Scribe: Cryptography and Network Security (Class.19.A)

Vishal Gourav

05-Oct-2020

1 Introduction

The discussion will be on the drawbacks of linear s-boxes and why non-linearity is abetter approach. Further, we will also discuss the properties of XOR and other components of Block cipher.

2 Algebraic Normal Form

We already know what CNF and DNF are but in cryptography we use something called ANF or Algebraic Normal Form of expressions to represent function used inside a S-Box. Some properties can be listed as follows:-

- It is basically AND-XOR expression i.e., variables $ANDed$ with each other in some manner which are in turn $XORed$ with each other. For example, $f(x, y, z) = xy \oplus yz$.
- The expressions might have different degrees based on the number of variables used inside each sub-expression. For example, $y = a_1x_1 \oplus a_2x_2$ has a degree 1 and $y = a_1x_1x_2 \oplus a_2x_2x_1$ has a degree 2.

3 Non-Linear S-Box

Non Linear S-Boxes are vital in encryption to achieve **confusion** because they protect the relationship between cipher text and key more comprehensibly. The drawbacks of Linear S-box and advantages of non-linearity can be further explained as follows:-

- Linear Functions follow the property that $f(x, y) = f(x) + f(y)$. They are of the form:-

$$y_1 = a_{11}x_1 \oplus a_{12}x_2..... \oplus a_{1n}x_n$$
$$y_2 = a_{21}x_1 \oplus a_{22}x_2..... \oplus a_{2n}x_n$$

$$y_3 = a_{31}x_1 \oplus a_{32}x_2 ..... \oplus a_{3n}x_n$$
$$y_4 = a_{41}x_1 \oplus a_{42}x_2 ..... \oplus a_{4n}x_n$$
$$.....$$
$$.....$$
$$y_m = a_{m1}x_1 \oplus a_{m2}x_2 ..... \oplus a_{mn}x_n$$

- But, the problem with linear functions is that as a linear function forms a line if plotted on a graph, there is a leak of information about the key from the cipher text.Therefore we fail in getting confusion.

x_1	x_2	0	x_1	x_2	$x_1 \oplus x_2$	$f(x_1, x_2) = x_1$	$f(x_1, x_2) = x_1x_2$
0	0	0	0	0	0	0	0
0	1	0	0	1	1	0	0
1	0	0	1	0	1	1	0
1	1	0	1	1	0	1	1

  Here, $f(x_1, x_2) = x_1$ is a linear function and every linear functions output matches exactly with at least one of the possible 2^n functions of given n variables in ANF. But, in $f(x_1, x_2) = x_1x_2$ which is a non-linear function we see that that the outputs don't match with any of the possible functions of functions of x_1, x_2 in ANF.

- Thus we can define a non-linear s-box function as one which has a **hamming distance** of at least 1 to any possible function of given variables and the least possible distance as **Non-Linearity**. As we see in above example the non-linearity= $min(1, 1, 1, 3) = 1$.

- So a good s-box is one which has a good set non-linear functions defining each constituent s-box. For example, $f(x_1, x_2) = x_1x_2$, $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3$, etc.

4 XOR and its properties

XOR or Exclusive OR function is represented by the symbol '$\oplus$' and is defined as $f(x_1, x_2) = x_1 \oplus x_2 = x_1\overline{x}_2 + x_2\overline{x}_1$. It has the following properties:-

- **Closure**. XOR follows closure property as output can be either 0 or 1 only.

- **Associative**. XOR follows associativity i.e., $(x_1 \oplus x_2) \oplus x_3 = x_1 \oplus (x_2 \oplus x_3)$.

- **Identity**. Every element has an identity under XOR operation which is 0. $x \oplus 0 = x$.

- **Inverse**. Every element has an inverse which is the element itself i.e., $x \oplus x = 0$.

- **Commutative**. XOR follows commutativity i.e., $(x_1 \oplus x_2) = (x_2 \oplus x_1)$

Thus we can conclude that XOR is an **Abelian Group**. This feature of XOR makes it possible to have **stochastical equivalence** of keys i.e., input keys are equivalent statistically, which in simple words means that the cipher text hides information about the key.

5 Circular Shift and Swap Operations

Another operation that is abundantly used in Block cipher is arithmetic circular shifts. Here we shift an element left or right by k bits, the MSB in case of left shift moves to LSB and LSB in case of right shift moves to MSB. Figure 1 expresses the notion :-

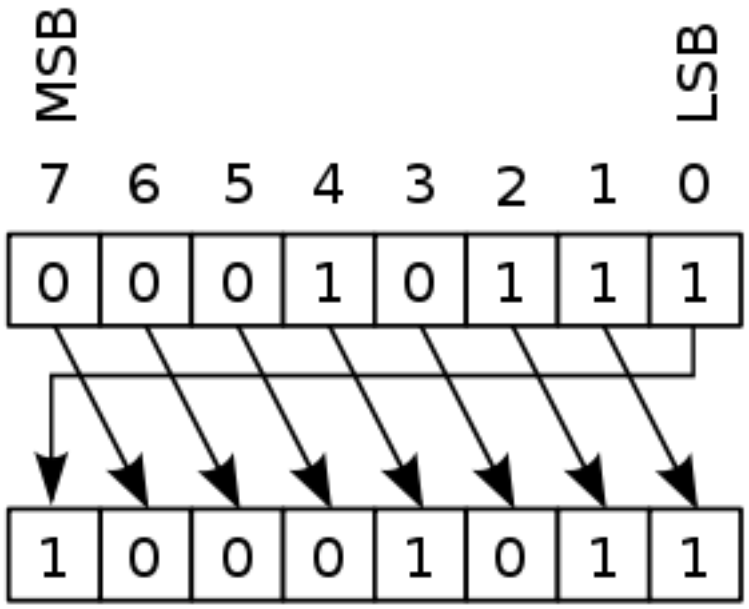

Figure 1: Example of Circular Right Shift

Swap operation is essentially circularly shifting the block left or right by half of its size. For example, 010100 after swapping becomes 100010.

6 Feistal Permutation

Feistel permutation is a pre-cursor of DES algorithm. Here we try to achieve what we call diffusion. How it works is that in every round we do a simple swap

operation on one part of block and the other part is encrypted using the key and the first part. In every round the parts we do the operation on are also exchanged. The operations done are as follows:-
Encryption. $L_i = R_{i-1}$ and $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
Decryption. $R_{i-1} = L_i$ and $L_{i-1} = R_i \oplus f(L_i, K_i)$
Here i is the round, L_i and R_i are the left and right parts of the block and K_i is the key in ith round. Figure 2 gives a diagrammatic representation of a Feistel Permutaion.

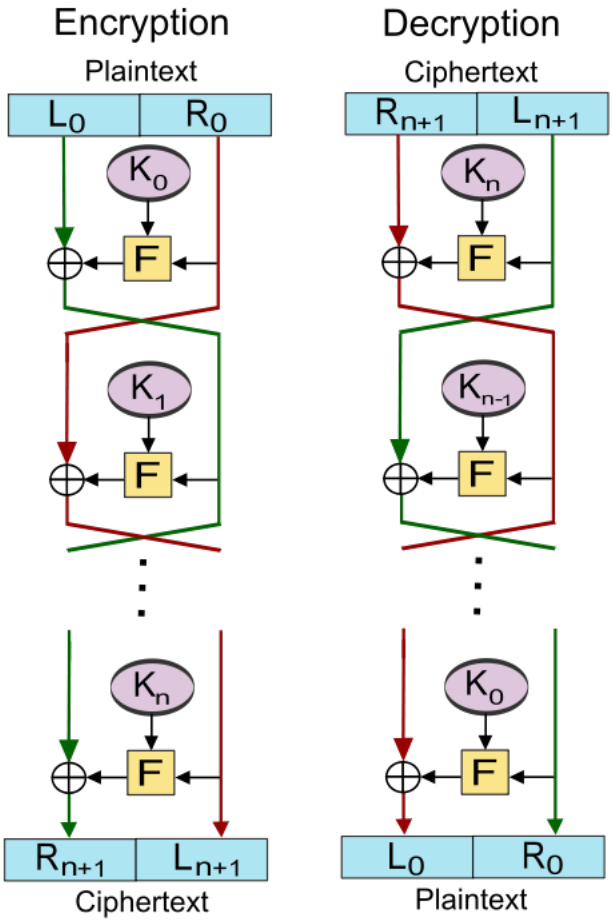

Figure 2: Feistal Permutaion

7 Conclusion

We have discussed the drawbacks of linear s-boxes and why non-linearity holds the key to become good s-box. We also discussed the properties of XOR operator and Feistel permutaion.