure we can see the sbox S_2^1 affects sbox S_3^2 in turn affects sbox S_2^3 and S_3^3.
Now we'll calculate prop-ratio for these s-boxes

$$S_2^1, R_p = N_D(1011,0010)/2^4 = 1/2$$

1/2 is the probability that the s box will give output differential of 0010 if input differential is fixed to 1011.

$$S_3^2, R_p = N_D(0100,0110)/2^4 = 3/8$$

3/8 is the probability that the s box will give output differential of 0110 if input differential is fixed to 0100

$$S_2^3, R_p = N_D(0010,0101)/2^4 = 3/8$$

3/8 is the probability that the s box will give output differential of 0101 if input differential is fixed to 0010

$$S_3^3, R_p = N_D(0010,0101)/2^4 = 3/8$$

3/8 is the probability that the s box will give output differential of 0101 if input differential is fixed to 0010
N_D(a,b) is taken from the table given above showing the frequency of output differential b on a fixed input differential a.

Thus resultant Prop-ratio is obtained as:

$$R_p(0000\ 1011\ 0000\ 0000,0000\ 0110\ 0000\ 0110)=(1/2)*(3/8)^3=27/1024$$

So now we choose a plain text whose XOR is 0000 1011 0000 0000 and we request for all the cipher text for which the plain text will XOR to 0000 1011 0000 0000 and then the differential at u^4 should be 0000 0110 0000 0110.
So we start guessing some part of the last round key and then go back to u^4 and check whether we got the same differential 0000 0110 0000 0110 .
Note that we need to guess 8 bits of the key.So total no of guesses=2^8=256.
Now if the guess was correct we'll have a probability of occurrence 27/1024.
If it is wrong then we'll have a lesser probability and then we make another guess.

2 Conclusion

In this lecture we discussed the Differential Cryptanalysis . We also learnt that certain characteristics are required for good sbox :
1.It should be built with a uniform distribution.
2.A low probability of the differential is desirable.

3 References

1.Lecture slides
2.Cryptography: Theory and Practice - Douglas Robert Stinson