Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **6**, November **2015**

A New AES S-Box Equation System Based on BES

Jie Cui, Hong Zhong*, Run-Hua Shi, Liang-Min Wang

School of Computer Science and Technology,
Anhui University, Hefei, 230039, China
cuijie@mail.ustc.edu.cn, hfsrh@sina.com, wanglm.ahu@qq.com
*Corresponding author: zhongh@mail.ustc.edu.cn

Received October, 2014; revised July, 2015

Abstract. *S-box is the unique nonlinear operation in Rijndael, and it plays a key role in ensuring AES security. In this paper, according to the principle of AES S-box and the Big Encryption System (BES) cryptography, an improved equation system over $GF(2^8)$ is proposed to describe Rijndael S-box. By comparing with other existing systems, this equation system has weaker resistance against algebraic attacks. So it has a lower complexity while applying algebraic attacks. This is helpful for the implementation of algebraic cryptanalysis.*
Keywords: AES, Big encryption system, S-box, Resistance of algebraic attacks, Multivariate quadratic equations

1. **Introduction.** Since Rijndael [1, 2], the substitution-permutation network (SPN) structure block cipher algorithm designed by Vincent Rijmen and Joan Danmen, was chosen by NIST as the Advanced Encryption Standard (AES) on October 2, 2000, many schemes have been proposed to attack it [3, 4, 5]. It has been proved that Rijndael has the security 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, S-box is a crucial element and it determines the performance of Rijndael [6].

S-box is the unique nonlinear operation in Rijndael, and it determines the performance of Rijndael, so much work has concentrated on Rijndael S-box. Many researchers devote time to design and improve the algebraic cryptanalysis scheme [1, 7, 8, 9]. Algebraic cryptanalysis consists of two steps. First, one must convert the cipher into a system of polynomial equations, usually over $GF(2)$, but sometimes over other rings. Second, one must solve the system of equations and obtain from the solution the secret key of the cipher. Many researchers focus on these two steps. Courtois and Pieprzyk [10] analyzed the overdefined system and proposed XSL (eXtended Sparse Linearization) attack on Rijndael. There exists too many assumptions in XSL attack technology, so its effectiveness has been questioned. Ling-Guo Cui [11] analyzed the algebraic structure of Rijndael S-box and proposed a new S-box structure. This further indicates that there exists security problems in AES S-box, and it is feasible to implement algebraic attack on AES. Murphy and Robshaw [12] defined a new block cipher, the BES (Big Encryption System), that uses only simple algebraic operations in $GF(2^8)$. The emergence of BES cryptography is helpful to optimize the system of equations, and then to provide a guideline for designing efficient algebraic cryptanalysis scheme. Because a key step of algebraic cryptanalysis

is optimizing the equation system, many researchers perform some particular studies on the equation system optimization technology. N. Li and W. Chen [13] proposed a new system of multivariate quadratic equations over $GF(2^8)$ to describe completely Rijndael in 2004. H. Xiao and G. Zhang [14] proposed an improvement on algebraic system of multivariate quadratic equations for Rijndael in 2008. The improved equation system had a lower complexity while applying the XSL technique. There have been few research results of the equation system optimization in recent years. The main work of this paper is to further optimize the equation system of AES S-box.

In this paper the BES cipher is analyzed, and an improved equation system over $GF(2^8)$ is proposed to describe Rijndael S-box. This paper is organized into sections: principle of AES S-box, the Big Encryption System, the improvement on equation system of AES S-box, and conclusion.

2. **Principle of AES S-box.** Looking upon 8-bit bytes as elements in $GF(2^8)$, Rijndael S-box is a combination of an inverse function $I(x)$ which is the multiplicative inverse modulo the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, and an affine transformation function $A(x)$. The $I(x)$ and $A(x)$ are as follows.

(1) The inverse function $I(x)$ is defined as:

$$I(x) = \begin{cases} (x)^{254} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

(2) The affine transformation function $A(x)$is defined as:

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

where $x_i (i = 0, \ldots, 7)$ are the bits of the byte x, and x_7 is the most significant bit. Therefore, Rijndael S-box can be denoted by

$$S(x) = A \circ I = A(I(x))$$

From the construction principle of Rijndael S-box, the algebraic expression of Rijndael S-box can be derived as follow:

$$\begin{aligned} S(x) = {} & 05x^{FE} + 09x^{FD} + F9x^{FB} + 25x^{F7} + F4x^{EF} + \\ & 01x^{DF} + B5x^{BF} + 8Fx^{7F} + 63 \end{aligned}$$

3. **The Big Encryption System.** The cipher AES has a 16-byte message and key space. The cipher BES has a 128-byte key space and message. There is a restriction of the BES spaces to a subset of size 2^{128} that corresponds to the AES. We denote these three sets (i.e. three message and key spaces) by A, B and $\mathrm{B_A}$ respectively, and the state spaces of the AES and the BES are shown in Table 1.

Both the BES and the AES use a state vector of bytes, which is transformed by the basic operations in a round. In both cases, the plaintext is the input state vector while the ciphertext is the output state vector. We now describe the basic techniques required to establish the relationship between the BES and the AES.

TABLE 1. The State spaces of the AES and the BES

Notation	Meanings	Vector space
A	State space of the AES	F^{16}
B	State space of the BES	F^{128}
B_A	Subset of B corresponding to A	Subset of F^{128}

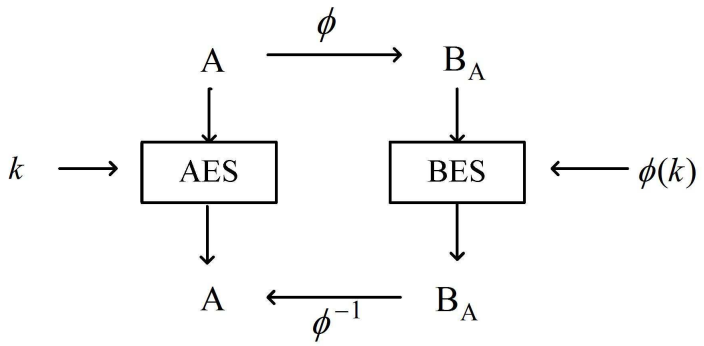

FIGURE 1. The relationship between the AES and the BES

(1) Inversion. For $b \in$ F, it is identical to standard field inversion for non-zero field elements with $0^{(-1)} = 0$. For an n-dimensional vector a=$(a_0, \ldots, a_{n-1}) \in F^n$, the inversion can be viewed as a componentwise operation and set

$$\mathrm{a}^{(-1)} = (a_0^{(-1)}, \ldots, a_{n-1}^{(-1)}).$$

(2) Vector conjugates. For any element $a \in$ F we can define the vector conjugate of a, $\tilde{\mathrm{a}}$, as the vector of the eight $GF(2)$-conjugates of a, so

$$\tilde{\mathrm{a}} = (a^{2^0}, a^{2^1}, a^{2^2}, a^{2^3}, a^{2^4}, a^{2^5}, a^{2^6}, a^{2^7})$$

We use a vector conjugate mapping φ from F^n to a subset of F^{8n}. For $n = 1$ and $a \in$ F, we have

$$\tilde{\mathrm{a}} = \varphi(a) = (a^{2^0}, a^{2^1}, a^{2^2}, a^{2^3}, a^{2^4}, a^{2^5}, a^{2^6}, a^{2^7}).$$

This definition extends in the obvious way to a vector conjugate mapping φ from F^n to a subset of F^{8n}. The n-dimensional vector a=$(a_0, \ldots, a_{n-1}) \in F^n$ is mapped to

$$\tilde{\mathrm{a}} = \varphi(\mathrm{a}) = (\varphi(a_0), \ldots, \varphi(a_{n-1})).$$

The vector conjugate mapping φ has desirable algebraic properties, namely that it is additive and preserves inverse, so

$$\varphi(a + a') = \varphi(a) + \varphi(a')$$

and

$$\varphi(a^{-1}) = \varphi(a)^{-1}.$$

When each successive set of eight components in a $\in F^{8n}$ form an ordered set of $GF(2)$-conjugates, we say that a has the conjugacy property. Based on this, it is easy to define φ^{-1} as an extraction mapping which recovers the basic vector from a vector conjugate.

(3) Embedding the AES state space in the BES state space. Any plaintext, ciphertext, intermediate text, or subkey for the AES is an element of the state space A. Similarly,

any plaintext, ciphertext, intermediate text, or subkey for the BES is an element of the state space B.

We can use the vector conjugate map φ to embed any element of the AES state space A into the BES state space B. We define $\mathrm{B_A} = \varphi(\mathrm{A}) \subset B$ to be the AES subset of BES, that is the embedded image of the AES state space in the BES state space. Elements of $\mathrm{B_A}$, that is embedded image of AES states or subkeys, have the vector conjugacy property. Furthermore, $\mathrm{B_A}$ is an additively closed set that also preserves inverses. Figure 1 describes the relationship between the AES and the BES.

4. The New AES S-box Equation System and Its Performance Analysis.

4.1. The Improvement on Equation System of AES S-box.

The important feature of the BES is that it is defined exclusively using simple operations in one field, $GF(2^8)$. After embedding AES into BES, we get $\mathrm{B_A}$, so we can easily use the system of polynomial equations to describe the AES. If the equation system can be solved, we can obtain the encryption key, so we can crack the AES. As the only nonlinear component of the AES, S-box is a crucial element and it determines the security of the AES. Therefore, the generation and improvement of AES S-box equation system is a key step of algebraic attack on the AES. The tool of embedding AES into BES is conjugate mapping, and each byte is mapped to 8 consecutive 2-power form. The selection of this mapping approach is to solve the inconsistent problem of the space of the two transformations (multiplicative inverse and affine transformation).

AES S-box is invertible and is constructed by the composition of two transformations:

(1) Taking the multiplicative inverse in $GF(2^8)$;

(2) Applying the affine transformation in $GF(2)$.

In order to solve the inconsistent problem of the space of the two transformations, we need apply conjugate mapping to both multiplicative inverse and affine transformation. Next we detail the conjugate mapping and construct the equation system of AES S-box.

Affine transformation matrix $L_A : F \mapsto F$ can be expressed as a polynomial function $f : F \mapsto F$

$$f(a) = \sum_{k=0}^{7} \lambda_k a^{2^k}.$$

where $(\lambda_0, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7)$ = (05,09,F9,25,F4,01,B5,8F). Here we construct the affine transformation matrix of $\mathrm{B_A}$. It is easy to get $L_B(a) = \phi(L_A(a)) = (f^{2^0}(a), \ldots, f^{2^7}(a))$, where the solution of each component is based on equation (1).

$$(f(a))^2 = \left(\sum_{k=0}^{7} \lambda_k a^{2^k}\right)^2 = \sum_{k=0}^{7} \lambda_k^2 a^{2^{k+1}} \tag{1}$$

Then we can obtain equation (2) from equation (1).

$$f^{2^i}(a) = \sum_{k=0}^{7} \lambda_k^{2^i} a^{2^{k+i}} \ (0 \le i \le 7) \tag{2}$$

The affine transformation matrix of $\mathrm{B_A}$can be denoted by $L_B : F^8 \mapsto F^8$, let $L_B = [l_{ij}]_{i,j=0,\ldots,7}$, the following equation (3) can be obtained by the undetermined coefficient method from equation (2).

$$l_{i,j} = \lambda_{8-i+j}^{2^i} \bmod 8 \tag{3}$$

We can further obtain equation (4) by computing.

$$L_B = \begin{pmatrix} (\lambda_0)^{2^0} & (\lambda_1)^{2^0} & (\lambda_2)^{2^0} & (\lambda_3)^{2^0} & (\lambda_4)^{2^0} & (\lambda_5)^{2^0} & (\lambda_6)^{2^0} & (\lambda_7)^{2^0} \\ (\lambda_7)^{2^1} & (\lambda_0)^{2^1} & (\lambda_1)^{2^1} & (\lambda_2)^{2^1} & (\lambda_3)^{2^1} & (\lambda_4)^{2^1} & (\lambda_5)^{2^1} & (\lambda_6)^{2^1} \\ (\lambda_6)^{2^2} & (\lambda_7)^{2^2} & (\lambda_0)^{2^2} & (\lambda_1)^{2^2} & (\lambda_2)^{2^2} & (\lambda_3)^{2^2} & (\lambda_4)^{2^2} & (\lambda_5)^{2^2} \\ (\lambda_5)^{2^3} & (\lambda_6)^{2^3} & (\lambda_7)^{2^3} & (\lambda_0)^{2^3} & (\lambda_1)^{2^3} & (\lambda_2)^{2^3} & (\lambda_3)^{2^3} & (\lambda_4)^{2^3} \\ (\lambda_4)^{2^4} & (\lambda_5)^{2^4} & (\lambda_6)^{2^4} & (\lambda_7)^{2^4} & (\lambda_0)^{2^4} & (\lambda_1)^{2^4} & (\lambda_2)^{2^4} & (\lambda_3)^{2^4} \\ (\lambda_3)^{2^5} & (\lambda_4)^{2^5} & (\lambda_5)^{2^5} & (\lambda_6)^{2^5} & (\lambda_7)^{2^5} & (\lambda_0)^{2^5} & (\lambda_1)^{2^5} & (\lambda_2)^{2^5} \\ (\lambda_2)^{2^6} & (\lambda_3)^{2^6} & (\lambda_4)^{2^6} & (\lambda_5)^{2^6} & (\lambda_6)^{2^6} & (\lambda_7)^{2^6} & (\lambda_0)^{2^6} & (\lambda_1)^{2^6} \\ (\lambda_1)^{2^7} & (\lambda_2)^{2^7} & (\lambda_3)^{2^7} & (\lambda_4)^{2^7} & (\lambda_5)^{2^7} & (\lambda_6)^{2^7} & (\lambda_7)^{2^7} & (\lambda_0)^{2^7} \end{pmatrix} \quad (4)$$

$$= \begin{pmatrix} 05 & 09 & f9 & 25 & f4 & 01 & b5 & 8f \\ cf & 11 & 41 & 07 & 7d & 56 & 01 & fc \\ 16 & 64 & 1a & aa & 15 & 8d & a4 & 01 \\ 01 & 0f & d7 & 5f & b2 & 0a & cb & e6 \\ 49 & 01 & 55 & 3f & e5 & e9 & 44 & 74 \\ cc & ea & 01 & a1 & 22 & 4c & 1c & bb \\ a8 & 61 & 19 & 01 & f7 & 68 & fb & 4b \\ ee & b6 & c6 & 5a & 01 & 53 & 87 & 03 \end{pmatrix}$$

The global affine transformation matrix $Lin_B : F^{128} \mapsto F^{128}$ in B is easily obtained from L_B, where Lin_B is a block diagonal matrix with 16 identical blocks L_B. Then we can get

$$Lin_B = \begin{bmatrix} L_B & & & \\ & L_B & & \\ & & \ddots & \\ & & & L_B \end{bmatrix}$$

The constant used in constant addition transformation of Rijndael S-box is $c_A =' 63' \in F$. Making the conjugate mapping of c_A, we can get

$$\begin{aligned} &\varphi(c_A) = ((63)^{2^0}, (63)^{2^1}, (63)^{2^2}, \\ &(63)^{2^3}, (63)^{2^4}, (63)^{2^5}, (63)^{2^6}, (63)^{2^7}) \ . \\ &= (63,C2,35,66,D3,2F,39,36) \end{aligned}$$

The corresponding constant vector used in BES is $c_B = \phi(\underbrace{c_A, \ldots, c_A}_{16}) = (\underbrace{\phi(c_A), \ldots, \phi(c_A)}_{16})$, that is

$$[c_B]_i = [\phi(c_A)]_{i \bmod 8} \ 0 \le i \le 127$$

For the AES-128, the intermediate state of each round encryption can be denoted as

$$\begin{aligned} s &= \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \\ &= (s_{00}, \ldots, s_{30}, s_{01}, \ldots, s_{31}, \ldots, s_{33})^T \end{aligned}$$

After embedding AES-128 into BES, the corresponding intermediate state of each round encryption can be denoted as

$$s' = (s'_{000}, \ldots, s'_{007}, s'_{100}, \ldots, s'_{107}, \ldots, s'_{330}, \ldots, s'_{337})^T$$

For S-box transformation of each round, the input, the intermediate variables (i.e. the result of taking multiplicative inverse) and the output are denoted by $x_{i,j,k}$, $y_{i,j,k}$ and $z_{i,j,k}$

respectively, where $0 \le i, j \le 3, 0 \le k \le 7$. The S-box transformation of each round can be expressed as

$$\begin{bmatrix} z_{000} \\ \vdots \\ z_{007} \\ z_{100} \\ \vdots \\ z_{107} \\ \vdots \\ \vdots \\ \vdots \\ z_{330} \\ \vdots \\ z_{337} \end{bmatrix} = Lin_B \cdot \begin{bmatrix} x_{000}^{-1} \\ \vdots \\ x_{007}^{-1} \\ x_{100}^{-1} \\ \vdots \\ x_{107}^{-1} \\ \vdots \\ \vdots \\ \vdots \\ x_{330}^{-1} \\ \vdots \\ x_{337}^{-1} \end{bmatrix} = Lin_B \cdot \begin{bmatrix} y_{000} \\ \vdots \\ y_{007} \\ y_{100} \\ \vdots \\ y_{107} \\ \vdots \\ \vdots \\ \vdots \\ y_{330} \\ \vdots \\ y_{337} \end{bmatrix} = \begin{bmatrix} L_B & & & \\ & L_B & & \\ & & \ddots & \\ & & & L_B \end{bmatrix} \cdot \begin{bmatrix} y_{000} \\ \vdots \\ y_{007} \\ y_{100} \\ \vdots \\ y_{107} \\ \vdots \\ \vdots \\ \vdots \\ y_{330} \\ \vdots \\ y_{337} \end{bmatrix}$$

The above equation can be abbreviated as

$$\begin{bmatrix} z_{i,j,0} \\ \vdots \\ z_{i,j,7} \end{bmatrix} = L_B \cdot \begin{bmatrix} y_{i,j,0} \\ \vdots \\ y_{i,j,7} \end{bmatrix}, \text{i.e. } z_{i,j,k} = g(y_{i,j,0}, y_{i,j,1}, \ldots, y_{i,j,7})$$

where $0 \le i, j \le 3, 0 \le k \le 7$, the function $g(\cdot)$ is a linear combination function.

Therefore, the equation system of the each round S-box transformation is as follow.

$$\begin{cases} x_{i,j,k} \cdot y_{i,j,k} = 1 \ , (0 \le i, j \le 3, 0 \le k \le 7) \\ y_{i,j,k+1} = (y_{i,j,k})^2 \ , (0 \le i, j \le 3, 0 \le k \le 7) \\ z_{i,j,k+1} = (z_{i,j,k})^2 \ , (0 \le i, j \le 3, 0 \le k \le 7) \\ z_{i,j,k} = g(y_{i,j,0}, \ldots, y_{i,j,7}) \ , (0 \le i, j \le 3, 0 \le k \le 7) \end{cases}$$

where the addition in $k + 1$ is modulo 8 plus.

4.2. **Comparisons of Equation Systems of Rijndael S-box.**

Definition 4.1. [1] *For r equations in $t$terms over $GF(2^n)$, the resistance of algebraic attacks (RAA) is denoted by Γ and is defined as follow:*

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

The resistance of algebraic attacks reflects a difficulty of solving multivariate equations. Thus we will use this quantity to measure the resistance of algebraic attacks in this paper.

In the above equation system in Section 4.1, the first three lines are quadratic equations, and the last line are linear equations. The S-box transformation of each round can therefore be described as a multivariate quadratic system using 512 equations, of which 384 are quadratic equations and 128 are linear equations. In the 384 quadratic equations, there exist 384 variables: $x_{i,j,k}$, $y_{i,j,k}$, $z_{i,j,k}$ and 641 terms: 1, $y_{i,j,k}$, $z_{i,j,k}$, $x_{i,j,k} \cdot y_{i,j,k}$, $(y_{i,j,k})^2$ and $(z_{i,j,k})^2$. In the 128 linear equations, there exist 256 variables: $y_{i,j,k}$, $z_{i,j,k}$ and 256 terms: $y_{i,j,k}$, $z_{i,j,k}$, where $0 \le i, j \le 3, 0 \le k \le 7$.

According to the definition 1, the resistance of algebraic attacks Γ reflects the difficulty of solving the multivariate equation. The comparison results are shown in table 2. It can be seen that our equation system has a smaller Γ than other existing equation systems, so it can decrease the complexity of algebraic cryptanalysis of Rijndael. That is, the new equation system has weaker resistance against algebraic attacks.

TABLE 2. The State spaces of the AES and the BES

Parameter	Notation	The equation system [13]	The equation system [14]	Our equation system
Number of quadratic equations of each round S-box transformation	r	272	256	384
Number of variables of quadratic equations in each round S-box transformation	m	256	176	384
Number of terms of quadratic equations in each round S-box transformation	t	544	448	641
Number of linear equations of each round S-box transformation	r'	16	16	128
Number of variables of linear equations in each round S-box transformation	m'	144	144	256
Number of terms of linear equations in each round S-box transformation	t'	144	144	256
Size of the S-box	n	8	3	8
Resistance of algebraic attacks of the S-box based on the quadratic equation system	Γ	2^{173}	2^{384}	2^{165}
Resistance of algebraic attacks of the S-box based on the linear equation system	Γ'	2^{64}	2^{233}	2^{64}

5. **Conclusions.** In this paper, an improved equation system over $GF(2^8)$ is proposed to describe Rijndael S-boxand it is helpful to decrease the complexity of algebraic cryptanalysis. Firstly, the construction principle and the algebraic expression of Rijndael S-box are described. Secondly, the Big Encryption System is introduced, and the conjugate map between AES and BES is analyzed. Finally, an improved equation system over $GF(2^8)$ is proposed to decrease the complexity of algebraic cryptanalysis. The new equation system has weaker resistance against algebraic attacks, so it has a lower complexity while applying algebraic attacks.

Acknowledgment. The work was supported by the National Natural Science Foundation of China (No. 61173188, No. 61502008), the Educational Commission of Anhui Province, China (No. KJ2013A017), The Natural Science Foundation of Anhui Province (No. 1508085QF132), the Research Fund for the Doctoral Program of Higher Education (No. 20133401110004), the Science and Technology Project of Anhui Province (No. 1401b042015), the Tender Project of the Co-Innovation Center for Information Supply & Assurance Technology of Anhui University (No. ADXXBZ2014-7), and the Doctoral Research Start-up Funds Project of Anhui University. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

REFERENCES

[1] Jung Hee, D. H. Lee, Resistance of S-boxes against algebraic attack, *http://www.math.snu.ac.kr/jhcheon/Published/2004_FSE/FSE04_CL.pdf*, 2004.

[2] H. Demirci, M. S. Sagiroglu, M. O. Kulekci, A time-memory trade-off approach for the solution of nonlinear equation systems, *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 21, no. 1, pp. 186-197, 2013.
[3] X. Zhang, Q. Wang, B. Wang, H. Kan, A Constructive Method of Algebraic Attack with Less Keystream Bits, *IEICE TRANSACTIONS on Fundamentals of Electronics*, vol. E94-A, no. 10, pp. 2059-2062, 2011.
[4] J. Kim, S. Hong, B. Preneel, Related-key rectangle attacks on reduced AES-192 and AES-256, *Proc. of FSE2007*, pp. 225–241, 2007.
[5] Q. Wang, D. Gu, V. Rijmen, Y. Liu, J. Chen, Improved impossible differential attacks on large-block rijndael, *Proc. Of ICISC 2012*, pp. 126-140, 2013.
[6] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, A projective general linear group based algorithm for the construction of substitution box for block ciphers, *Neural Computing and Applications*, vol. 22, no. 6, pp. 1085-1093, 2013.
[7] W. Zhang, W. Wu, L. Zhang, and D. Feng, Improved related-key impossible differential attacks on reduced round AES-192, *Proc. of SAC 2006*, pp. 15-27, 2007.
[8] S. Ghosh, A. Das, Improvements of Algebraic Attacks Based on Structured Gaussian Elimination, *http://eprint.iacr.org*, 2012.
[9] L. Babinkostova, K. W. Bombardier, M. C. Cole, T. A. Morrell, C. B. Scott, Algebraic properties of generalized Rijndael-like ciphers, *Groups Complexity Cryptology*, vol. 6, no. 1, pp. 37-54, 2014.
[10] N. Courtois, J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, *Proc. Of Asiacrypt 2002*, pp. 267-287, 2002.
[11] L. G. Cui, A New S-box Structure Named Affine-Power-Affine, *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 751-759, 2007.
[12] S. Murphy, M. J. B. Robshaw, Essential algebraic structure within the AES, *Proc. of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, pp. 1-16, 2002.
[13] N. Li and W. Chen, A new system of multivariate quadratic equations for rijndael, *Journal of Electronics & Information Technology*, vol. 26, no. 12, pp. 1990-1995, 2004.
[14] H. Xiao, G. Zhang, The improvement on algebraic system of multivariate quadrtic equations for Rijndael, *Journal of Electronics & Information Technology*, vol. 30, no. 10, pp. 2459-2463, 2008.