THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 16, Special Issue 2015, pp. 339-344

CONSIDERATIONS ABOUT THE POSSIBILITIES TO IMPROVE AES S-BOX CRYPTOGRAPHIC PROPERTIES BY MULTIPLICATION

Florin MEDELEANU[1], Ciprian RACUCIU[2], Marius ROGOBETE[3]

[1]Ministery of National Defense, Romania
[2]Titu Maiorescu University, Romania
[3]Alstom GRID Romania, Romania
E-mail: fmedeleanu@dcis.ro

The algorithm Rijndael was tested and chosen as the Advanced Encryption Standard (AES) in 2001, at the end of a security evaluation that lasted for years. Testing and evaluation process proved the algorithm's strength and efficiency. The algorithm AES is a block cipher with a SPN (Substitution Permutation Network) structure. The cornerstone of the algorithm's security is the substitution box (S-box) and its strength relies on its special algebraic construction which uses mixed operation in different order Galois Fields (base field and extended field). This paper is a study on the possibilities to improve some cryptographic properties of Rijndael Substitution box and the effect of these changes.

Key words: S-box, Galois Field factoring, non-linearity, algebraic expression.

1. INTRODUCTION

The algorithm Rijndael was developed by Joan Daemen and Vincent Rijmen, and was selected by National Institute of Standards and Technology (NIST) as standard encryption algorithm (Advanced Encryption Standard - AES) in 2001. The algorithm is a symmetric block cipher based on a substitution-permutation network (SPN). AES has long been a subject of interest for developers, cryptanalysts and the researchers, due to following:

– Security: the algorithm was extensively tested for long period of time (4 years, by NIST, in order to be adopted as a standard and 14 years, by the academic community, since the adoption as standard). During the evaluation, the algorithm was tested against linear and differential cryptanalysis attacks. The exceptional resistance against these attacks was obtained by so called „design by cryptanalysis" technique. This design approach means that the developers intended to create an algorithm especially resistant to some specific attacks, in this case linear and differential cryptanalysis attacks.

– Speed: AES is the fastest algorithm compared to other block algorithm offering the same level of cryptographic strength.

– Simplicity: The structure of the algorithm is easy to understand and can be easily decomposed in parts to be analyzed and evaluated.

2. THE STRUCTURE OF AES

The algorithm AES is fully described in FIPS-PUB-197 standard. For the sake of completeness, a brief description of the algorithm presenting the main parameters will also be given here. AES is a key-iterated block cipher composed of repeated application of round transformations on the data block. The block length size of AES is 128 bit length and there are three variants of the algorithm, with various key sizes: 128, 192 and 256 bits. The input and output of AES are considered one-dimensional arrays with the dimension of 8-bit bytes. For the encryption operation the inputs are the plaintext block and the key, and the output is the ciphertext block. For the decryption operation the inputs are the ciphertext block and the key, and the output

is the plaintext block. The round transformation of AES operates on an intermediate result named *state*. The state is interpreted as a rectangular matrix of bytes having 4 rows and a number of columns N_b which is equal to the block length (128) divided by 32, hence 4 columns. The key is mapped onto a two-dimensional cipher key. The cipher key is also a rectangular array with four rows similar to the state. The number of columns of the cipher key is denoted by N_k and is equal to the key length (128, 192 or 256) divided by 32, hence 4, 6 or 8 columns. The bytes of the key are mapped onto the bytes of the cipher key in the order: $k_{0,0}$, $k_{1,0}$, $k_{2,0}$, $k_{3,0}$, $k_{0,1}$, $k_{1,1}$, $k_{2,1}$, $k_{3,1}$, $k_{0,2}$…

p_0	p_4	p_8	p_{12}
p_1	p_5	p_9	p_{13}
p_2	p_6	p_{10}	p_{14}
p_3	p_7	p_{11}	p_{15}

k_0	k_4	k_8	k_{12}	k_{16}	k_{20}
k_1	k_5	k_9	k_{13}	k_{17}	k_{21}
k_2	k_6	k_{10}	k_{14}	k_{18}	k_{22}
k_3	k_7	k_{11}	k_{15}	k_{19}	k_{23}

Fig.1 – The state and the key (N_b =4 and N_k =6).

The AES has a number of rounds indicated by N_r which depends on the size of the key. For key sizes of 128, 192 or 256 bits, the number of rounds is respectively 10, 12 or 14. The AES encryption process is composed of the initial key addition, denoted by *AddRoundKey*, followed by N_r – 1 applications of the transformation *Round*, and finally one application of *FinalRound*. The initial key addition and every round take as input the *State* and a round key. The round key for round *i* is denoted by *ExpandedKey* [*i*], and *ExpandedKey* [0] denotes the input of the initial key addition. The derivation of *ExpandedKey* from the *CipherKey* is denoted by *KeyExpansion*.

The round transformation is denoted *Round*, and is a sequence of four transformations, called steps. The final round of the cipher is slightly different, it is denoted *FinalRound*, and is a sequence of three steps instead of four steps. Below, in the form of command script, there are described the operations of rounds that operates on arrays to which pointers (*State*, *ExpandedKey*[*i*]) are provided.

```
Round (State, ExpandedKey[i])
{
        SubBytes (State);
        ShiftRows (State);
        MixColumns (State);
        AddRoundKey (State, ExpandedKey[i]);
}
FinalRound (State, ExpandedKey [Nr])
{
        SubBytes (State);
        ShiftRows (State);
        AddRoundKey (State, ExpandedKey [Nr]) ;
}
```

The transformation SubByte (Substitution of Bytes) is the only non-linear step of the cipher. *SubByte* is a layer of permutation consisting of S-box applied bytes of the state. The figure 2 describes the effect of *SubByte* transformation to the state. The designers of the AES applied the following design criteria for S-box, as follows:

1. Non-linearity

a) Correlation. The maximum input-output correlation amplitude must be as small as possible.

b) Difference propagation probability. The maximum difference propagation probability must be as small as possible.

2. Algebraic complexity. The algebraic expression of Substitution of Bytes operation (S_{RD}) in GF(2^8) has to be complex.

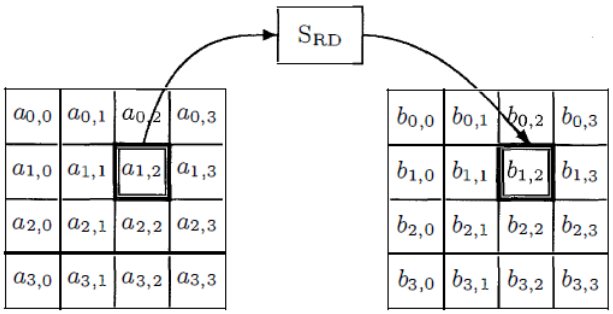

Fig. 2 – SubByte operation on the state.

The AES S-box was chosen being defined by the following function in GF(2^8) :

$$g : a \rightarrow b = a^{-1}. \tag{1}$$

In the formula (1), the elements of GF(2^8) are considered to be polynomials having a degree smaller than eight, with coefficients in the finite field GF(2). By definition, the multiplication is done modulo the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$, and the multiplicative inverse a^{-1} is defined accordingly. The value 00 is mapped onto itself. By definition, g has a very simple algebraic expression, that is $g = x^{254}$. This simple expression could allow algebraic manipulations to be used to effectuate algebraic attacks on the cipher. Therefore, the authors of the AES built the S-box as the sequence of g and an invertible affine transformation f. The affine transformation f has no impact on the non-linearity properties, but if it is properly chosen, it allows S_{RD} to have a complex algebraic expression. The authors have chosen an affine transformation that has a very simple description, but a complicated algebraic expression if it is combined with the transformation g.

3. THE ALGEBRAIC EXPRESSION OF THE AES S-BOX

In [1], the authors present five methods to find the algebraic expression of Rijndael S-box. These methods are as follows:

(1) Lagrange formula;
(2) Partition equivalence;
(3) Solve the equations of the polynomial base;
(4) Solve the dual trace of natural base;
(5) Solve the q-polynomial.

The authors of the present paper started to find the algebraic expression by using the Lagrange interpolation formula in finite fields. In order to do this, having in mind the high complexity of the calculus involved, the authors developed a program in Mathematica ®. They noticed that for polynomial expression that has to approximate more than 13 points, the calculus complexity is too high and the program cannot cope with it. So they changed the approach and made the decision to find the algebraic expression of AES S-box through solving a linear system with coefficients in GF(2^8). For this purpose, the authors also developed a program in Mathematica ® to solve the linear equation system described below. An algebraic expression that describes any transformation in finite fields, including an S-box, has the general expression:

$$SB(x) = b_0 + b_1 \cdot x + b_2 \cdot x^2 + b_3 \cdot x^3 + \ldots + b_{253} \cdot x^{253} + b_{254} \cdot x^{254} + b_{255} \cdot x^{255} . \tag{2}$$

By setting all possible values for $x \in$ GF(2^8) and considering the coefficients $\{b_0, b_1 \ldots b_{255}\}$ as variables, it is obtained the linear system with coefficients in GF(2^8):

$$\begin{cases} b_0 + \quad 0 + ... \quad +0 \quad +0 \quad = 63 \\ b_0 + \quad b_1 + ... \quad +b_{254} \quad +b_{255} \quad = 7C \\ b_0 + \quad b_1 \cdot 02 + ... \quad +b_{254} \cdot 02^{254} \quad +b_{255} \quad = 77 \\ ... \\ b_0 + \quad b_1 \cdot FE + ... \quad +b_{254} \cdot FE^{254} \quad +b_{255} \quad = 16 \end{cases} \tag{3}$$

Many papers, including [1] and [2] give the expression of the AES- GF S-box, in the form:

$f_{RD}(x) = 05 \cdot x^{254} + 09 \cdot x^{253} + F9 \cdot x^{251} + 25 \cdot x^{247} + F4 \cdot x^{239} + 01 \cdot x^{223} + B5 \cdot x^{191} + 8F \cdot x^{127} + 63$ (4)

Solving the linear system (3) the coefficients b_0, b_1 … b_{255} of algebraic expression of the S-box are found easily. For example, solving the system (3) for unmodified AES S-box, the coefficients $\{b_0, b_1 \dots b_{255}\}$ = { A256[99],0,A256[143],0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,A256[181],0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, A256[1],0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, A256[244],0,0,0,0,0,0,0, A256[37],0,0,0, A256[249],0, A256[9], A256[5],0}. In this notation, A256[249] represents the 249th element of Galois Field, corresponding to 'F9' hex value. The obtained values are according to algebraic form of S-box (4), which confirms the validity of the method.

In [1], the authors pretend that the AES S-box can be vulnerable to the interpolation attack due to the fact that has only 9 terms are involved in the algebraic expression. In order to increase the number of terms involved in the algebraic expression of proposed S-box, the authors tried the multiplication of AES S-box algebraic expression.

4. THE MULTIPLICATION OF THE AES S-BOX

It is expected that multiplying an algebraic expression by itself, the number of terms may increase or may remain the same. Caution must be taken in order to verify if the obtained function is still a permutation. This condition is to be checked for an S-box in order to be invertible.

In this section the authors start to multiply the algebraic expression (4), thus:

$f_{RD}^{(i)}(x) = (05 \cdot x^{254} + 09 \cdot x^{253} + F9 \cdot x^{251} + 25 \cdot x^{247} + F4 \cdot x^{239} + 01 \cdot x^{223} + B5 \cdot x^{191} + 8F \cdot x^{127} + 63)^i$ (5)

where $i \in \{1,2,\dots 254\}$. Due to the fact that the programs Mathematica ®, which the authors used, is unable to factor complex algebraic expressions with coefficients in GF(2^8), the authors chose another approach, that is the multiplication of every other element of AES S-box by itself for a number i of times. Then the algebraic expression for the resulting equivalent S-box is found by solving the linear system of equation with coefficients in GF(2^8), similar to (3).

Finding the algebraic expression of:

$f_{RD}^{(i)}(x) = (05 \cdot x^{254} + 09 \cdot x^{253} + F9 \cdot x^{251} + 25 \cdot x^{247} + F4 \cdot x^{239} + 01 \cdot x^{223} + B5 \cdot x^{191} + 8F \cdot x^{127} + 63)^i$ (6)

is equivalent to solve the linear system given in:

$$\begin{cases} b_0 + \quad 0 + ... \quad +0 \quad +0 \quad = (63)^i \\ b_0 + \quad b_1 + ... \quad +b_{254} \quad +b_{255} \quad = (7C)^i \\ b_0 + \quad b_1 \cdot 02 + ... \quad +b_{254} \cdot 02^{254} \quad +b_{255} \quad = (77)^i \\ ... \\ b_0 + \quad b_1 \cdot FE + ... \quad +b_{254} \cdot FE^{254} \quad +b_{255} \quad = (16)^i \end{cases} \tag{7}$$

The solution of system (7), for i=239 is:

$\{b_0, b_1 \dots b_{255}\}$=

A256[99],A256[120],A256[244],A256[238],A256[219],A256[234],A256[241],A256[106],A256[78],A256[198],A256[140],A256[62],A256[79],A256[105],A256[7],A256[25],A256[229],A256[88],A256[118],A256[73],A256[131],A256[137],A256[117],A256[72],A256[217],A256[119],A256[220],A256[251],A256[165],A256[57],A256[151],A256[41],A256[126],A256[157],A256[57],A256[75],A256[233],A256[221],A256[122], A256[124],A256[125],A256[129],A256[162],A256[144],A256[204],A256[247],A256[186],A256[29],A256[28],A256[119],A256[239],A256[79],A256[17],A256[169],A256[4],A256[2],A256[185],A256[206],A256[1

55],A256[122],A256[11],A256[117],A256[7],A256[100],A256[127],A256[78],A256[126],A256[56],A256[93],A256[97],A256[11],A256[19],A256[121],A256[48],A256[57],A256[63],A256[45],A256[182],A256[39],A256[147],A256[81],A256[167],A256[10],A256[18],A256[57],A256[190],A256[149],A256[75],A256[101],A256[233],A256[43],A256[104],A256[119],A256[160],A256[17],A256[47],A256[46],A256[92],A256[16],A256[3],A256[25],A256[5],A256[238],A256[12],A256[145],A256[255],A256[4],A256[167],A256[163],A256[126],A256[104],A256[231],A256[199],A256[73],A256[232],A256[171],A256[249],A256[214],A256[180],A256[173],A256[78],A256[117],A256[96],A256[22],A256[4],A256[122],A256[30],A256[146],A256[226],A256[189],A256[204],A256[186],A256[213],A256[200],A256[201],A256[20],A256[203],A256[59],A256[8],A256[84],A256[123],A256[194],A256[190],A256[42],A256[153],A256[48],A256[179],0,A256[229],A256[132],A256[59],A256[235],A256[123],A256[71],A256[192],A256[158],A256[21],A256[133],A256[101],A256[12],A256[130],A256[50],A256[83],A256[242],A256[136],A256[73],A256[234],A256[42],A256[92],A256[149],A256[64],A256[241],A256[150],A256[121],A256[230],A256[160],A256[113],A256[39],A256[21],A256[105],A256[46],A256[246],A256[227],A256[222],A256[76],A256[44],A256[201],A256[197],A256[139],A256[119],A256[244],A256[26],A256[55],A256[52],A256[37],A256[68],A256[216],A256[96],A256[79],A256[73],A256[72],A256[13],A256[215],A256[176],A256[241],A256[189],A256[61],A256[84],A256[58],A256[72],A256[145],A256[191],A256[208],A256[106],A256[232],A256[189],A256[206],A256[53],A256[242],A256[112],A256[63],A256[186],A256[195],A256[250],A256[114],A256[254],A256[105],A256[254],A256[168],A256[235],A256[57],A256[189],A256[245],A256[6],A256[115],A256[37],A256[65],A256[222],A256[142],A256[242],A256[196],A256[50],A256[202],A256[16],A256[128],A256[216],A256[146],A256[110],A256[20],A256[192],A256[205],A256[155],A256[10],A256[75],A256[246],0}. We can notice that for $f_{RD}^{(239)}(x)$ there are involved 254 terms.

5. RESULTS

After solving the system (7) for any $i \in \{1,2,\ldots 254\}$, the authors noticed that:

(*i*) For $i \in \{1,2,4,8,16,32,64,128\}$, the number of terms involved in the resulting algebraic expression remains unchanged, that is 9;

(*ii*) For $i \in \{1,2,\ldots 254\} \setminus \{1,2,4,8,16,32,64,128\}$, the number of terms involved in the resulting algebraic expression increases, being larger than 91 with a maximum of 254;

(*iii*) However, only 128 of the resulting $f_{RD}^{(i)}(x)$ are permutations, that is almost half;

(*iv*) The authors considered the general expression (2) having 256 terms. But in GF(2^8) for any value of *x*, excepting the null value, the following expression holds:

$$x^{255}=1. \quad (8)$$

As consequence, the coefficient b_{255} found by solving the linear system (7) is null for any $i \in \{1,2,\ldots 254\}$. This was expected because the value of the coefficient b_{255} can be included in the value of b_0 in all equations of (7), due to (8), but not in the first equation. This exception explains the null value for b_{255}.

Table 1

Order of multiplication/ number of terms for algebraic expression (*i*/*k*)

i/*k*	1/9	2/9	4/9	7/91	8/9	9/93
13/92	14/91	16/9	19/93	22/93	23/163	26/92
28/91	29/163	31/218	32/9	37/93	38/93	41/93
43/163	44/93	46/163	47/217	49/93	52/92	53/162
56/91	58/163	59/219	61/219	62/218	64/9	67/92
71/163	73/93	74/93	76/93	77/162	79/219	82/93
83/162	86/163	88/93	89/163	91/219	92/163	94/217
97/93	98/93	101/163	103/219	104/92	106/162	107/219
108/219	112/91	113/163	116/163	118/219	121/217	122/219
124/218	127/254	128/9	131/91	133/93	134/92	137/93
139/163	142/163	143/218	146/93	148/93	149/163	151/217

152/93	154/162	157/219	158/219	161/92	163/163	164/93
166/162	167/219	169/162	172/163	173/219	176/93	178/163
179/219	181/219	182/219	184/163	188/217	191/254	193/91
194/93	196/93	197/163	199/218	202/163	207/217	206/219
208/92	209/163	211/219	212/162	214/219	217/219	218/219
223/254	224/91	226/163	227/218	229/217	232/163	233/219
236/219	239/254	241/218	242/217	244/219	247/254	248/218
251/254	253/254	254/254	-	-	-	-

In Table 1 there are given the results after solving the systems of equations (7) for any $i \in \{1,2,\ldots 254\}$. In this table *i* represent the order of multiplication for elements of standard AES S-box, and *k* represents the number of terms for corresponding algebraic expression. The missing orders of multiplication (e.g. $k \in \{3,5,6\ldots 252\}$) correspond to noninvertible maps which are not appropriate for building S-boxes, and they are not listed here.

Taking into consideration additional requirement for an S-box, given in [2], that are non-linearity and difference propagation probability, the authors noticed that the non-linearity of algebraic expressions (*i*) remains 112 and difference propagation probability is 2^{-6}, but for algebraic expressions (*ii*) the non-linearity decreases under 100 (in average 96) and difference propagation probability is higher than 2^{-6}.

6. CONCLUSIONS

Even if the proposed purpose of S-box multiplication (that is to increase the number of terms involved in the algebraic expression of S-box) was attained for some powers of *i*, the authors noticed that the other design criteria for S-box deprecated. These deprecated properties are non-linearity and difference propagation probability. This study concludes that it is not possible to improve all design criteria for S-box at the same time by multiplication.

REFERENCES

1. L. JINGMEI, W. BAODIAN, W. XINMEI, *New Method to Determine Algebraic Expression of Rijndael S-box*, InfoSecu04, pp. 181-185, 2004.
2. J. DAEMEN, V. RIJMEN, *The Design of Rijndael AES – The Advanced Encryption Standard*, Springer, 2002.
3. NIST, *Specification for the ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards Publication 197, 2001.
4. S. D. SINHA, C. P. ARYA, *Algebraic Construction and Cryptographic Properties of Rijndael Substitution Box*, Defence Science Journal, **62**, *1*, pp. 32-37, 2012.