Different Types of Attacks on Block Ciphers

Wageda Alsobky, Hala Saeed, Ali N.Elwakeil

Abstract: ***Cryptanalysis is a very important challenge that faces cryptographers. It has several types that should be well studied by cryptographers to be able to design cryptosystem more secure and able to resist any type of attacks. This paper introduces six types of attacks: Linear, Differential , Linear-Differential, Truncated differential Impossible differential attack and Algebraic attacks. In this paper, algebraic attack is used to formulate the substitution box(S-box) of a block cipher to system of nonlinear equations and solve this system by using a classical method called*** *Gröbner* ***Bases . By Solving these equations, we made algebraic attack on S-box.***

Keywords: Linear attack; Differential attack; Algebraic attack; S-box; *Gröbner* ***Bases***

I. INTRODUCTION

Cryptography is an essential process to transmit data in a secure way. It protects data against passive and active attacks [1]. More generally, cryptography is almost constructing protocols that prevent public from reading private data[1]. Cryptographers face a huge number of difficults to design the cryptosystem. One of these challenges is the attack that tries to penetrate the cryptosystem [2]. There are two types of attacks based on the method of treating data transmitted: active attack and passive attack[1,2]. In active attack, the hacker attempts to modify and change the data transmitted between sender and receiver[2]. This type of attack is divided into five types: Masquerade, Modification of messages, Repudiation, Replay and Denial of service[1,2]. On the other hand, hacker in the passive attack uses the data being transmitted but doesn't affect it[2]. This type includes another two types: The release of message content and Traffic analysis[1,2]. Based on what type of information the hacker has available, there are two types: Statistical and Algebraic attacks. Statistical attacks are divided into linear and differential attacks[3]. Statistical attacks are considered easier than algebraic attacks since they avoid the complexity of the algebraic attacks[3]. Algebraic attacks depend on formulating the cipher into system of equations and then solve it[4]. The block ciphers depend on the substitution boxes(S-boxes). These S-boxes are static and have no relation with the secret key, so the secret key is the only volatile parameter [4] .The design of S-boxes was published by Don Coppersmith in 1994. Until this date, the use of S-boxes in the standard wasn't perfectly understood [5]. Since S-boxes are the only nonlinear component of block ciphers, they have an important effect on cryptographic strength [5]. The design of S-boxes represents an important problem for security because they are the only nonlinear part in an encryption process and each successful linearization approximation can help break a few bits of the key [5].S-box operates independently on each byte of the state using a substitution table [6]. The main limitation of S-box is that it is fixed through the encryption algorithm. This main point of weakness attracts the cryptanalyst to exploit it for certain attacks [7]. There are four evaluation criteria for S-Boxes : bijectivity, nonlinearity, strict avalanche, and independence of output bits [7]. The nonlinearity of S-box reflects the algebraic degree that should be highly enough to resist the algebraic attacks [7] . In this paper, we have used algebraic attack to penetrate the S-box of a block cipher.

In our study, we will explain the different types of attacks on block ciphers and use one type of them called algebraic attack to penetrate the S-box.

In section 2, we introduce the definition of the attack. Then in section 3, different types of attacks are introduced. In section 4, the principle of light weight AES S-box is explained. In section 5, the resistance of algebraic attacks (Γ) explained to measure the strength of the S-box. In section 6, we apply *Gröbner* Bases as a method for solving multivariate system of nonlinear equations included in the mathematical model of the S-box to penetrate it.

II. DEFINITION OF ATTACK

Attack of cryptosystem (also called cryptanalysis) means understanding how the cryptosystem works with the aim of finding and improving techniques in order to defeat or weak this system [8]. Results of cryptanalysts' research are used by cryptographers to improve the strength of the encryption algorithm to be able to resist any attack [8]. Abroad range of organizations (such as government and companies) practiced cryptanalysis to decrypt other nations' confidential communications.[8]

A. Different types of attacks

There are different types of attacks based on what type of information the hacker has available. These types are explained as follows:[3]

1) *Statistical attacks*

In these attacks statistical weaknesses are exploited in a targeted algorithm. They includes six types: Differential , Linear, Differential-linear , Truncated differential and Impossible differential attack.[3]

- **Differential attack** [9]

This type of attack try to find the difference between related plaintexts that are encrypted . The plaintexts may differ by a few bits.

Revised Manuscript Received on August 05, 2020.

***** Correspondence Author

Wageda Hafez*, Department of Basic Engineering Sciences, Benha Faculty of Engineering, Benha University, Egypt. E-mail: WAGEDA.ALSOBKY@bhit.bu.edu.eg

Hala Saeed, *****, Department of Basic Engineering Sciences, Benha Faculty Of Engineering, Benha University, Egypt. E-mail: hala.saeed@bhit.bu.edu.eg.

Ali N.Elwakeil, Department of Basic Engineering Sciences, Benha Faculty Of Engineering, Benha University, Egypt.

The plaintext to be encrypted are chosen by the attacker (but attacker doesn't know the key) and then encrypts related plaintexts . Then statistical analysis is used by the cryptanalyst to search for signs of non-randomness in cipher texts, zeroing in on areas where the plaintexts differ . Every bit of the related cipher texts should have a 50/50 chance of flipping; the cryptanalyst searches for areas where this is not true. Any such underlying order is a clue to recover the key.

- **Linear attack** [10]

It is one of the two most widely used attacks on block ciphers; the other being differential attack. It seeks to find affine approximations to the action of a cipher. There are two parts to linear attack. The first one is about constructing linear equations relating plaintext, cipher text and key bits that have a high bias , whose probabilities of holding (over the space of all possible values of their variables) are as close as possible to 0 or 1. The second is about using these linear equations in conjunction with known plaintext-cipher text pairs to derive key bits.

- **Differential- Linear attack** [11]

In this type a differential characteristic is used over part of the cipher with a probability of 1 (this probability would be much lower for the whole cipher for a few rounds). The rounds immediately following the differential characteristic have a linear approximation defined, and we expect that the probability of the linear approximation that holding for one chosen plaintext but not the other will be lower for the correct key for each chosen plaintext pair.

- **Truncated differential attack** [12]

This type of attack is a generalization of differential cryptanalysis. In this type, the full difference between two texts is analyzed by ordinary differential cryptanalysis and the truncated variant considers differences that are only partially determined. It makes predictions of only some of the bits instead of the full block.

- **Impossible differential attack** [13]

This attack is a form of differential attack for block ciphers. differences ,that propagate through the cipher , that are impossible (having probability 0) are exploited at some intermediate state of the cipher algorithm.

2) *Algebraic attack [14]*

This type uses polynomials with several variables over finite field. It depends on converting the encryption system into a simultaneous multivariate equations system then solve it by one of algebraic tools such as grobner bases. This type requires very small number of known plaintexts.

III. PRINCIPLE OF LIGHT WEIGHT AES S-BOX

Definition 1 *(mathematical definition of S-box)* [15]

A substitution operation or a $m \times m$ S-box (or S-box of the size $m \times m$) is a mapping $V : \mathrm{F}_2^m \to \mathrm{F}_2^m$,where $m \geq 2$ is a fixed positive integer. A m -argument Boolean function if a mapping $g : \mathrm{F}_2^m \to \mathrm{F}_2$. An S-box $V : \mathrm{F}_2^m \to \mathrm{F}_2^m$ can be decomposed into the sequence, $V = (f_1, f_2, ..., f_m)$ of Boolean functions such that $V(f_1, f_2, ..., f_m) = (f_1(x_1, x_2, ..., x_m), f_2(x_1, x_2, ..., x_m), ..., f_m(x_1, x_2, ..., x_m))$. We say that the functions $f_1, f_2, ..., f_m$ are the components functions of S-box.

The S-box is constructed by the composition of two transformations:[16]

1) Taking multiplicative inverse $(\mathrm{x}')^{-1}$ *in* $GF(2^4)$. $(\mathrm{x}')^{-1}$ *is* defined by the inverse function $I(x')$ as follows:

$$I(x') = \begin{cases} (x')^{14}, x' \neq 0 \\ 0, x' = 0 \end{cases}$$

2) Applying an affine transformation function $y(x')$ over GF (2) defined by:

$$y(x') = Ma \times x' + '2' = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_3' \\ x_2' \\ x_1' \\ x_0' \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad (1)$$

Where $x_i' (i = 0,1,2,3)$ are the bits of the byte x' and x_3' is the most significant bit.

Case Study :

Let the design equation of the S-box be $13x^{-1} + 2$ of $GF(2^4 / x^4 + x + 1)$, then the S-box can be as shown in Table 1:

Table I: S-box of equation $13x^{-1} + 2$ of $GF(2^4 / x^4 + x + 1)$

Input	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
Output	9	1	5	7	8	E	C	D	B	6	A	3	0	4	F	2

Step 1: The mathematical model of S-box formed as follows:[17]

$$x_3z_3 + x_3 + x_0 + x_3z_2 + x_1z_0 + x_2z_1 = 0, \quad (2)$$

$$x_3z_3 + x_3 + x_2z_3 + x_2 + x_3z_0 + x_0z_0 + x_2z_2 + x_1z_1 = 0, \quad (3)$$

$$x_2z_3 + x_2 + x_3z_0 + x_2z_0 + x_3z_1 + x_1z_3 + x_1 + x_0z_1 + x_1z_2 = 0, \quad (4)$$

$$x_3z_3 + x_3 + x_3z_2 + x_2z_1 + x_1z_0 + x_0z_3 + x_0 + z_3 + 1 = 0, \quad (5)$$

$$x_3z_3 + x_3 + x_3z_0 + x_2z_3 + x_2 + x_2z_2 + x_1z_1 + x_0z_0 + z_0 = 0, \quad (6)$$

$$x_3z_0 + x_3z_1 + x_2z_3 + x_2 + x_2z_0 + x_1z_3 + x_1 + x_1z_2 + x_0z_1 + z_1 = 0, \quad (7)$$

$$x_3z_1 + x_2z_0 + x_1z_3 + x_1 + x_0z_2 + z_2 = 0, \quad (8)$$

$$x_3z_3 + x_3z_2 + x_2z_1 + x_1z_0 + x_0z_3 + x_0 = 0, \quad (9)$$

$$x_3z_3 + x_3 + x_3z_0 + x_2z_3 + x_2z_2 + x_1z_1 + x_0z_0 = 0, \quad (10)$$

$$x_3z_0 + x_3z_1 + x_2z_3 + x_2 + x_2z_0 + x_1z_3 + x_1z_2 + x_0z_1 = 0, \quad (11)$$

$$x_3z_1 + x_2z_0 + x_1z_3 + x_1 + x_0z_2 + x_0 = 0. \quad (12)$$

After making the mathematical model, we should determine the difficulty of solving these equations by using the resistance of algebraic attacks (Γ) which will be explained in the next section.

IV. THE RESISTANCE OF ALGEBRAIC ATTACKS (RAA)

One S-box with good cryptographic properties can ensure the cipher to resist against a variety of cryptanalysis methods, so any shortcomings of S-box will weaken the security of the cipher. [18]

Definition 2 [18]
Given r equations of t terms in $GF(2^4)$, the resistance of algebraic attacks (RAA) is denoted by Γ and is defined to be

$$\Gamma = ((t-r)/n)^{\lceil (t-r)/n \rceil} \quad (13)$$

This resistance reflects the difficulty of solving multivariate equations system. Thus, in this paper we will use this quantity ' Γ' to measure the resistance of the light weight S-box against algebraic attacks. [18]

Step 2:In our case study, $n = 4$, $r = 11$ and $t = 24$, so the resistance will be

$$\Gamma = ((24-11)/4)^{\lceil (24-11)/4 \rceil} = 45.09888 \quad (14)$$

Step 3: After estimating 'r' we will apply *Gröbner* Bases to this system to be solved.

V. GRÖBNER BASES AS A METHOD TO ATTACK

Gröbner is a classical method used to solve multivariate nonlinear system of equations. "Buchberger" developed the basic algorithm for computing *Gröbner Bases* in 1965 [19]. The discovery of this algorithm solved many problems that needed a computational treatment in commutative algebra, such as deciding whether a polynomial belongs to the ideal generated by some sequence of polynomials [20]. For more understanding *Gröbner Bases*, there are some definitions described as follows:

Definition 3 [19]
The lexicographic order: is the order > such that $y^{x_1} > y^{x_2}$ exactly when the first non-zero entry of the vector $x_1 - x_2$ is positive.

The graded lexicographic order: is the order > such that $y^{x_1} > y^{x_2}$, if deg y^{x_1} > deg y^{x_2} or deg y^{x_1} =deg y^{x_2}, and the first non-zero entry of $x_1 - x_2$ is positive.

The graded reverse lexicographic order: is the order > such that $y^{x_1} > y^{x_2}$ if deg y^{x_1} > deg y^{x_2} or deg y^{x_1} = deg y^{x_2}, and the last non-zero entry of $x_1 - x_2$ is negative.

We have defined each of these so that in every case, $y_1 > y_2 > \ldots > y_n$ for $R = k[y_1, y_2, y_3]$, the graded reverse lexicographic order satisfies

$$y_1^2 > y_1y_2 > y_2^2 > y_1y_3 > y_2y_3 > y_3^2,$$

While the graded lexicographic order has

$$y_1^2 > y_1y_2 > y_1y_3 > y_2^2 > y_2y_3 > y_3^2$$

Definition 4 [19]

Given a monomial order, a *Gröbner Bases* G of a nonzero ideal I is a generating set $\{g_1, g_2, \ldots, g_k\} \subseteq I$ such that for all $f \in R$, f leaves a remainder 0 when divided by G if and only if $f \in I$.

Definition 5 [20]
Let

$$S(f,g) = \frac{lcm(LM(f), LM(g))}{LT(f)} f - \frac{lcm(LM(f), LM(g))}{LT(f)} g \quad (15)$$

Where lcm is the least common multiple, LT is the leading term, and LM is the leading monomial. This is the S-polynomial of f and g, where's' stands for "Subtraction or Syzygy".

Theorem 1 *(Buchberger's Criterion)* [20]
Let $G = \{g_1, g_2, \ldots, g_k\} \subseteq I$ for some ideal I. If $S(g_i, g_j)$ gives a remainder 0 when divided by G for all pairs $g_i, g_j \in G$, then G is a *Gröbner* Bases of I.

Buchberger's Algorithm

- A monomial ordering is chosen.
- Starting with any generating set $G = \{g_1, g_2, \ldots, g_k\}$ of I.
- Selecting a pair of generators g_i, g_j from G.
- The remainder r when $S(g_i, g_j)$ is divided by G
- If $r = 0$ then continue, otherwise add r to the generating set G.
- Repeating from step 2 until processing all possible pairs from G.

Note that adding generators to G at any time, suddenly many more pairs have to be considered.
In our case study, after applying *Gröbner* Bases method to the mathematical model, then the **Result** will be as follows: (equations16-23)

Table II: Results of the Case Study

$1+z_3=0$,	(16)
$z_2+z^2{}_2=0$	(17)
$z_1=0$	(18)
$z_0=0$	(19)
$x_3=0$	(20)
$x_2=0$	(21)
$x_1=0$	(22)
$x_0-z_2=0$	(23)

Then the resistance will be

$$\Gamma=((3-2)/4)^{\sqrt{(3-2)/4}}=0.707106 \quad (24)$$

Hence the ratio of penetrating this S-box is 98.43209854%. This ratio means that this S-box has weak algebraic structure.

VI. CONCLUSION

In this paper, we have introduced different types of attacks on block ciphers .Also, we have used the algebraic cryptanalysis type to convert the S-box into a system of multivariate nonlinear equations . After that, we have solved it by a classical method called *Gröbner* bases . Finally, we have made an algebraic attack on the S-box by exploiting its weak algebraic construction.

REFERENCES

1. Christof Paar · Jan Pelzl2009Understanding Cryptography: A Textbook for Students and PractitionersSpringer Heidelberg Dordrecht London New York.
2. William Stallings2011Cryptography and network security : principles and practiceFifth edition. Boston Prentice Hall.
3. Blondeau, C., & Gérard, B. (2009, May). On the data complexity of statistical attacks against block ciphers. In Workshop on coding and cryptography-wcc (Vol. 2009, pp. 469-488).
4. Weinmann, R. P. (2009). Algebraic methods in block cipher cryptanalysis (Doctoral dissertation, Technische Universität).
5. The Laws of Cryptography with Java Code2003Available online at Neal Wagner's home page1-334
6. Analysis of Development of Dynamic S-Box Generation2017Computer Science and Information Technology154-163
7. Cryptographic analysis of all 4 × 4-bit S-boxes2012Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)118-133
8. Abomhara, M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.
9. Lai, X., Massey, J. L., & Murphy, S. (1991, April). Markov ciphers and differential cryptanalysis. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 17-38). Springer, Berlin, Heidelberg.
10. Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 386-397). Springer, Berlin, Heidelberg.
11. Langford, S. K., & Hellman, M. E. (1994, August). Differential-linear cryptanalysis. In Annual International Cryptology Conference (pp. 17-25). Springer, Berlin, Heidelberg.
12. Lee, S., Hong, S., Lee, S., Lim, J., & Yoon, S. (2001, December). Truncated differential cryptanalysis of Camellia. In International Conference on Information Security and Cryptology (pp. 32-38). Springer, Berlin, Heidelberg.
13. Kim, J., Hong, S., Sung, J., Lee, S., Lim, J., & Sung, S. (2003, December). Impossible differential cryptanalysis for block cipher structures. In International Conference on Cryptology in India (pp. 82-96). Springer, Berlin, Heidelberg.
14. Bard, G. (2009). Algebraic cryptanalysis. Springer Science & Business Media.
15. Improved rijndael-like S-box and its transform domain analysis2006Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)153-167
16. Evaluating algebraic attacks on the AES2003Diplom thesis, Technische
17. Generating S-Box Multivariate Quadratic Equation Systems And Estimating Algebraic Attack Resistance Aided By SageMath20151-21
18. Resistance of S-boxes against algebraic attacks2004Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)83-93
19. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations1983Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)146-156
20. An introduction to Gröbner bases1994American Mathematical Soc.
21. "Algebraic Construction of Powerful Substitution" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277 3878, Volume-8 Issue-6, March 2020.
22. -"Performance Analysis of Advanced Encryption Standard (AES) S-boxes "International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-1, May 2020.
23. "A Review of Advanced Encryption Standard (AES) Performance" Benha Journal of Engineering Science and Technology (BJEST) ISSN: 2357-0105, Volume-1 Issue-1, July 2018

AUTHORS PROFILE

Wageda Ibrahim Al Sobky was born in Egypt in 1981. She received the B.Sc. degree in communications and computers from benha faculty of engineering in 2003. She received the B.Sc. degree in science from benha faculty of science in 2008. She received the M.Sc. in applied mathematics from Benha University, Cairo, Egypt, in 2012 and the Ph.D. degree in cryptography from Ain Shams University, Cairo, Egypt, in 2017. She is currently a doctor in basic engineering sciences, at Benha Faculty of Engineering, Benha University, Egypt. Her current research interests include data security, and cryptography.

Hala Saeed Omar was born in Benha, Egypt in 1993. She received the B.Sc. degree in electrical power engineering computers from benha faculty of engineering in 2016. She is currently a demonstrator at Benha Faculty of Engineering, Benha University, Egypt.