

ALGEBRAIC PENETRATION OF LIGHT WEIGHT S-BOX IN IMAGE ENCRYPTION BY GROBNER BASIS

AHMED H. ELDEEB

Communications Department, Egyptian Chinese College for Applied Technology, Suze Canal University, Ismailia, EG41511, Egypt.

HAMED SHAWKY ZIED

Department of Communications and Electronic Engineering, Air Defense Collage, Alexandria.

WAGEDA I. AL SOBKY *

Basic Engineering Sciences Department, Benha Faculty of Engineering, Benha University, Banha 13511, Egypt. *Corresponding Author Email: wageda.alsobky@bhit.bu.edu.eg

HALA S. OMAR

Basic Engineering Sciences Department, Benha Faculty of Engineering, Benha University, Banha 13511, Egypt.

NADIA M.G. ALSAIDI

Department of Applied Sciences, University of Technology, Baghdad, 110066, Iraq.

SARA FOUAD

Electronic Department, Egyptian Chinese College for Applied Technology, Suze Canal University, Ismailia, EG41511, Egypt.

Abstract

Light weight encryption has a lot of applications in our technical life such as mobile security, which is based on block cipher with core S-Box. Substitution box (S-box) is the core of nonlinearity of block ciphers. So, it must be secure enough to avoid linear, differential, integral and algebraic attack. In this paper, light weight S-box was converted into a mathematical model containing multivariate system of equations, which were solved by a classical method called Grobner Bases. It was found that the Grobner Bases succeeded to penetrate the lightweight S-box with high efficiency which render this type of S-box weak for algebraic attack. In addition, the encryption system was applied after the hacking of S-box to verify the extent to which the theoretical results were achieved. Indeed, the theoretical and practical results were identical to confirm that the hacking of S-box was to a large extent.

Keywords: Encryption, Block Cipher, S-Box, Attack, Grobner

1. INTRODUCTION

The block cipher Rijndael has been declared the new Advanced Encryption Standard (AES) by the National Institute of Standards and Technology (NIST), which noted some limitations with the Data Encryption Standard (DES) in 1999[1]. The AES was published as a final standard (Federal Information Processing Standards Publications FIPS PUBS 197) in 2001. AES is a nonlinear transformation method that works well for both software and hardware cryptography applications since it has been shown to be a robust cryptographic primitive against linear, differential, integral, and algebraic attacks. Versions of the key sizes 128,192,256 bits and extra block sizes are used in these implementations [2].

The finite field Galois field $GF(2^8)$ is the domain over which all AES operations are conducted [3]. A Windows Phone software built in C#, an Android app written in Java [4], and a Windows console application written in C++ have all effectively implemented AES. It took significantly less time to implement AES using a 32-bit round lookup table than it did with an 8-bit separate subBytes, shiftRows, mixColumns, and AddRoundKey transformation. Block ciphers that are lightweight have been designed for effective hardware applications. Lightweight cryptographic techniques, including mix columns and parallel byte substitution, are much sought after for Internet of Things (IoT) applications in the current decade [5, 6].

Substitution Bytes is the initial transformation (Sub Bytes). It is employed in the encryption process, and the decryption procedure uses inverse Sub Bytes. This replacement causes difficulty in the AES method since it is a nonlinear substitution of bytes that works independently on each byte of the state using a substitution table [7]. Throughout the cryptography algorithm, this box remains unchanged. The primary area of vulnerability that draws cryptanalysts to examine the flaw in preparation for specific attacks is this limitation. Don Coppersmith published the S-box design in 1994. The use of S-boxes in the standard was not fully understood until this point.

From 2000 onwards, several algebraic attacks have been launched against the security of AES [8]. A mapping $S:GF(2^8) \rightarrow GF(2^8)$ that consists of an affine transformation function $A(x)$ and an inverse function $I(x)$ that yields the multiplicative inverse is known as Rijndael's S-box [9]. An affine transformation should be done to perform the Sub Bytes transformation after taking the multiplicative inverse in the finite field Galois field for the encryption procedure. Find the inverse affine transformation for the inverse Sub Bytes transformation before performing a multiplicative inverse of that byte as part of the decryption procedure. Both processes are completed simultaneously in this manner.

The values in S-box that relate to it are substituted for the corresponding values in the row and column. In a similar manner, inverse substitution of bytes is carried out [10]. Since the multiplication of the Galois field is a laborious procedure, the values are pre-calculated and replaced in the design as needed. To accomplish this, use the lookup table. To cut down on delay, Sub Bytes are handled similarly [11]. S-Boxes are evaluated based on four criteria: independence of output bits, stringent avalanche, nonlinearity, and bijectivity [12]. The algebraic degree that should be high enough to withstand algebraic attacks is reflected in the nonlinearity of the S-box [13], [29–37].

A novel method has been put out for creating S-boxes in the Advanced Encryption Standard (AES). This proposed S-box's construction method builds from small S-boxes specified over $GF(2^4)$ rather than $GF(2^8)$, as in the case of conventional AES. Using the new method has altered the Rijndael Algorithm (RA). The construction of this Modified Rijndael Algorithm (MRA) involved substituting small S-boxes for the S-box of RA, and as a result, the key expansion procedure of RA was altered. Every single little S-box has a unique equation. One of $GF(2^4)$'s three irreducible polynomials has been used to extract each equation. Compared to the S-box of RA, which used one equation and one

irreducible polynomial, this made cryptanalysis via finding distinct equations exceedingly challenging [14]. A Modified Rijndael Algorithm (MRA) S-box hardware implementation technique that is both efficient and effective has been proposed in [15,29]. Each little S-box's Boolean functions have been implemented through the use of combinational logic gates in this implementation. Therefore, in order to minimize the implementation complexity that arises from employing the composite field required for the reduction from GF (2⁸) to GF (2⁴) in the SubByte transformation of the Rijndael Algorithm (RA), a tiny field in MRA has been employed. Compared to the S-box of RA, which used one equation and one irreducible polynomial, this made cryptanalysis via finding distinct equations exceedingly challenging [14]. A Modified Rijndael Algorithm (MRA) S-box hardware implementation technique that is both efficient and effective has been proposed in [15,29]. Each little S-box's Boolean functions have been implemented through the use of combinational logic gates in this implementation. Therefore, in order to minimize the implementation complexity that arises from employing the composite field required for the reduction from GF (2⁸) to GF (2⁴) in the SubByte transformation of the Rijndael Algorithm (RA), a tiny field in MRA has been employed. In order to cryptanalyze the lightweight AES S-box, we will describe in this work how to transform the lightweight AES S-box into a mathematical model made up of multivariate systems of equations and then solve these equations using the Grobner Bases approach. We refer to this kind of attack as an algebraic attack.

In section 2, the process of light weight AES is described. And in section 3, a mathematical definition of S-box is introduced to understand the principle of light weight AES S-box which is explained in section 4. Section 5 explains how to convert S-box into a mathematical model, and then measures the strength of this S-box using the resistance of algebraic attacks (Γ) is explained in section 6. in section 7, Grobner Bases is applied as a method for solving multivariate system of nonlinear equations included in the mathematical model of the S-box to penetrate it. Finally, section 8 mention all practical tests of the system after penetration of s-box

2. DESCRIPTION OF LIGHTWEIGHT AES

The input of $A = (a_0, a_1, a_2, a_3)$ of the lightweight S-Box is represented as a 2×2 matrix of 4 bits (a nibble) as shown below.

$$A = \begin{pmatrix} a_0 & a_2 \\ a_1 & a_3 \end{pmatrix}$$

Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit	Bit
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

where $a_0 = \text{Bit}_{0,1,2,3}$, $a_1 = \text{Bit}_{4,5,6,7}$, $a_2 = \text{Bit}_{8,9,10,11}$, $a_3 = \text{Bit}_{12,13,14,15}$.

There are 4 main components of light weight AES: Nibble Sub, Shift Row, Mix Column, and Key Addition

A. Nibble Substitution (Nibble Sub) [16]

S-box of the lightweight AES is called nibble sub because it takes each input nibble and

substitutes it with an output nibble according to 4x4 look up table called substitution box (S-box). It applies the non-linear invertible function "S-Box function" to each element of the state.

B. Shift Row [16]

In this step, each row of the input block is rotated left wise by using different nibble amounts. The first row is unchanged while the second row is rotated left wise by one nibble. This is illustrated in Fig 2, where $U = (u_0, u_1, u_2, u_3)$, is the input and $V = (v_0, v_1, v_2, v_3)$, is the output.

$$\begin{pmatrix} u_0 & u_2 \\ u_1 & u_3 \end{pmatrix} \xrightarrow{\text{shift row}} \begin{pmatrix} u_0 & u_2 \\ u_3 & u_1 \end{pmatrix} = \begin{pmatrix} v_0 & v_2 \\ v_1 & v_3 \end{pmatrix}$$

C. Mix Column [16]

In this step, each column of the input block is taken and multiplied by a constant matrix in order to obtain a new output column, as shown below, $\mathbf{V} = (v_0, v_1, v_2, v_3)$, denotes the input and $\mathbf{W} = (w_0, w_1, w_2, w_3)$, denotes the output.³

$$\begin{pmatrix} v_0 & v_2 \\ v_1 & v_3 \end{pmatrix} \xrightarrow{\text{mix column}} \begin{pmatrix} w_0 & w_2 \\ w_1 & w_3 \end{pmatrix}$$

where $\begin{pmatrix} w_0 \\ w_1 \end{pmatrix} = \begin{pmatrix} \beta + 1 & \beta \\ \beta & \beta + 1 \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \end{pmatrix}$

and $\begin{pmatrix} w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} \beta + 1 & \beta \\ \beta & \beta + 1 \end{pmatrix} \begin{pmatrix} v_2 \\ v_3 \end{pmatrix}$

where

$$\beta = 0010,$$

$$w_0 = (0011 \otimes v_0) + (0010 \otimes v_1),$$

$$w_1 = (0010 \otimes v_0) + (0011 \otimes v_1)$$

and so on.

D. Key Addition [16]

In this step, the input block, $\mathbf{W} = (w_0, w_1, w_2, w_3)$ is excluded-ORed with the round key, $\mathbf{K}_i = (k_0, k_1, k_2, k_3)$, bit by bit to produce the 16 bit output block key, $\mathbf{S} = (s_0, s_1, s_2, s_3)$, as shown in Fig 4. The round key is derived from the secret key \mathbf{K} by using the key schedule. The exclusive-OR operation produces '1' if the bits of the input block and round key are different. Otherwise, the output bit is '0'

$$\begin{pmatrix} w_0 & w_2 \\ w_1 & w_3 \end{pmatrix} \oplus \begin{pmatrix} k_0 & k_2 \\ k_1 & k_3 \end{pmatrix} = \begin{pmatrix} s_0 & s_2 \\ s_1 & s_3 \end{pmatrix}$$

E. The Lightweight AES Key-schedule [17]

In light weight AES, one 16-bit round key, \mathbf{k}_0 , is produced from the 16-bit secret key which passed through a key-schedule to be used prior to the first round, and a 16-bit round key,

\mathbf{k}_i to be used in each round of light weight-AES. Light weight-AES encryption is defined to have 2 rounds, hence three round keys, \mathbf{k}_0 , \mathbf{k}_1 and \mathbf{k}_2 are generated as shown below.

$$\begin{aligned} \text{At round 0} &\rightarrow \begin{pmatrix} t_0 = k_0 \\ t_1 = k_1 \\ t_2 = k_2 \\ t_3 = k_3 \end{pmatrix} \\ \text{At round 1} &\rightarrow \begin{pmatrix} t_4 = t_0 \oplus \text{nipplesub}(t_3) \oplus \text{rcon}(1) \\ t_5 = t_4 \oplus t_1 \\ t_6 = t_5 \oplus t_2 \\ t_7 = t_6 \oplus t_3 \end{pmatrix} \\ \text{At round 2} &\rightarrow \begin{pmatrix} t_8 = t_4 \oplus \text{nipplesub}(t_7) \oplus \text{rcon}(2) \\ t_9 = t_8 \oplus t_5 \\ t_{10} = t_9 \oplus t_6 \\ t_{11} = t_{10} \oplus t_7 \end{pmatrix} \end{aligned}$$

Define the 16-bit secret key, K , as a 4 nibbles, $K = (k_0, k_1, k_2, k_3)$, and likewise, $k_0 = (t_0, t_1, t_2, t_3)$, $k_1 = (t_4, t_5, t_6, t_7)$ and $k_2 = (t_8, t_9, t_{10}, t_{11})$, then the round key values are obtained from the secret key as above. Noting that a round constant $\text{rcon}(i)$ is used in each round, where $\text{rcon}(1) = 0001$, and $\text{rcon}(2) = 0010$. As it is known that the S-box is the core of the Light weight AES so we will first need to know the definition of this core.

3. PRINCIPLE OF LIGHT WEIGHT AES S-BOX

Definition 1 (mathematical definition of S-box) [18]

The substitution S-box of size $n \times n$ maps n input to n outputs according to the mapping $V: f_2^n \rightarrow f_2^n$, where $n \geq 2$ is a constant positive integer. The Boolean function components of the S-box $V = (f_1(u_1, u_2, \dots, u_m), f_2(u_1, u_2, \dots, u_m), \dots, f_m(u_1, u_2, \dots, u_m))$. The evaluation of S-box is performed by taking multiplicative inverse $(u')^{-1}$ in $\text{GF}(2^4)$ and applying an affine transformation function $v(u')$ over $\text{GF}(2)$. The inverse function $I(u')$ and affine transform are defined as follows.

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

$$v(u') = \text{Max } u' + '2' = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} u'_3 \\ u'_2 \\ u'_1 \\ u'_0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

where u'_i ($i = 0, 1, 2, 3$) are the bits of the byte u' and u'_3 is the most significant bit.

The three irreducible polynomials in $\text{GF}(2^4)$ are defined as follows:

$$\begin{cases} u^4 + u + 1, \\ u^4 + u^3 + u^2 + u + 1, \\ u^4 + u^3 + 1. \end{cases}$$

4. MATHEMATICAL MODEL OF S-BOX

S-Box consists of some Boolean functions as presented before section 2. These functions consisting of the S-Box mathematical model is evaluated based on the following methods.

A. Algebraic Normal Form of the S-box (ANF)

ANF is described as follows: [20]

$$g(u) = b_0 \oplus \sum_{i=1} b_i u_i \oplus \sum_{1 \leq i < j \leq m} b_{ij} u_i u_j \oplus \dots \oplus b_{12\dots m} u_1 u_2 \dots u_m$$

where Σ, \oplus denote the modulo 2 summations.

B. Multivariate Quadratic Equation System of Light weight S-box

Light weight S-box composes of “patched” inverse in $GF(2^4)$ with 0 mapped on to itself with a multivariate affine transformation $GF(2^4) \rightarrow GF(2^4)$. These functions are called f and g respectively and let $s = g \circ f$. An input value will be denoted by u and the corresponding output value will be $v = f(u)$. And $W = s(u) = g(v) = g(f(u))$. Obviously, for the inverse transformation $v = f(u)$, $uv = 1$, when $u \neq 0$, i.e. [21]

$$\left(\left(\sum_{i=0}^3 u_i t^i \right) \left(\sum_{i=0}^3 u_i t^i \right) \right) = \sum_{k=1}^3 0t^k + 1$$

Expanding equation (7), we have

$$\sum_{i=0}^3 \sum_{j=0}^3 (u_i v_j)_{m(t)} (t^{i+j})_{m(t)} = \sum_{k=1}^3 0t^k + 1$$

In our case study, $t^4 = t^4 + t + 1$, By comparing coefficients of $t^k (0 \leq k \leq 4)$ of both sides in Equation (7), the four multivariate quadratic equations of the inverse transformation can be obtained. Since, $v \rightarrow z$ is linear, four multivariate quadratic equations of light weight AES S-box can be obtained. Now, we give the principle of generation of light weight AES S-box equations system. Multiplying u by v and the multiplication result modulo $m(t)$, the coefficients c_0, \dots, c_3 of $t^k (0 \leq k < 4)$ can be obtained. First, we explain the process of computation of the coefficients c_0, \dots, c_3 . We put $(u_0, \dots, u_3) = u$, $(v_0, \dots, v_3) = v$ and $(w_0, \dots, w_3) = w$ [8].

$$\begin{aligned} & u_3 v_3 t^6 + (u_2 v_3 + u_3 v_2) t^5 + (u_2 v_2 + u_3 v_1 + \\ & u_1 v_3) t^4 + (u_0 v_3 + u_3 v_0 + u_1 v_2 + u_2 v_1) t^3 + \\ & (u_0 v_2 + u_2 v_0 + u_1 v_1) t^2 + (u_0 v_1 + u_1 v_0) t + \\ & u_0 v_0 t^0 = 0t^3 + 0t^2 + 0t + 1t^0 \end{aligned} \quad (9)$$

Then, the multiplication results modulo $m(t)$ one by one and by comparing coefficients of both sides as follows: equations (10-13)

$$u_3 v_3 + u_0 v_3 + u_3 v_0 + u_1 v_2 + u_2 v_1 = c_0$$

$$u_3v_3 + u_2v_3 + u_3v_2 + u_0v_2 + u_2v_0 + u_1v_1 = c_1$$

$$u_2v_3 + u_3v_2 + u_2v_2 + u_3v_1 + u_1v_3 + u_0v_1 + u_1v_0 = c_2$$

$$u_0v_0 + u_2v_2 + u_3v_1 + u_1v_3 = c_3$$

According to the principle of light weight S-box, the relation between w and v is given by:

$$w = Dv + '2'$$

And,

$$v = 4w + '8'$$

Where,

$$\begin{pmatrix} v_3 \\ v_2 \\ v_1 \\ v_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} w_3 \\ w_2 \\ w_1 \\ w_0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Then,

$$\begin{cases} v_3 = w_3 + 1, \\ v_2 = w_0, \\ v_1 = w_1, \\ v_0 = w_2. \end{cases}$$

Substituting Equation (17) into the four equations (10-13), retrieving (equations18-21)

$$u_3w_3 + u_3 + u_0 + u_3w_2 + u_1w_0 + u_2w_1 = 0,$$

$$u_3w_3 + u_3 + u_2w_3 + u_2 + u_3w_0 + u_0w_0 + u_2w_2 + u_1w_1 = 0$$

$$u_2w_3 + u_2 + u_3w_0 + u_2w_0 + u_3w_1 + u_1w_3 + u_1 + u_0w_1 + u_1w_2 = 0,$$

$$u_0w_3 + u_0 + u_2w_1 + u_2 + u_3w_0 + u_1w_2 = 1,$$

Because there is no nonzero constant term in three of these equations (18-21), for $u = 0$, these three equations (18-20) are true with probability 1. When $u \neq 0$, the fourth equation (21) is true, so this equation is true with probability 15/16.

Since $uv = 1 (\forall u \neq 0)$, we have

$$\forall u \neq 0 \rightarrow u = u^2v$$

This equation is also true when $u = 0$, so we have

$$\forall u \in \text{GF}(2^4) \rightarrow \begin{cases} v \times u^2 \\ u^2 \times v^4 \\ \vdots \\ u^8 = v^8 \times u^{16} = v^8 \times u \end{cases}$$

The last equation is chosen in Equation (23). Noting that it is symmetric with respect to exchange of u and v , so the following two equations can be obtained:

$$\begin{cases} u^8 = v^8 \times u \\ v^8 = u^8 \times v \end{cases}$$

Then there are two equations over $GF(2^4)$ which are true with probability 1. Each of above two equations will give four quadratic equations with four variables because $u \rightarrow u^8$ is linear. Similarly, these eight equations can be obtained as follows: equations (25-32)

$$\begin{aligned} u_3w_3 + u_3 + u_3w_2 + u_2w_1 + u_1w_0 + u_0w_3 + u_0 + w_3 + 1 &= 0, \\ u_3w_3 + u_3 + u_3w_0 + u_2w_3 + u_2 + u_2w_2 + u_1w_1 + u_0w_0 + w_0 &= 0, \\ u_3w_0 + u_3w_1 + u_2w_3 + u_2 + u_2w_0 + u_1w_3 + u_1 + u_1w_2 + u_0w_1 + w_1 &= 0, \\ u_3w_1 + u_2w_0 + u_1w_3 + u_1 + u_0w_2 + w_2 &= 0, \\ u_3w_3 + u_3w_2 + u_2w_1 + u_1w_0 + u_0w_3 + u_0 &= 0, \\ u_3w_3 + u_3 + u_3w_0 + u_2w_3 + u_2w_2 + u_1w_1 + u_0w_0 &= 0, \\ u_3w_0 + u_3w_1 + u_2w_3 + u_2 + u_2w_0 + u_1w_3 + u_1w_2 + u_0w_1 &= 0, \\ u_3w_1 + u_2w_0 + u_1w_3 + u_1 + u_0w_2 + u_0 &= 0, \end{aligned}$$

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.

5. THE RESISTANCE OF ALGEBRAIC ATTACKS (RAA)

One S-box which has good cryptographic properties can ensure the cipher system to have high resistance against a variety of cryptanalysis methods, so any shortcomings of S-box will weaken the security of the cipher. Light weight AES S-box is a 4×4 Boolean functions and these 4 Boolean functions are affected each other. Even if these 4 functions have some properties simultaneously, the S-box Boolean function may not have similar properties. So, it is necessary for any S-box function to be analyzed according to its algebraic properties.

Definition2[22]

Given r equations of t terms in $GF(2^4)$, the algebraic attacks resistance (RAA) is denoted by Γ and is defined as follows.

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

The measures of multivariate equations system solving difficulty is based on the value of Γ . The lightweight S-box resistance for our case study, $n = 4$, $r = 11$, and $t = 24$, so the resistance will be.

$$\Gamma_1 = ((24 - 11)/4)^{\lceil 24-11/4 \rceil} = 45.09888$$

we use Gröbner Bases for solving the system and evaluate the .

6. Gröbner BASES AS AN ATTACKING METHOD

Multivariate nonlinear system of equations is solve based on Gröbner.. For more understanding Gröbner Bases, there are some definitions presented as follows:

Definition 4 [24,25]

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

Definition5 [26]

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

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) [25]

Let $G = \{g_1, g_1, \dots, g_k\} \subseteq I$ 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

1. Choose a monomial ordering.
2. Set $G = \{g_1, g_1, \dots, g_k\}$ of I as a started generating.
3. g_i, g_j from G are chosen as a pair of generators.
4. The remainder r when $S(g_i, g_j)$ is divided by G .
5. If $r = 0$ continue, otherwise add r to the generating set G .
6. Repeat this process from step 2 until all possible pairs from G are processed.

The results obtained in our case study after applying *Gröbner*Bases to the mathematical model is presented as below.

$$\begin{aligned} 1 + w_3 &= 0, \\ w_2 + w_2^2 &= 0, \\ w_1 &= 0, \\ w_0 &= 0, \\ u_3 &= 0, \\ u_2 &= 0, \\ u_1 &= 0, \\ u_0 - w_2 &= 0. \end{aligned}$$

Then the AAR resistance will be

$$\Gamma_2 = ((3 - 2)/4)^{\lceil 3-2/4 \rceil} = 0.70$$

This ratio means that this S –box has weak algebraic structure.

Case Study

Let the S –box design equation is $Au^{-1} + B$ of $GF(2^4/u^4 + u^3 + u^2 + u + 1)$, where $A=$ large prime number in the field, $B=$ the smallest prime number in the field then the S –box can be as shown in Table 3:

Table2: S-box (2)

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

Then the ANF will be (equations 45-48)

$$\begin{aligned}
 f_1 &= u_2 \oplus u_3 \oplus u_4 \oplus u_1u_2 \oplus u_1u_3 \oplus u_1u_4 \oplus u_2u_3 \oplus u_2u_4 \oplus u_2u_3u_4 \\
 f_2 &= u_1 \oplus u_3 \oplus u_4 \oplus u_1u_2 \oplus u_1u_4 \oplus u_2u_3 \oplus u_2u_4 \oplus u_3u_4 \oplus u_1u_3u_4 \\
 f_3 &= u_1 \oplus u_2 \oplus u_3 \oplus u_1u_3 \oplus u_1u_4 \oplus u_2u_3 \oplus u_2u_4 \oplus u_3u_4 \oplus u_1u_2u_3 \oplus 1 \\
 f_4 &= u_1 \oplus u_2 \oplus u_3 \oplus u_4 \oplus u_1u_2 \oplus u_1u_3 \oplus u_2u_4 \oplus u_3u_4 \oplus u_1u_2u_3 \oplus u_1u_3u_4 \\
 &\quad \oplus u_1u_2u_4 \oplus u_2u_3u_4
 \end{aligned}$$

Hence, the mathematical model of this S –box is as follows: (equations49-59)

$$\begin{aligned}
 u_2w_0 + u_3w_1 + u_1w_3 + u_1 + u_0w_3 + u_0w_0 + u_0 + u_3w_3 + u_3 + u_1w_1 + u_2w_2 &= 0, \\
 u_2w_0 + u_2w_1 + u_3w_2 + u_3w_1 + u_1w_3 + u_1w_0 + u_1 + u_0w_0 + u_0w_1 + u_2w_3 + u_2w_2 + u_2 + u_1w_2 + u_1w_1 &= 0, \\
 u_3w_3 + u_3w_0 + u_3 + u_2w_0 + u_2w_1 + u_3w_2 + u_3w_1 + u_1w_0 + u_0w_2 + u_0w_1 + u_1w_2 &= 0 \\
 u_3w_1 + u_3w_3 + u_3 + u_2w_0 + u_2w_2 + u_1w_3 + u_1 + u_1w_1 + u_0w_3 + u_0w_0 + u_0 + w_3 + w_0 + 1 &= 0, \\
 u_3w_2 + u_3w_1 + u_2w_0 + u_2w_1 + u_2w_3 + u_2w_2 + u_2 + u_1w_3 + u_1w_0 + u_1 + u_1w_2 + u_1w_1 + u_0w_0 + u_0w_1 + w_0 + w_1 &= 0 \\
 u_3w_3 + u_3w_0 + u_3 + u_3w_2 + u_3w_1 + u_2w_0 + u_2w_1 + u_1w_0 + u_1w_2 + u_0w_2 + u_0w_1 + w_2 + w_1 &= 0 \\
 u_3w_0 + u_3w_2 + u_2w_3 + u_2 + u_2w_1 + u_1w_3 + u_1w_0 + u_1 + u_0w_3 + u_0w_2 + u_0 + w_3 + w_2 + 1 &= 0 \\
 u_3w_1 + u_3w_3 + u_2w_0 + u_2w_2 + u_1w_3 + u_1 + u_1w_1 + u_0w_3 + u_0w_0 + u_0 &= 0, \\
 u_3w_2 + u_3w_1 + u_2w_0 + u_2w_1 + u_2w_3 + u_2w_2 + u_1w_3 + u_1w_0 + u_1 + u_1w_2 + u_1w_1 + u_0w_0 + u_0w_1 &= 0, \\
 u_3w_3 + u_3w_0 + u_3 + u_3w_2 + u_3w_1 + u_2w_0 + u_2w_1 + u_1w_0 + u_1w_2 + u_0w_2 + u_0w_1 + u_1 &= 0, \\
 u_3w_0 + u_3w_2 + u_2w_3 + u_2 + u_2w_1 + u_1w_3 + u_1w_0 + u_1 + u_0w_3 + u_0w_2 &= 0,
 \end{aligned}$$

Then, the factor Γ is $\Gamma = 45.09888$

By applying *Gröbner Bases* to this mathematical model, the following reduced equations (61-71) are deduced.

$$\begin{aligned}
 u_0w_1 + u_0w_2 + u_1w_0 + u_1w_2 + u_2w_0 + u_2w_1 + u_3w_0 + u_3w_1 + u_3w_2 + u_3w_3 &= 0 \\
 u_0w_1 + u_0w_2 + u_1w_2 + u_1w_3 + u_3w_0 + u_3w_3 &= 0, \\
 u_0w_1 + u_0w_3 + u_1w_0 + u_1w_2 + u_2w_1 + u_2w_3 + u_3w_2 + u_3w_3 &= 0 \\
 u_0w_0 + u_0w_1 + u_1w_1 + u_1w_2 + u_2w_2 + u_2w_3 &= 0, \\
 1 + w_2 + w_3 &= 0, \\
 1 + w_1 + w_3 &= 0, \\
 1 + w_0 + w_3 &= 0, \\
 u_3 &= 0, \\
 u_2 &= 0, \\
 u_1 &= 0, \\
 u_0 &= 0,
 \end{aligned}$$

Then, the resistance will be $\Gamma = 0.707106$, hence, the ratio of penetrating this light weight S-box is

$$1 - \left(\frac{\Gamma_2}{\Gamma_1} \times 100 \right) = 1 - \left(\frac{0.707106}{45.09888} \times 100 \right) = 98.43209854\%.$$

So, this S-box is algebraically weak. Finally, we concluded that S-box with design equation $Ax^{-1} + B$ in $GF(2^4)$ suffers from weak algebraic structure exposing it to algebraic attacks.

7. STATISTICAL ATTACK ANALYSIS

There are various ways to test the statistical analysis of the original and ciphered image, including the following:

I. The Histogram

The distribution of the statistical features of the encrypted image is obtained when the histogram of the encrypted image has a uniform distribution as shown in the figure. The figure shows the horizontal, vertical and diagonal correlations for the plain image and the scrambled image.

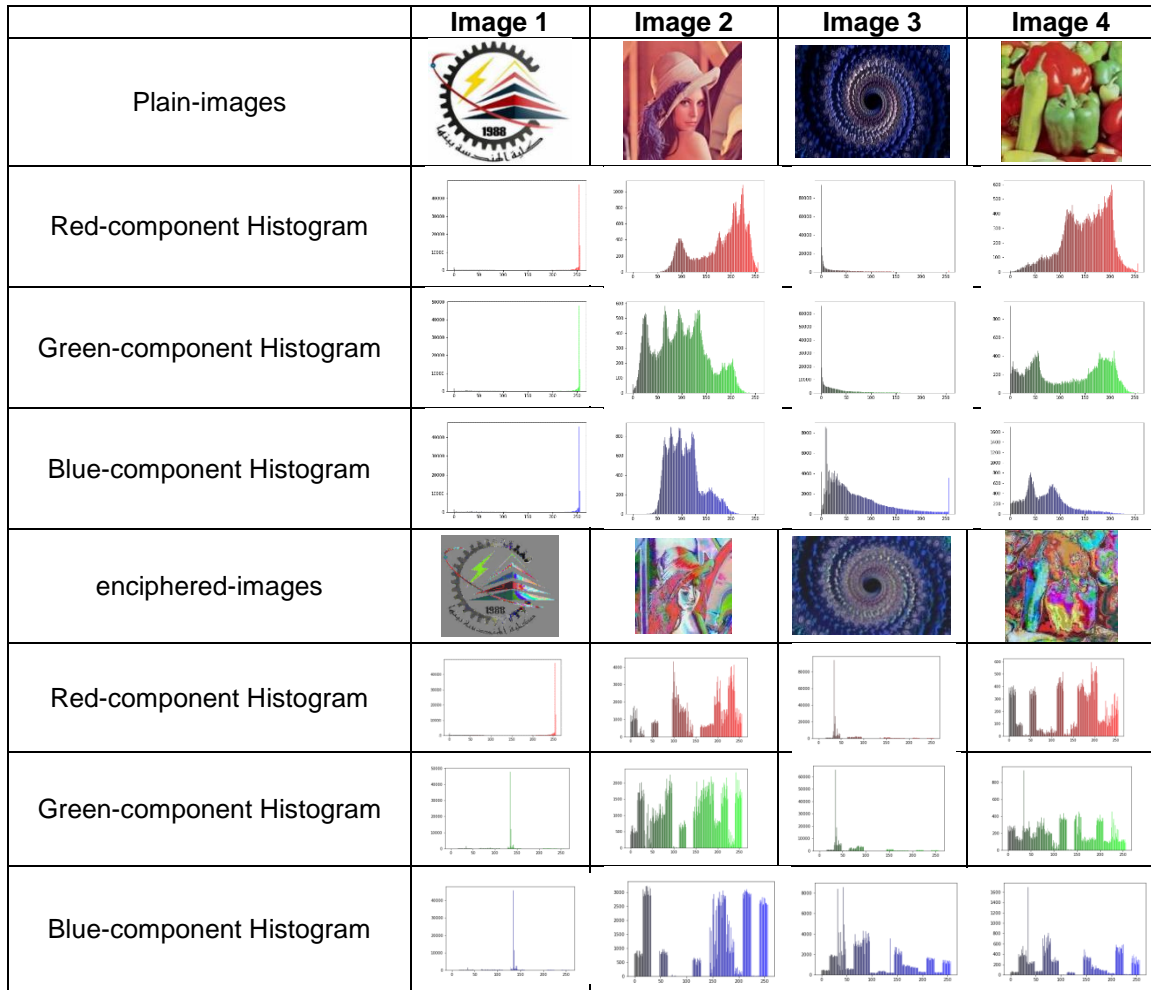


Figure 4: RGB mode Plain-images and enciphered- images using broken proposed enciphering scheme based on proposed S-Box with their corresponding histograms

III. Adjacent pixels Correlations

The correlation coefficient can be computed as follows

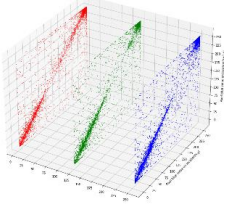
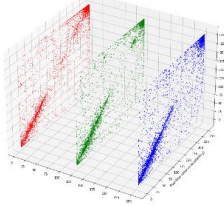
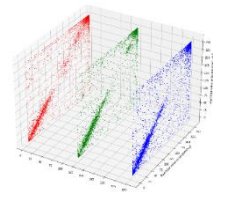
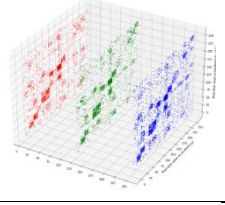
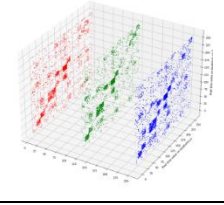
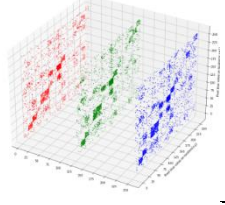
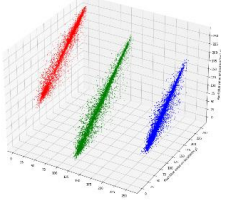
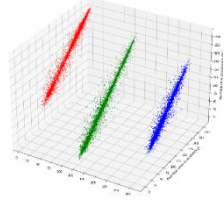
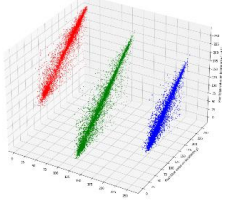
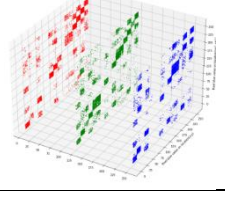
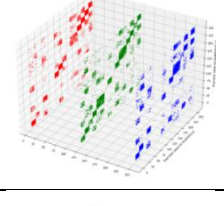
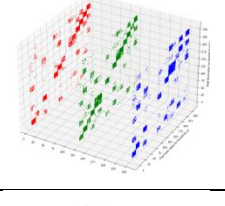
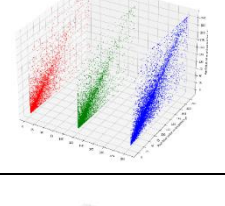
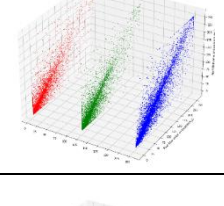
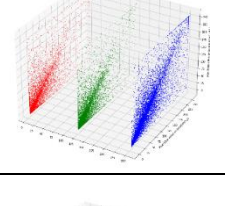
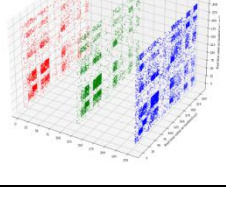
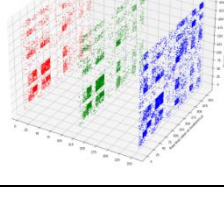
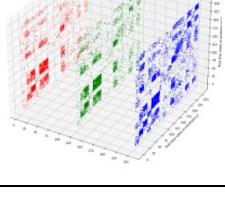
$$corr_{xy} = \frac{cov(x, y)}{\sqrt{D(x)D(y)}} \tag{3}$$

$$cov(x, y) = \frac{1}{n} \sum_{i=1}^n (x_i - E(x)) (y_i - E(y))$$

$$D(x) = \frac{1}{n} \sum_{i=1}^n (x_i - E(x))^2$$

The following figures show the ability of the proposed encryption scheme to break the correlation of the plain image on an all directions

The correlation values are shown in Table 2 as shown below

Image	Size	Image type	Correlation		
			Horizontal	Vertical	Diagonal
Image 1	350 × 306	Plain-image			
		Enciphered-image			
Image 2	256 × 256	Plain-image			
		Enciphered-image			
Image 3	728 × 455	Plain-image			
		Enciphered-image			

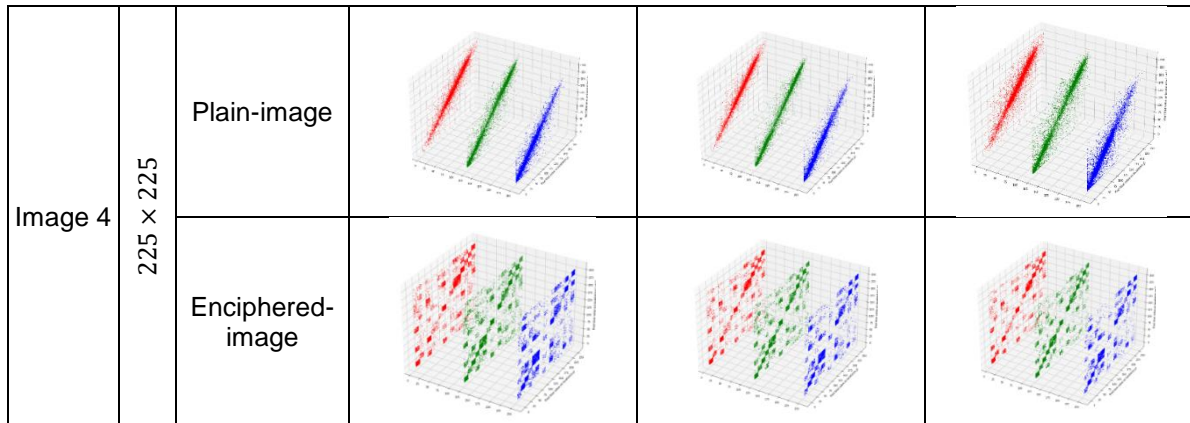


Table 2: Correlation values

Image	Plain Image Correlation			Ciphared Image Correlation		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Theoretical value	1	1	1	0	0	0
Image 1	0.9423187	0.9781144	0.966667	0.4572469	0.4781144	0.5412053
Image 2	0.7436674	0.8941671	0.97743378	0.4875409	0.5495421	0.47743378
Image 3	0.951328	0.939624	0.9042711	0.47060221	0.59079917	0.66335718
Image 4	0.6970602	0.7990799	0.89633571	0.4930021	0.47114002	0.76633571

Now it has become very clear that the results are very bad, which in turn reflects the weakness of the encryption system used by S-Box.

Differential Attack Analysis

Two factors can be used to define the impact of a single bit change in the plain image and how it affects the ciphared image. The NPCR (number of pixels change rate) is the first, and the UACI (unified average changing intensity) is the second. These are calculated in this way:

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i,j)}{M \times N} \times 100\%$$

$$D(i,j) = C_1(i,j) \oplus C_2(i,j)$$

$$UACI = \frac{1}{M \times N} \left(\sum_{i=1}^M \sum_{j=1}^N \frac{|E_1(i,j) - E_2(i,j)|}{255} \right) \times 100\%$$

The following table displays the NPCR and UACI values for the examined images.

Table 3: Differential Attack Analysis

Image	UACI	NPCR
Theoretical	33.9	100
Image 1	12.9945501792802	38.5336486192651
Image 2	12.9627556746402	37.763709919089
Image 3	10.7567018356325	37.5198179780855
Image 4	10.183756709573	37.5198179780855

From the above table we conclude that we already using bad nonlinear function for image encryption

8. CONCLUSION

It is shown that the problem of computing the resistance of algebraic attacks (RAA) of the nonlinear system (s-box) before and after attack by *Gröbner* algorithm is not easy but gives excellent results to prove that algebraic attack is a strong tool. This paper presents how to convert s-box into a mathematical model containing multivariate system of equations. After this conversion operation, the resulting equations are solved by a classical method, which has not been used in any applications since its discovery, in which efficient techniques for solving these problems such as converting it into a mathematical model containing multivariate system of equations. This method called *Gröbner* as already succeeded in solving these equations. Finally, we made an algebraic attack on the lightweight AES S-box by exploiting its weak algebraic construction. So, our advice is to use another bent function, to make S-Box hard to be broken.

References

- 1) Arabnezhad-Khanoki, H., Sadeghiyan, B., & Pieprzyk, J. (2019). S-boxes representation and efficiency of algebraic attack. IET Information Security.
- 2) Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.
- 3) Stallings, W. (2017). Cryptography and network security: principles and practice (pp. 92-95). Upper Saddle River: Pearson.
- 4) Annaqeeba, M., El-Sheikh, H. M., Elgarfc, T. A., & Zekryd, A. Software Implementation of Advanced Encryption Standard Algorithm on Android and Windows Phone Platforms..
- 5) Prathiba, A., & Bhaaskaran, V. S. (2018). Lightweight S-Box Architecture for Secure Internet of Things. Information, 9(1), 13.
- 6) Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. Journal of Cryptographic Engineering, 8(2), 141-184.
- 7) Wagner, N. R. (2003). The laws of cryptography with java code. Available online at Neal Wagner's home page.
- 8) Singh, A., Agarwal, P., & Chand, M. (2017). Analysis of Development of Dynamic S-Box Generation.
- 9) Leventi-Peetz, A. M., & Peetz, J. V. (2017, August). Generating and exploring S-box Multivariate quadratic equation systems with SageMath. In 2017 IEEE Conference on Dependable and Secure Computing (pp. 377-383). IEEE.
- 10) Vacca, J. R. (2012). Computer and information security handbook. Newnes.
- 11) Ahmed AAbdel-hafez, Reda-Elbarkouky, wageda_hafez."Comparitive Study of Algebraic Attacks", International Advanced Research Journal in Science Engineering and Technology(IARJSET), Volume 10, Issue 4 Ver. II (MAY -2016), PP52-57
- 12) Ahmed AAbdel-hafez, Reda-Elbarkouky, wageda_hafez."Algebraic Cryptanalysis of AES using Grobner basis", International Advanced Research Journal in Science Engineering and Technology(IARJSET), Volume 17, Issue 4 Ver. II (MAY -2016), PP52-57

- 13) Medhat Mansour, Wageeda Elsobky, Ayman Hasan, Wagdy Anis." Appraisal of Multiple AES Modes Behavior using Traditional Enhanced Substitution Boxes ", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020
- 14) Eslam wahba afify, Wageda I. El sobky, Abeer T. Khalil, Reda Abo Alez." Algebraic Construction of Powerful Substitution Box",International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-6, March 2020
- 15) Eslam w. afify, Abeer T. Khalil, Wageda I. El sobky, Reda Abo Alez." 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
- 16) Wageda Alsobky, Hala Saeed, Ali N.Elwakeil." Different Types of Attacks on Block Ciphers ", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-3, September 2020
- 17) Wageda I. El Sobky, Ahmed R. Mahmoud, Ashraf S. Mohra, T. El-Garf."
- 18) Enhancing Hierocrypt-3 performance by modifying its S-Box and modes of operations ", Journal of Communications Vol. 15, No. 12, December 2020
- 19) Abdel Halim A. Zikry, Ashraf Y. Hassan, Wageeda I. Shaban, Sahar F. Abdel-Momen..." Performance Analysis of LDPC Decoding Techniques ", International Journal of Recent Technology and Engineering (IJRTE)ISSN: 2277-3878, Volume-9 Issue-5, January 2021
- 20) wageda El Sobky, Sara Hamdy, Mustafa Hussien Mohamed"Elliptic Curve Digital Signature AlgorithmChallenges and Development Stages"International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278-3075 (Online), Volume-10 Issue-10, August 2021
- 21) Wageda I. El Sobky, Abdelkader A. Ismail; Ashraf S. Mohra; Ayman M. Hassan" Implementation Mini (Advanced Encryption Standard) by Substitution Box in Galois Field (2^4)" 2021 International Telecommunications Conference (ITC-Egypt) DOI: 10.1109/ITC-Egypt52936.2021.9513927
- 22) Wageda I. El Sobky, Sherif Hamdy Gomaa, Ashraf Y.Hassan" A Survey of Blockchain from the Viewpoints ofApplications, Challenges and Chances" International Journal of Scientific & Engineering Research Volume 12, Issue 4, April-2021ISSN 2229-5518
- 23) Wageda Ibrahim Alsobky ,Abdelkader Esmail ,Ashraf S. Mohra, Ayman Abdelaziem "Design and Implementation of Advanced Encryption Standard by New Substitution Box in Galois Field (2^8)" International Journal of Telecommunications, IJT'2022, Vol.02, Issue 01
- 24) Nada E. El-Meligy, Tamer O. Diab , Ashraf S. Mohra , Ashraf Y. Hassan and Wageda I. El-Sobky"A Novel Dynamic Mathematical Model Applied in Hash Function Based on DNA Algorithm and Chaotic Maps". Mathematics 2022, 10, 1333. <https://doi.org/10.3390/math10081333>
- 25) Yassein, H. R., Zaky, H. N., Abo-Alsoo, H. H., Mageed, I. A., & El-Sobky, W. I. (2023). QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra. Appl. Math, 17(1), 49-53.
- 26) Saeed, H., Ahmed, H. E., Diab, T. O., Zayed, H. L., Zaky, H. N., & Elsobky, W. I. Evaluation of the Most Suitable Hyperchaotic Map in S-Box Design Used in Image Encryption.
- 27) Nasry, H., Abdallah, A. A., Farhan, A. K., Ahmed, H. E., & El Sobky, W. I. (2022, August). Multi Chaotic System to Generate Novel S-Box for Image Encryption. In Journal of Physics: Conference Series (Vol. 2304, No. 1, p. 012007). IOP Publishing.
- 28) Mahfouz, A. M., Ismail, A. S., Nasry, H., & Elsobky, W. I. (2022, July). Path Detection for A Moving Target in Wireless Sensor Network Based on Clifford Algebra. In 2022 International Telecommunications Conference (ITC-Egypt) (pp. 1-5). IEEE.
- 29) Basha, H. A. M. A., Mohra, A. S. S., Diab, T. O. M., & El Sobky, W. I. (2022). Efficient image encryption based on new substitution box using DNA coding and bent function. IEEE Access, 10, 66409-66429.

- 30) Alsobky, W., Ismail, A., Mohra, A., Hassan, A., & Abdelaziem, A. (2022). Design and Implementation of Advanced Encryption Standard by New Substitution Box in Galois Field (**28**). *International Journal of Telecommunications*, 2(01), 1-11.
- 31) El Sobky, W., Hamdy, S., & Mohamed, M. H. (2021). Elliptic curve digital signature algorithm challenges and development stages. *Int. J. Innov. Technol. Exploring Eng.*, 10(10), 121-128.
- 32) F. E. Abd Elbary. "Image Encryption on Chaotic Maps: A Survey of Chaos Detection Algorithms." *IOSR Journal of Mathematics (IOSR-JM)*, 18(4), (2022): pp. 32-39
- 33) Maolood, A. T., Farhan, A. K., El-Sobky, W. I., Zaky, H. N., Zayed, H. L., Ahmed, H. E., & Diab, T. O. (2023). Fast Novel Efficient S-Boxes with Expanded DNA Codes. *Security and Communication Networks*, 2023.
- 34) Tamer O. Diab, Mofreh A. Hego, Wageda I. Al Sobky, Hany Nasry zaky, Salwa M. SeragEldin and Ahmed Khairy, "Fast Simple Image Encryption Technique Based on Chao Based Sytem", *International Conference of Telecommunication ITC Egypt 2023*.
- 35) S. M. SeragEldin, Musheer Ahmad, Ahmed H. Eldeeb, Tamer O.Diab, Wageda I. Al sobky, and Hany Nasry Zaky "Design and Analysis of New Version of Cryptographic Hash Function Based on Improved Chaotic Maps with Induced DNA Sequences," in *IEEE Access*, doi: 10.1109/ACCESS.2023.3298545.
- 36) Hala Saeed, Tamer O. Diab, M. S. Abdel-wahed, M. A. Elsis, Wageda I. El sobky, and Ahmed Khairy Mahmoud. " Famous Digital Signatures Used in Smart Contracts" ", *International Conference of Telecommunication ITC Egypt 2023*.