IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 3, Issue 12, December 2016

Algebraic Cryptanalysis of AES using Gröbner Basis

Ahmed A. Abdel-Hafez[1], Reda-Elbarkouky[2], Wageda_Hafez[3]

Department of Communication, Military Technical College, Egypt[1]

Department of Mathematics, Engineering Faculty, Ain Shams University, Egypt[2]

Department of Mathematics, Engineering Faculty, Benha University, Egypt[3]

Abstract: Algebraic cryptanalysis is a potentially powerful attack on symmetric key block ciphers. This paper presents Algebraic cryptanalysis on Rijndael AES, based on its rich algebraic structure. The paper begins by defining the mathematical model of AES then constructing a system of mostly nonlinear polynomial equations representing S-Box. Then applying a powerful algebraic tool; Gröbner basis; to overcome the nonlinearity features of S-Box. Finally, it shows that how applying Gröbner basis of AES constructs a spare matrix which makes the system easy to be solved. Moreover, we have proved the "Resistance of Algebraic Attack" RAA value ($\boldsymbol{\Gamma}$) has been reduced.

Keywords: Algebraic cryptanalysis, multivariate quadratic polynomial equation system, S-box, Gröbner bases, Rijndael AES, RAA.

I. INTRODUCTION

Block ciphers are an important and omnipresent building block of modern cryptography. In August 2000, the Belgianblock cipher Rijndael was selected as a winner to be the Advanced Encryption Standard (AES)[1]. This happened in an unprecedented way – an open contest with international participation was held by the NIST to find a successor for the 24-year old Data Encryption Standard (DES). Rijndael is a key-iterated block cipher with a very rich and strong algebraic structure. The block and key length are variable in steps of 32 bits between 128 and 256 bits. The only valid data block length for AES is 128 bits however; the key length for AES may be 128, 192 or 256 bits. For the Rijndael block cipher, two algebraic representations in the form of multivariate polynomial systems of equations have been proposed so far. Courtois and Pieprzyk[2]have demonstrated how to obtain over defined systems of quadratic equations over GF(2), while [3]have constructed an embedding for the AES called Big Encryption System (BES) for which a system of over defined quadratic equations over $GF(2^8)$ exists. A representation considering the output of the S-Box as a polynomial expression of the input over GF(2^8) has thus far been neglected because the polynomials in this case are of relatively high degree. Using this representation; the key recovery problem for the AES cipher with a key length of 128 bits can be described asa system of 200 polynomial equations of degree 254 and 152 linear equations.

This paper will shows that by choosing an appropriate term order and by applying linear operations only, a Gröbner basis for AES-128 from this system can be generatedwithout a single polynomial reduction.

The structure of this paper is as follows: in Section IIthe cryptanalysis types on AES will be discussed. While in Section III the basic structure of AES will be explained., in Section IVwe study the mathematical model of AES , Finally we generate the Grobner basis of AES then compute RAAand summarize the impact of our result in Section Vand conclude.

II. CRYPTANALYSIS OF RIJNDAEL

Cryptanalysis is a general tool which permits one to breach the security of a wide range of cryptographic schemes. This section discusses various types of AES Cryptanalysis.

- **Differential and linear cryptanalysis**

Differential and linear cryptanalysis are the two most powerful general purpose cryptographic attacks known up to date. Providing lower bounds for the complexity of these attacks was the main cryptographic criterion in the design of Rijndael. For Rijndael, an upper bound of $2^{150}$for the probability of any 4-round differential trail and of $2^{75}$for the correlation of any 4-round linear trail has been proven. In combination with the number of rounds in Rijndael, these bounds provide a high security margin against both differential and linear cryptanalysis [4]. Nowadays, a new block cipher is only taken seriously if it is accompanied with evidence that it resists differential and linear cryptanalysis. Naturally, differential and linear cryptanalysis approaches are not the only attacks that can be mounted against block ciphers.

Linear and differential attacks have been extended in several ways and new attacks have been published that are related to them. The best known extension is known as truncated differentials. They have been already taken into account in the design of Rijndael from the start. Other

DOI 10.17148/IARJSET.2016.31235

attacks use difference propagation and correlation in different ways. There exists an impossible differential attack on 5 rounds, requiring $2^{29.5}$ chosen plaintexts [5], 2^{31} encryptions, 2^{42} bytes of memory and 2^{26} time for pre-computation. This result was improved in [6] and lead to an attack on a 6 round version. The resistance against differential cryptanalysis is measured by $\delta(F)$.

Definition 1 . Assume $F(x) = \left(f_1(x), \dots, f_n(x)\right)$ From $GF(2)^n$to $GF(2)^n$ is a multiple output Boolean function, the differential uniformity is denoted by $\delta(F)$which is defined by

$$\delta(F) = \max|\{x: F(x) - F(X + \alpha) = \beta\}|$$

Where $\alpha \in GF(2)^n, \beta \in GF(2)^n, \alpha \neq 0$

Theorem1: AES S-box has $\delta(F) = 4$
Proof: see [7].
Its known that the minimum of $\delta(F)$ is 1,so thatAES S-box has a certain ability to resist against differential attack . While the resistance against linear cryptanalysis is measured by $N(F)$.

Definition 2.Assume $F(x) = \left(f_1(x), \dots, f_n(x)\right)$ From $GF(2)^n$to $GF(2)^n$ is a multiple output Boolean function, the nonlinearity is denoted by $N(F)$ which is defined by

$$N(F) = \min d\left(u.F(x), l(x)\right)$$

Where $u \neq 0 \in GF(2)^n$,$l(x) \in L_n(x)$ and $L_n(x)$ is the set of all linear function from $F(2)^n$to $GF(2)^n$, AES S-Box have $N(F) = 112$.Wen while[8] Pointed out that the $N(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$=$2^{8-1} - 2^{\frac{8}{2}-1} = 120$.
AES S-Box is not perfect nonlinearity function.

- **Square attacks**.

The most powerful cryptanalysis of Rijndael to date is the square attack. This is a chosen-plaintext attack that exploits the byte-oriented structure of the cipher and works on any cipher with a round structure similar to that one of Rijndael. It was first described in the paper presenting a predecessor of Rijndael, the block cipher Square [8] and since then, it is often referred to as the Square attack. Other names for this attack are 'saturation-attack' (proposed by Lucks in [9]).This attack can break a 7 rounds of Rijndael for 192 and 256-bit keys, i.e. AES-192 and AES-256, 'Integral Cryptanalysis' by L. Knudsen and D. Wagner [10] or 'Structural attacks' by A. Biryukov and A. Shamir [11] (neither of the two last papers describe an attack on Rijndael). The original square attack can break round-reduced variants of Rijndael up to 6 or 7 rounds faster than exhaustive key search. N. Ferguson et. al. [12] proposed some optimizations that reduce the work factor of the attack. So, this attack breaks 9-round AES-256 keys with 2^{77} plaintexts under 256 related keys, and 2^{224}encryptions.

- **Collision Attacks**.

This attack has been introduced by Gilbert and Minier in [13] and is still the best attack in the sense that it can break 7 rounds of AES-128, AES-192 and AES-256 (for 128-bit keys the authors claimed that the complexity of the attack is marginally lower than the complexity of an exhaustive key search).

- **Algebraic cryptanalysis**

Algebraic techniques have been successfully applied against a number of multivariate schemes and stream ciphers. Yet, their feasibility against block ciphers remains the source of much speculation. The goal of algebraic cryptanalysis is to break cryptosystems by using mathematical tools coming from symbolic computation and modern algebra. More precisely, an algebraic attack can be decomposed in two steps: first the cryptosystem and its specifics have to be converted into a set of multivariate polynomial equations, then the solutions of the obtained polynomial system have to be computed. The security of a cryptographic primitive thus strongly relies on the difficulty of solving the associated polynomial system. These attacks have been proven to be very efficient for both public key or symmetric cryptosystems;block and stream ciphers.

In this paper, the focus will be on the polynomial system solving part. It is well known that this problem is very difficult (NP-hard in general). However, for many instances coming from algebraic attacks, the resolution is easier than in the worst-case scenario. Gröbner bases, first introduced in [14], are a fundamental tool for tackling this problem the basic idea behind the algebraic attack is to set up a system of equations including key bits and output bits and then to solve this system to recover key or key stream information [15]. A system of linear equations may be solved by Gaussian elimination method or any other known method. However, a cipher algorithm may contain a non-linear part. In this case the equations will be non-linear. If the system of equations is clearly defined then the equation set can be solved using techniques such as linearization, or other methods such as Gröbner basis.

Since successful Gröbner basis attacks on block ciphers are possible, it must be studied carefully how Gröbner basis algorithms depend on the structure of polynomial systems corresponding to block ciphers. One of the possible approaches is based on the notation of semi-regular sequences of polynomials[15,16].

Using the AES as an example, we have considered three algebraic representations for block ciphers. It was proved (where?) that the BES and AES polynomial equations over $GF(2^8)$ are not semi-regular, and that the AES systems of quadratic equations over GF(2) are not semi-regular over GF(2).

III.The Basic Structure of the AES

Now consider the basic version of the AES, which encrypts a 16-byte block using a 16-byte key with 10 encryption rounds.The input to the AES round function can be viewed as a rectangular array of bytes or, equivalently, as a column vector of bytes. Throughout the encryption process this byte-structure is fully respected[17]. The AES specification defines a round in terms of the following three transformations

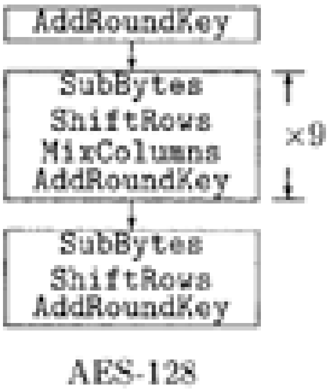


Figure1AES Encryption

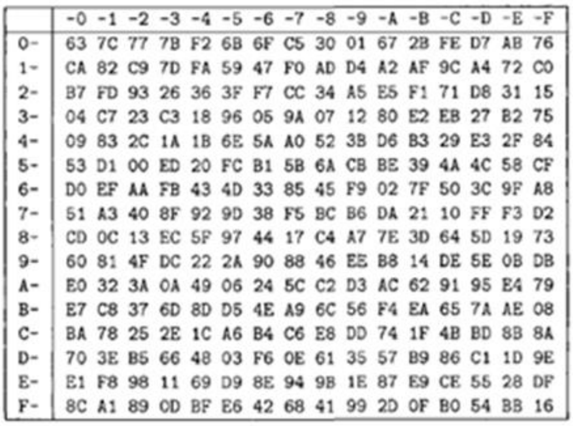
There are four basic operations when encrypting with the AES., operate on the state array of 16 bytes.

- **SubBytes** modifies the bytes in the array independently.
- **ShiftRows** rotates the four rows of the array independently.
- **MixColumns** modifies the four columns of the array independently.
- **AddRoundKey** adds the bytes of the round key and the array.

These basic operations form a typical round of encryption. A complete description of AES encryption requires an initial AddRoundKey ("Round 0") followed by NR rounds of computation, where N_r= 10, 12, or 14 for AES-128, AES-196, or AES-256 respectively. The last round of computation does not contain a MixColumns operation[18]. Each round of the AES is considered to have three parts. The first is Sub Bytes, in which a substitution is performed on each byte of the state array. This is termed the substitution layer. The second part is Shift Rows followed by Mix Columns, which gives diffusion across the state array. This is termed the diffusion layer. The final part of an AES round introduces key material by Add Round Key. This paper focus on the substitution layer

Substitution layer: The substitution layer is based on the AES S-box which is, in turn, can be defined by the composition of three operations:

Inversion: AES inversion operation is inversion in the field F, but extended so that 0 → 0. Thus, the input byte to the S-box is regarded as an element $w \in F$ and for $W \neq 0$ the output x satisfies $X = W^{-1}$ and wx = 1. We denote the extension to the case $W = 0\ by X = W^{-1}$ and give a look-up table in Figure 2



	-0	-1	-2	-3	-4	-5	-6	-7	-8	-9	-A	-B	-C	-D	-E	-F
0-	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1-	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2-	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3-	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4-	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5-	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6-	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7-	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8-	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9-	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A-	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B-	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C-	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D-	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E-	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F-	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 2 AES GF(2) linear mapping within S-box

The GF (2)- linear mapping is a linear transformation $A: GF(2)^8 \to GF(2)^8$specified by an 8x8 circulated matrixover GF(2). The result x of inversion is regarded as a vector in$GF(2)^8$ and the output y is given by $y = A(x)$

$$A(x)=La \times x + \text{'63'} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

This inversion is actually optimal with respect to several measures of non-linearity.Non-linearity is important to protect against several common families of attack, we apply an affine (over GF(2)) transformation. The affine transformation function A(x) is defined as:

$$A(x) = 05x^{FE} + 09x^{FD} + F9x^{FB} + 25x^{F\,7} + F4x^{EF} + 01x^{DF} + B5x^{BF} + 8Fx^{7F} + 63$$

Where, $x_i, (i = 0, \ldots, 7)$ are the bits of the byte $x_i$and x_7, is the most significant bit.

S-box constant. The output byte y of the GF(2)-linear mapping is regarded as an element of the Rijndael field F and added to the field element 63 to produce the output from the S-box. It has been proved that Rijndael has the immunity against differential attack and linear attack which are the most well-known attacks on block ciphers. Because of the simple algebraic structure of Rijndael S-box, many cryptanalysts focus on the algebraic attack which may be an efficient method. As the only nonlinear component of Rijndael is S-box and it is a crucial element. Recovering a key using a known plain-text attack is clearly an NP problem. So, as MQ is an NP-complete problem, in theory one should be able to reexpress AES key recovery as an MQ problem. Not all instances of an NP-complete problem are hard to solve, so perhaps the AES MQ problem would be more tractable than the key recovery problem in other guises. Courtois and Pieprzyk translated AES key recovery (indeed, key recovery for a general class of block ciphers) into an MQ problem over GF(2) in the following way[19,20]: Consider a single Rijndael S-box. This has one byte, x, of input and one byte, z of output. We may specify further and let y be the patched inverse of x, so y is x after inversion but before applying the affine transformation. The state starts out as the 128-bit input. We operate on the stateby performing successive rounds. A round is made up of three parts: application of the S-box, linear diffusion, and sub key addition.

IV. GENERATING S- BOX POLYNOMIALS

S-boxes or substitution boxes are common in block ciphers. These are bijective functions on the blocks that are, ideally, highly non-linear. Much of the security of block ciphers can be thoughtof as ‘residing’ in their S-boxes. S-box is the same in every round, and it acts independently on each byte. Cui et al. [21] (as Courtois and Pieprzyk [22] before them) utilize the Rijndael S-box composition of two functions to derive an MQ for it. With x,as an input, and z,as an output value, this leads to the first eight multivariate quadratic equations for Rijndael S-box. The authors give all the steps and in-between results of the complete length of the calculation. They formulate and evaluate two additional equations of the byte variables to define the S-box completely. Doing so, Cui et al.[20]replicate results already presented in 2002 by Courtois and Pieprzyk in the extended version of [21].Cui et al. derive multivariate quadratic equation coefficients of the polynomial expression of the S-box. They write up the equation system with indices for rounds and input bytes for the AES algorithm (without further using them) which will, for clarity, be omitted in what follows. As before, by x is denoted the input byte variable of the S-box function. Intermediate variables are denoted by y_0, y_1, . . . , y_{253} and the output variable by z, the S-box transformation can be described by the following quadratic equations over GF(2^8) :

$$0=x3+x5+x6+x1+x2z2+x5z7+x7z4+x7z1+x7z3+x0z1+x6z5+x6z3+x7z7+x4z6+x4z1+x4z5+x4z0+x4z2+x1z5+x1z3+x5z5+x5z3+x5z0+x3z1+x3z3+x6z6+x3z4+x2z3+x2z6+x4z7+x0z5+x0z3+x1z4+x1z7+x6z1+x3z0+x4z3+x0z7+x1z6+x2z5,$$

$$0=x3+x6+x1+x2z4+x5z1+x7z1+x5z6+x0z6+x0z4+x6z3+x6z4+x6z7+x7z7+x7z5+x7z2+x4z5+x4z0+x1z5+x1z3+x5z5+x5z3+x3z1+x3z3+x3z6+x2z1+x2z3+x4z7+x0z5+x0z3+x1z2+x6z1+x3z5+x3z0+x3z2+x4z3+x0z7+x3z7+x1z6+x2z0,$$

$$0=x3+x4+x5+x1+x2z2+x2z7+x5z1+x5z4+x5z7+x7z6+x7z4+x7z1+x0z6+x6z5+x6z2+x6z7+x7z7+x4z6+x4z1+x4z5+x1z3+x1z0+x5z3+x3z3+x2z1+x2z3+x2z6+x0z5+x0z3+x1z4+x6z1+x3z5+x3z0+x4z3+x0z2+x3z7+x1z1+x2z5+x2z0,$$

$$0=x3+x4+x1+x2z7+x5z1+x5z7+x7z4+x0z4+x0z1+x6z4+x6z7+x7z7+x7z5+x7z2+x4z4+x4z1+x1z5+x1z3+x1z0+x5z5+x3z1+x3z3+x3z6+x6z6+x5z2+x2z3+x4z7+x0z3+x0z0+x1z2+x1z7+x6z1+x3z5+x4z3+x1z1+x1z6+x2z5+x2z0,$$

$$0=x2+x6+x7+x1+x2z2+x5z1+x5z4+x7z4+x7z1+x5z6+x7z3+x0z6+x6z3+x6z2+x6z4+x6z7+x7z7+x7z2+x4z6+x4z0+x1z0+x5z5+x5z3+x5z0+x6z6+x2z1+x0z0+x1z4+x6z1+x3z0+x4z3+x0z2+x3z7+x1z6,$$

$$0=x2+x3+x4+x5+x1+x2z2+x2z7+x5z1+x5z4+x7z6+x7z1+x5z6+x0z6+x0z4+x0z1+x6z5+x6z2+x6z4+x6z7+x7z2+x4z4+x4z2+x1z5+x1z3+x5z5+x5z0+x3z1+x3z6+x6z6+x5z2+x3z4+x2z3+x2z6+x4z7+x0z5+x0z3+x0z0+x1z2+x1z4+x1z7+x0z7+x1z1+x1z6+x2z5+x2z0,$$

$$0=x0+x2+x3+x7+x2z4+x5z4+x5z7+x7z6+x7z1+x5z6+x0z6+x0z4+x0z1+x6z2+x7z7+x4z6+x4z4+x4z1+x4z5+x4z0+x4z2+x1z5+x1z3+x1z0+x5z5+x6z6+x5z2+x3z4+x2z1+x2z6+x7z0+x0z5+x0z3+x1z2+x1z7+x6z1+x3z2+x0z2+x0z7+x3z7+x1z6,$$

$$0=x3+x5+x2z4+x2z7+x5z1+x5z7+x7z6+x7z1+x5z6+x7z3+x0z6+x0z1+x6z5+x6z3+x6z0+x6z7+x7z5+x4z4+x4z1+x4z0+x1z5+x1z3+x5z5+x5z3+x5z0+x3z3+x3z6+x5z2+x2z3+x2z6+x0z0+x1z7+x3z5+x3z2+x4z3+x0z2+x1z1+x2z,$$

$$0=x5+x7+z7+z5+z3+z1+x5z1+x5z4+x7z3+x0z6+x0z4+x0z1+x6z3+x7z2+x4z4+x4z2+x1z5+x1z0+x5z3+x6z6+x3z4+x2z3+x4z7+x7z0+x6z1+x3z7+x2z5+x2z0,$$

$$0=x3+x5+x7+z6+z7+z5+z4+z3+x2z2+x2z4+x2z7+x7z1+x6z5+x6z0+x6z2+x6z4+x7z7+x7z2+x4z6+x4z1+x5z3+x5z0+x3z1+x3z3+x6z6+x5z2+x3z4+x0z5+x0z3+x0z0+x1z4+x1z7+x6z1+x4z3,$$

$$0=x3+x5+x6+x7+x1+z6+z5+z3+z2+x5z1+x5z7+x7z6+x7z1+x0z4+x6z5+x6z3+x6z0+x6z7+x4z6+x4z4+x4z1+x4z5+x4z0+x4z2+x1z3+x3z3+x6z6+x5z2+x2z1+x2z3+x2z6+x7z0+x1z4+x3z0+x3z2+x0z2+x0z7+x1z1,$$

$$0=x3+x4+x5+x1+z4+z3+z1+z0+x2z2+x2z4+x5z1+x5z6+x0z6+x0z1+x6z5+x6z2+x6z4+x6z7+x7z7+x7z5+x4z6+x4z5+x4z0+x1z3+x1z0+x5z0+x3z1+x6z6+x2z1+x2z6+x4z7+x7z0+x0z3+x1z2+x3z2+x4z3+x3z7+x2z5+x2z0,$$

$$0=x2+x3+x5+x6+x1+z6+z2+z0+x2z7+x5z1+x5z4+x5z7+x7z6+x7z4+x7z3+x6z5+x7z7+x7z2+x4z6+x4z5+x1z5+x1z0+x5z5+x5z3+x5z0+x3z1+x3z6+x6z6+x3z4+x2z6+x7z0+x0z5+x0z0+x1z2+x1z7+x6z1+x3z0+x0z2+x3z7+x1z1,$$

$$0=x0+x3+x4+x5+x1+z6+z7+z5+z4+z3+z1+z0+x5z1+x5z7+x7z4+x5z6+x0z4+x0z1+x6z5+x6z3+x6z0+x6z4+x7z7+x7z5+x4z6+x4z4+x4z1+x4z5+x4z2+x1z5+x5z0+x3z1+x3z3+x6z6+x5z2+x2z3+x2z6+x4z7+x7z0+x1z4+x1z7+x6z1+x3z5+x3z0+x0z7+x1z1+x1z6+x2z0,$$

$$0=x2+x3+x7+x1+z6+z7+z5+z4+z3+z2+z1+1+x2z2+x2z4+x2z7+x5z4+x5z7+x7z1+x7z3+x0z6+x6z5+x6z3+x6z0+x6z2+x6z4+x6z7+x7z7+x4z6+x4z4+x4z1+x4z5+x4z0+x1z5+x1z3+x1z0+x5z5+x5z0+x3z1+x3z6+x2z1+x2z6+x0z3+x0z0+x3z0+x3z2+x4z3+x3z7+x1z1+x2z5,$$

$$0=x0+x7+x1+z6+z2+z1+z0+1+x2z4+x5z4+x5z7+x7z4+x7z1+x7z3+x6z2+x6z4+x6z7+x4z5+x4z0+x1z5+x2z1+x2z6+x0z5+x1z2+x1z7+x3z5+x3z0+x4z3+x0z2+x0z7+x1z1+x1z6$$

V. CONSTRUCTION OF THE GRÖBNER BASIS

One way to solve a system of polynomial equations is to construct a new system of polynomial equations with the same solutions as the initial one, but with a simpler structure and then solve this “simpler” system .This method is based on polynomial ideal theory and

DOI 10.17148/IARJSET.2016.31235

multivariate polynomial division and then generates special bases of these ideals, called Gröbner bases. The algorithm is based on the construction of S-polynomials and on polynomial division of these S-polynomials [22,23]. Multivariate polynomial division requires a monomial ordering and different orderings can give rise to radically different Gröbner bases.

Definition 1: (Ideal)[23] The ideal defined by a set of polynomials $F = \{f_1, \dots, f_m / f_i \in \mathbb{F}[x_1 \dots, x_n]\}$ is the set of all polynomials that can be generated as polynomial combinations of the initial polynomials $f_1, \dots, f_m$

$$I = \{\sum_{i=1}^{m} f_i h_i : h_i \in \mathbb{C}[x_1 \dots, x_n]\}$$

Where h_i are arbitrary polynomials from$\mathbb{F}[x_1 \dots, x_n]$.

Definition2:[24] (Lexicographic ordering) let x^α and x^β be some monomials.we say $x^\alpha >_{lex} x^\beta$ if,in the difference $\alpha - \beta \in \mathbb{Z}^n$, the left most nonzero entry is positive.

Definition3:[24] (Graded Reverse lexicographic ordering)) let x^α and x^β be some monomials. we say $x^\alpha >_{grevlex} x^\beta$ if$\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i$ or if $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ and the difference $\alpha - \beta \in \mathbb{Z}^n$, the right most nonzero entry is negative.

Definition 4: [24](S-Polynomial) let $f, g \in \mathbb{F}[x_1 \dots, x_n]$ be non zero polynomials and $>$
Some fixed monomial ordering on $\mathbb{F}[x_1 \dots, x_n]$.
The S-Polynomial of f and g, denoted $S\,(g_p, g_q)$, is the polynomial

$$S\,(g_p, g_q) = \frac{LCM(LM(g_p), LM(g_q))}{LT(g_p)} g_p - \frac{LCM(LM(g_p), LM(g_q))}{LT(g_q)} g_q$$

Where $LCM(LM(g_p), LM(g_q))$ is the least common multiple of the monomial $LM(g_p)$ and $LM(g_q)$.Theabove mentioned definition indicates that S-polynomials are cross product of leading terms and are constructed to cancel leading terms. The leading terms of the two components of $S(g_p, g_q)$ are equal and therefore, cancel each other.

Example: Let G=$\{g_1, g_2\}$ where $g_1 = xy^2z - xyz$ and $g_2 = x^2yz - z^2$.These polynomial are ordered with respect to Lex order .$LM(g_1) = xy^2z$, $LM(g_2) = x^2yz$ so $LCM(LM(g_1), LM(g_2)) = x^2y^2z$ .then $S\,(g_1, g_2) = \frac{x^2y^2z}{xy^2z} g_1 - \frac{x^2y^2z}{x^2yz} g_2$
$= -x^2yz + yz^2$.

Theorem 1: (Buchberger's criterion)
A finite set of polynomials $\underline{G = \{g_1, \dots, g_l\}}, G \subset I$ isa Gröbner basis of I if and only if $\overline{S(g_p, g_q)}^G = 0$ for all pairs $i, j \in 1, \dots, t, i \neq j$.

Proof: The proof of this theorem can be found in [24]
The simplest version of the Buchberger's algorithm for computing a Gröbner basis of a givenideal is based on this criterion.The main problem of AES was nonlinearity of S-Box and no non-zero linear structure

Theorem 4 [25]:AES S-Box has no non zero linear structure.

Proof: suppose that, on the contrary,AESS-Boxhas no non zero linear structure. in this case , let $c \neq 0$ satisfies $(La * (x + c)^{-1} + 63) + (La * x^{-1} + 63) = \beta$ where β is a constant .it is immediately obvious that $La * (x + a)^{-} + La * x^{-1} = \beta$. let $x = 0$
we can obtain $\beta = La * c^{-1}$, therefore, we have $(La * (x + c)^{-1} + 63) + (La * x^{-1} + 63) = La * c^{-1}$
since$\det(La) \neq 0$, thus $(x + c)^{-1} = x^{-1} + c^{-1}$ however , according to the principle of taking multiplicative inverse , it is obvious that$(x + c)^{254} = x^{254} + c^{254}$,i.e., $(x + c)^{-1} \neq x^{-1} + c^{-1}$ then there exist a contradiction between $(x + c)^{-1} = x^{-1} + c^{-1}$ and $(x + c)^{-1} \neq x^{-1} + c^{-1}$ therefore AES S-Box has no non zero linear structure.
Now our focus in this paper will appear, Gröbner basis is efficient tool to overcome the nonlinearity of S-Box also after applying Gröbner basis the RAA will be reduced , in the previous section the system of S-Box algebraic equations was introduced by applying the Buchberger's theorem with Lexicographic ordering we obtain these results

Our Results can be expressed as follows
{x0,x0z0,x0z1,x0z2,x0z3,x0z4,x0z5,x0z6,x0z7,x1,x1z0,x1z1,x1z2,x1z3,x1z4,x1z5,x1z6,x1z7,x2,x2z0,x2z1,x2z2,x2z3,x2z4,x2z5,x2z6,x2z7,x3,x3z0,x3z1,x3z2,x3z3,x3z4,x3z5,x3z6,x3z7,x4,x4z0,x4z1,x4z2,x4z3,x4z4,x4z5,x4z6,x4z7,x5,x5z0,x5z1,x5z2,x5z3,x5z4,x5z5,x5z6,x5z7,x6,x6z0,x6z1,x6z2,x6z3,x6z4,x6z5,x6z6,x6z7,x7,x7z0,x7z1,x7z2,x7z3,x7z4,x7z5,x7z6,x7z7,z0,z1,z2,z3,z4,z5,z6,z7}]
{{0, 1, 2, -1, 0, 0, -1, -2, 0, 0, 0, 0, 0, 0, 0, 1, 1, 2, 0, -1, -2, 0, 0, -1, 1, 0, 0, 0, -1, 1, -1, 0, 1, -1, 0, -2, 0, 0, 1, 1, 0, 1, -1, 0, 1, 0, 1, -1, 1, -1, -1, 1, -1, 1, 0, 0, 0, -1, 0, 0, 0, 2, -1, 0, 0, -1, 0, 1, 1, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0}, {0, 4, 0, 5, -5, 0, -5, 5, -3, 0, 1, 4, -1, 0, -2, 1, -1, -1, 0, 1, 2, -3, 2, 3, 0, 0, 2, 0, 1, -3, 4, 2, -6, 6, 4, 2, 0, 3, 0, -4, 3, 3, -2, -2, -2, 0, 2, 7, 2, 3, 0, 2, 6, 1, 0, 4, -1, -1, 5, 2, 0, -3, 6, 0, 0, 1, 1, 3, 0, 6, 2, -1, 1, 1, 0, 0, 0, 0, 0, 0}, {0, -8, 0, -8, 8, 1, 8, -7, 4, 0, 1, -7, 4, 0, 0, -1, 0, 0, 0, 0, -2, 3, -4, -4, 0, 0, -4, 0, -2, 5, -5, -5, 10, -10, -6, 0, 0, -5, -2, 6, -6, -5, 5, 3, 4, 0, -5, -10, -5, -5, 1, -4, -10, -2, 0, -8, 2, 1, -9, -4, -1, 5, -10, 0, 3, -4, -1, -5, -1, -9, -3, 2, 0, 0, 1, 1, 0, 0, 0, 0}, {0, 7, 0, 5, -6, -2, -7, 6, -2, 0, -4, 4, -4, 0, 2, -1,

1, 0, 0, -1, 2, 0, 2, 5, -1, 0, 2, 0, 1, -3, 5, 4, -9, 7, 4, -2, 0, 6, 1, -5, 6, 3, -5, -2, -3, 0, 7, 7, 5, 3, -3, 3, 11, -1, 0, 8, -4, 1, 8, 6, 2, -4, 9, 0, -4, 5, 0, 3, -1, 8, 1, -2, 0, 0, -2, 0, 2, 0, 0, 0}, {0, 6, 0, 5, -7, 2, -7, 7, 0, 0, -5, 6, -3, 1, 1, 1, 1, -1, 0, 1, 2, -3, 5, 4, -1, 0, 2, 0, 1, -4, 6, 4, -9, 8, 6, -2, 0, 5, 0, -3, 3, 6, -5, -5, -2, 0, 4, 9, 6, 2, -2, 3, 11, -1, 0, 8, -5, -1, 9, 5, 1, -5, 10, 0, -3, 5, 1, 2, -3, 8, 3, -5, -1, 0, -1, 0, 0, 1, 0, 0}, {0, -7, 0, -9, 10, 0, 11, -8, 2, 0, 4, -8, 4, -2, 0, 1, 1, 2, 0, 1, -4, 4, -4, -5, 1, -2, -2, 0, -1, 7, -9, -4, 13, -9, -6, 2, 0, -8, -1, 5,

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

-4, -7, 5, 4, 5, 0, -5, -11, -7, -1, 3, -3, -13, -1, 0, -10, 8, 1, -10, -4, -2, 6, -13, 0, 2, -5, 2, -3, 3, -10, -5, 6, 0, 0, 0, 0, 0, 0, 0, 2}, {0, 1, 0, 1, -1, -1, -1, -2, -2, 0, 2, 1, 0, -1, -1, 0, -1, 1, 0, -1, -1, -1, -1, -1, 0, 0, 1, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, -1, 1, -1, 0, 0, 0, 1, -1, 0, 0, 0, 0, 0, 0, 0, -2, 2, 0, 0, 1, -1, -1, -1, 0, 1, -1, 0, 1, -2, 0, 1, 2, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0}, {0, 3, 0, 5, -2, -2, -3, 2, -4, 0, 4, 2, -2, 0, 0, -1, -1, 0, 0, -1, 2, 0, 0, 1, 1, 0, 2, 0, 1, -3, 1, 2, -3, 3, 0, 2, 0, 2, 3, -3, 4, 1, -1, 2, -3, 0, 1, 3, 1, 3, 1, 1, 1, 3, 0, 2, 2, 1, 2, 0, 0, 0, 3, 2, 0, 1, 0, 3, 3, 2, 1, 2, 0, 0, 0, 0, 0, 0, 0, 0}, {0, 2, 0, 5, -4, -2, -5, 1, -5, 0, 5, 2, -3, -1, -1, -1, -2, -1, 0, -1, 1, -2, 0, -1, 0, 0, 1, 0, 2, -3, 1, 2, -4, 3, 0, 3, 0, 1, 3, -3, 2, 1, 0, 3, -3, 0, 1, 4, 0, 3, 0, 1, 1, 4, 1, 2, 3, -2, 3, -2, 0, 0, 1, 0, 2, -2, -1, 3, 4, 3, 1, 3, 1, 0, 0, 0, 0, 0, 0, 0}, {0, -1, 0, 1, 0, -2, 1, 0, 0, 0, 0, 0, -2, 0, 2, -1, -1, 0, 0, -1, 0, 2, 0, -1, 1, 2, 0, 0, 1, -1, -1, 0, 1, -1, -2, 0, 0, 0, 1, 1, 0, -1, 1, 2, -1, 2, 1, -1, -1, 1, 1, -1, -1, 1, 0, 0, 0, 1, 0, -2, 2, 0, -1, 0, 0, 1, -2, 1, 1, -2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0}, {0, 5, 0, 11, -8, -4, -11, 2, -12, 0, 12, 6, -6, -2, -2, -3, -5, -2, 0, -1, 2, -4, 0, -3, 1, 0, 4, 0, 3, -7, 1, 4, -9, 7, 0, 6, 2, 0, 7, -7, 4, 3, -1, 6, -7, 0, 1, 9, 1, 5, 1, 1, 1, 9, 0, 4, 6, -3, 4, -4, 0, 0, 3, 0, 4, -5, -2, 5, 9, 6, 3, 6, 2, 0, 0, 0, 0, 0, 0, 0}, {0, 1, 0, 1, 0, 1, 0, 2, 0, 0, 0, 1, 1, 1, -1, 1, 0, 0, 0, 1, 1, -1, 1, 2, 0, 0, 1, 1, 0, 0, 2, 1, -1, 2, 2, 1, 0, 1, 0, -1, 1, 1, 0, -1, 0, 0, 0, 2, 1, 1, 0, 1, 2, 0, 0, 1, 0, 0, 1, 1, 0, -1, 2, 0, 0, 1, 1, 0, -1, 2, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0}, {0, 1, 0, -1, 0, 2, 1, 2, 2, 0, -2, 0, 2, 0, 0, 1, 1, 0, 2, 1, 0, 0, 0, 1, -1, 0, 0, 0, -1, 1, 1, -2, 1, -1, 2, 0, 0, 0, -3, 1, -2, 1, -1, -2, 1, 0, 1, 1, 1, -1, 1, 1, 3, -3, 0, 0, -2, 1, 0, 2, 0, 0, 1, 0, 0, 1, 2, -1, -3, 0, 1, -2, 0, 0, 0, 0, 0, 0, 0, 0}, {0, -3, 0, -6, 5, 2, 6, -2, 6, 1, -5, -3, 3, 1, 2, 1, 3, 1, 0, 1, -1, 3, 0, 0, 0, 0, -2, 0, -1, 4, -2, -2, 5, -4, -1, -3, 0, -1, -3, 4, -2, -2, 1, -2, 4, 0, -1, -5, -1, -3, 0, -1, -2, -4, 0, -3, -2, 2, -3, 2, 0, 1, -2, 0, -2, 2, 1, -3, -3, -4, -2, -2, -1, 0, 0, 0, 0, 0, 0, 0}, {2, -7, 0, -3, 4, 0, 5, -4, 4, 0, 0, -4, 0, 0, 2, -1, 1, 0, 0, -1, 0, 2, -2, -3, -1, 2, -4, 0, 1, 1, -3, -2, 5, -5, -6, 0, 0, -2, 1, 5, -4, -3, 5, 4, 1, 0, -3, -7, -3, -3, 1, -3, -5, 1, 0, -4, 2, 1, -4, -4, 0, 2, -7, 0, 2, -1, -4, -3, 1, -6, -1, 2, 0, 0, 0, 0, 0, 0, 0, 0}}

After notice this result zeros can be seen as majority in our work which means S-box can be spare matrix and the order of nonlinearity reduced which make S –box easy to be solved which was the big problem for breaking AES system now no problem for any number of rounds AES as a total system become linear.Another advantage can be appears after applying Gröbner basis; which is reducing RAA "Resistance of AlgebraicAttacks".The value of this reducing can be defined by Γ.

Definition [26]:given r equations of t monomials in $GF(2)^8$resistance of algebraic attacks is defined by

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

For AES t=81,r=23,n=8 we can obtain $\Gamma \approx 2^{22.9}$ .jung[24] claimed Γ should be greater than2^{32} for secure ciphers . WhileAES S-Box has $\Gamma \approx 2^{22.9}$, it can be a weakness of AES. So we can try to conduct our attack and apply Gröbner method to reduce RAA our results makes t=80,r=24,n=8andthen $\Gamma \approx 2^{19.8}$ also from these result there exist spare matrix which proves that our result are true. Now we can reformulate the results in the following figure hence white colour express zero number.

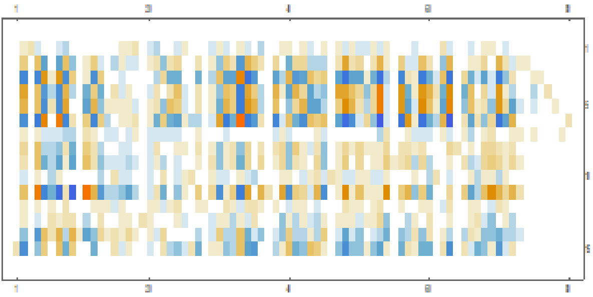


Figure 3 Gröbner result as a matrix

VI. CONCLUSION

In this paper we discussed various types of cryptanalysis techniques.We have demonstrated that Gröbnerbasis algorithms can be used to successfully breaking nonlinearity of S-Box which considered as being a big problem to attack AES even when they are practically secure against differential and linear cryptanalysis. We have demonstrated that Gröbnerbases for ciphers that follow our construction principle can be calculated by hand. These Gröbner bases are relative to a lexicographical order and thus do not give the solution to the polynomial system directly. However, our contribution shows that the problem of breaking AES can be reduced to a Gröbner basis conversion,by giving a closed formula for the ideal of all S-Box polynomials. This allowed us to determine solution of the total system as nonlinearity is decreased,now it is become easy to break any number of rounds

REFERENCES

[1] J. Daemen and V. Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard." Springer-Verlag, 2002

[2] Nicolas T. Courtois and Josef Pieprzyk. "Cryptanalysis of block ciphers with overdefined systems of equations" . In YuliangZheng, editor, Proceedings of Asiacrypt'02, Lecture Notes in Computer Science. Springer-Verlag, 2002.

[3] W. Millan. "How to improve the nonlinearity of bijective s-boxes". In Australian Conference on Information Security and Privacy 1998, volume 1438, pages 181{192. Springer Verlag, 1998.

[4] MagaliBardet, Jean-Charles Faug`ere, Bruno Salvy, and Bo-Yin Yang." Asymptotic Behaviour of the Degree of Regularity of Semi-Regular Polynomial Systems". In P. Gianni, editor, Mega 2005, 2005.

[5] L. R. Knudsen. Contemporary Block Ciphers. In I. Damg°ard, editor, Lectures on Data Security. Modern Cryptology in Theory and Practice, volume 1561 of LectureNotes in Computer Science, pages pp. 105–126. Springer Verlag Heidelberg, 1999.

[6] EladBarkan and Eli Biham. In how many ways can you write Rijndael? In YuliangZheng, editor, Proceedings of Asiacrypt'02, Lecture Notes in Computer Science. Springer-Verlag, 2002. Also a NESSIE report.

[7] Eli Biham and Nathan Keller. Cryptanalysis of reduced variants of RIJNDAEL. In Proceedings of the Third Advanced Encryption Standard Conference. NIST, April 2000.

[8] Jung HeeCheon, MunJu Kim, Kwangjo Kim, Jung-Yeun Lee, and SungWoo Kang." Improved Impossible Differential Cryptanalysis of SBox and its performance analysis". In K. Kim, editor, Information Security and Cryptology - ICISC 2010, number 2288

DOI 10.17148/IARJSET.2016.31235

in Lecture Notes in Computer Science, pages 39–49. Springer, 2010.

[9] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. In Birgit Pfitzmann, editor, Proceedings of Eurocrypt'01, number 2045 in Lecture Notes in Computer Science, pages 394–405. Springer-Verlag, 2001.

[10] D. Coppersmith. XSL against Rijndael. CRYPTO-GRAM, October 2002. Cop02b, Don Coppersmith. Impact of Courtois and Pieprzyk results. NIST AES Discussion Forum, September 2002. Available from http://www.nist.gov/aes.

[11] Joan Daemen and Vincent Rijmen. The Design of Rijndael. Information Security and Cryptography. Springer Verlag, 2002.

[12] N. Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, M. Stay, D. Wagner, David Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, Proceedings of Fast Software Encryption – FSE'00, number 1978 in Lecture Notes in Computer Science, pages 213–230. Springer-Verlag, 2000.

[13] ZazunaKukelova, Algebraic Methods in Computer vision, Doctoral thesis Czech Technical Universtyinpragne, Feb 2013

[14] ChengqingLi, ―Cryptanalysis of Some Multimedia Encryption Schemes‖,IEEE transactions on multimedia ,vol.10,no.3,2008.

[15] B. Buchberger. Bruno buchberger'sphd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. Journal of Symbolic Computation, pages 475–511, 2006.

[16] J. Daemen and V. Rijmen. Rijndael. Submission to NIST AES Process, 1997.http://csrc.nist.gov/CryptoToolkit/aes/.

[17] J. Daemen and V. Rijmen. Answer to "New Observations on Rijndael". Submission to NIST AES Process, 2000. http://csrc.nist.gov/CryptoToolkit/ aes/.

[18] J. Daemen and V. Rijmen. The Design of Rijndael. Springer-Verlag, 2002.

[19] National Institute of Standards and Technology. Advanced Encryption Standard. FIPS 197. 26 November 2001.

[20] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. IACR eprint server http://www.iacr.org, April 2002.

[21] Nicolas T. Courtois and Josef Pieprzyk, Cryptanalysis of Block Ciphers with Overdefined Systems of Equations, Proc. of Asiacrypt 2002, LNCS 2501, Springer-Verlag, 267–287, 2002.

[22] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations,. In Asiacrypt 2002, Volume 2501 of Lecture Notes in Computer Science, pages 267-287, Springer-Verlag.

[23] Jie Cui, Hong Zhong, Jiankai Wang and Runhua Shi, "Generation and Optimization of Rijndael S-box Equation System", Information Technology Journal, 13: 2482–2488, 2014.

[24] MagaliBardet, Jean-Charles Faug`ere, and Bruno Salvy. Complexity of Gr¨obner Basis Computation for Semi-Regular Overdetermined Sequences over GF(2) with Solutions in GF(2). Technical Report RR-5049, INRIA, 2003.

[25] Jie Cui, Liusheng , Hong Zhong , Chang and Wei Yang ,"An Improved AES-S Box And Its Performance Analysis" International Journal of Innovative Computing information and Control, volume 7 ,number 5 A, MAY 2014

[26] A.M.Leventi-Peetz and J.V.Peetz, "Generating S Box Multivariate quadratic equation Systems and Estimating Algebraic Attack Resistance Aided by Sage Math "GodesbergerAllee 185-18, DE-53175 Bonn, Germany ,June ,2015