Scribe: Cryptography and Network Security (Week.7.Class.4.B)

Prashant Shishodia

21-Oct-2020

Introduction

Differential analysis is used for chosen plain text attacks (CPA). Unlike linear analysis that uses linear approximation it is based on the analysis of the xor of two inputs, and the corresponding outputs, which we will see in this discussion is called a differential.

Differential

For a given x', let's consider the set of pairs $\Delta(x') = \{(x, x^*) : x \oplus x^* = x'\}$. Considering the bit size to be m, we first note the following few properties of differentials.

- $|\Delta(x')| = 2^m$. This is because for each value of x there will be a distinct value of $x^* = x \oplus x'$. Also if for the sake of contradiction, say $x \oplus x_1 = x \oplus x_2, x_1 \neq x_2$, then xor'ing with x on both sides would give $x_1 = x_2$
- Therefore set of all x or x^* is same as $\{0,1\}^m$. Therefore for fixed x', both x and x^* are distributed uniformally.
- Not only sum of all entries in a row is 2^m ($\Delta(x') = \{0,1\}^m$), but also the sum of all entries in a column. This can be realised by observing that for each y there will be an x such that $S(x) = y$, and therefore the x, x^* corresponding to $y, y^* = y' \oplus y$ would correpsond to the differential $(x' = x \oplus x^*, y')$ for all y.

We say, $y = S(y), y^* = S(x^*)$, and we further define $y' = S(y) \oplus S(x^*)$. The intution behind this xor'ing is to xor'out the key from $S(y), S(y^*)$, making y' independent of the key. The property that we exploit in this attack is the expected non-uniform distribution of y' for pairs in $\Delta(x')$, for fixed x'. The pair (x', y') is then called a **differential**. The count of differentials (informal name) denoted by $N_D(x', y')$ is the number of pairs (x, x^*) such that $y' = y \oplus y^*$.

Difference Table

Similar to Linear Approximation Table, in Linear Analysis, we create a difference table in Differential analaysis, in which rows corresponds to x' and columns to y', and the cell corresponding to x', y' denotes $N_D(x', y')$.

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

We note the following properties about the table.

- $N_D(x' = 0, y' = 0) = 2^m$. Because $x \oplus x^* = x' = 0 \implies x = x^* \implies y = y^* => y' = 0$
- $N_D(x' \neq 0, y' = 0) = 0$. Because $x \oplus x^* = x' \neq 0 \implies x \neq x^* \implies y \neq y^* \implies y' \neq 0$. Therefore in the first row and first column, only one cell corresponding to $(x' = 0, y' = 0)$ will be non-zero.
- Each entry is even, i.e, $N_D(x', y')$ is always even. This is because the pair (x, x^*) and (x^*, x) correspond to the same y'. This also mean, that since $N_D(x', y')$ is never 1, for some of the $y's$ $N_D(x, y)$ will be 0 giving us a non-uniform distribution.

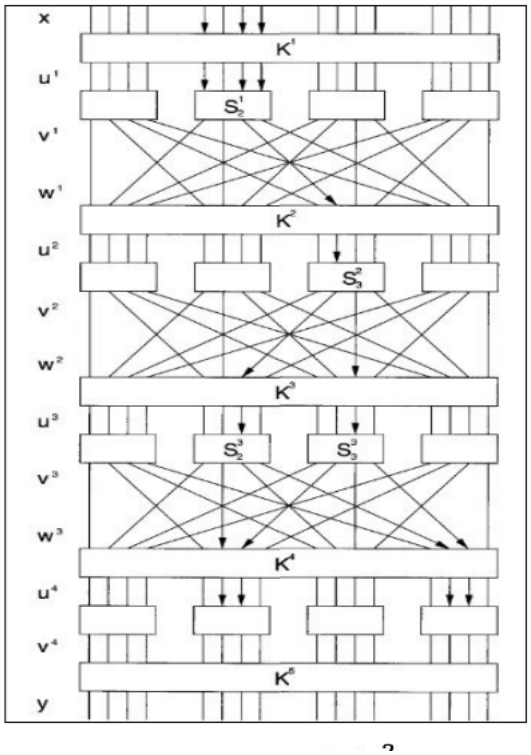
Proppagation Ratio (aka Prop Ratio) for a differential (a', b'), denoted by $R_p(a', b')$ is the probability of getting b' as output difference, for input difference a', and is defined as

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

For multiple rounds, the propagation ratios are assumed to be independent. Therefore, given a series of differentials, i.e, a **differential trail**, $(x'_1, x'_2), (x'_2, x_3), ...(x'_{Nr-1}, x'_{Nr})$, we can find the probability of getting x_{Nr} as the output differential when x'_1 is the input differential as:

$$R_p(x_{Nr'}, x'_1) = \prod_{i \in [0, Nr-1]} R_p(x_i, x_{i+1})$$

The Attack



The idea behind the attack is to choose a differential that occurs with maximum probability. Suppose we're just dealing with a single layer. Then we can choose then differential (x', y') which has the maximum probability of occuring, i.e, $R_p(x', y')$. Now, to find the key, for each (x, x^*) such that $x \oplus x^* = x'$, we compute $y'_{emp} = y \oplus y^*$ (y'_{emp} denotes the empirical value), and we choose the key that has the maximmum matches.

For multiple rounds, we can calculate a differential with high enough probability using the indepndency among each round's differential. We can then again calculate empirical values and choose the last round key to be the one with the maximum matches. We also try to choose the differentials with minimum number of bits, to ensure that least possible number of S-Box'es are affected. Note that we only needs to guess the bits of the key that are set in differential, thus further reducing our search space. Also, it has to be noted that the intermediate keys don't affect our final differential because they get's xor'ed out while calculating the differential.

The Defense

We saw that the non-uniformity could be exploited to get the keys. Therefore two protect against a differential attack, S-Box should be designed in a way to ensure low prop ratio for all pairs of differential. The less is the maximum prop ratio, the more number of plain, cypher text pairs attacker will have to check, thus ensuring low prop ratio would make it harder for the attacker to break the cipher.

Conclusion

Differential attack exploits the non-uniformity in the system, to break the cipher. Since, it is not possible to make such ciphers completely uniform in terms of difference, the best defence strategy is to make them as uniform as possible, thus decreasing the maximum probability for any differential.