http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (15): 2482-2488, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2482.2488

Generation and Optimization of Rijndael S-box Equation System

[1]Jie Cui, [1]Hong Zhong, [2]Jiankai Wang and [1]Runhua Shi
[1]School of Computer Science and Technology, Anhui University, Hefei, 230039, China
[2]School of Natural Sciences, Anhui Agricultural University, Hefei, 230036, China

Abstract: In this study, according to the inverse transformation principle and the affine transformation principle of Rijndael S-box, a new approach to generating the multivariate quadratic equation system over GF(2) is proposed and the generation process is given explicitly. According to the algebraic expression of the new Rijndael S-box, an equation system over GF(2^8) is proposed to describe Rijndael. By comparing with other existing systems, this system has stronger resistance against algebraic attacks. So, the equation system of the new Rijndael S-box is much securer than other existing equation systems.

Key words: Rijndael, multivariate quadratic equation, S-box, resistance of algebraic attacks

INTRODUCTION

Since, Rijndael (Cheon and Lee, 2004; Demirci *et al*., 2013), the 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 (Zhang *et al*., 2011; Kim *et al*., 2007; Chen *et al*., 2011). 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.

Many researchers devote time to design and improve the algebraic cryptanalysis scheme (Zhang *et al*., 2007; Ghosh and Das, 2012; Cheon and Lee, 2004). Courtois and Pieprzyk (2002) analyzed the overdefined system and proposed XSL attack on Rijndael. Hussain *et al*. (2013) analyzed the algebraic structure of Rijndael S-box and proposed a new S-box structure. Much study has concentrated on Rijndael S-box, however they did not explicitly give the approach to generating its multivariate quadratic equation system over GF(2). Murphy and Robshaw (2002) showed that the Rijndael preserves algebraic curves and that it can be expressed as a very simple system of multivariate quadratic equations over GF(2^8). Cheon and Lee (2004) proposed a new system of multivariate quadratic equations over GF(2^8) to describe completely Rijndael in 2004. There have been few research results of the equation system optimization in recent years.

In this study a new approach to generating the multivariate quadratic equations of Rijndael S-box over GF(2) is given explicitly and an equation system over GF(2^8) is proposed to describe the new Rijndael S-box. This study is organized into sections: Principle of Rijndael S-box, new approach to generating multivariate quadratic equation system of Rijndael S-box, the optimization of Rijndael S-box equation system and conclusion.

PRINCIPLE OF RIJNDAEL 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:

- The inverse function I(x) is defined as:

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

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

Corresponding Author: Hong Zhong, School of Computer Science and Technology, Anhui University, Hefei, 230039, China

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

where, $x_i(i = 0,..., 7)$ 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:

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

NEW APPROACH TO GENERATING MQ EQUATION SYSTEM OF RIJNDAEL S-BOX

Rijndael S-box is a composition of the "patched" inverse in $GF(2^8)$ with 0 mapped on itself with a multivariate affine transformation $GF(2^8)\rightarrow GF(2^8)$. We call these functions, respectively g and f and we call $S = f\circ g$. We note x an input value and $y = g(x)$ the corresponding output value. We will also note $z = S(x) = f(y) = f(g(x))$.

For inverse transformation $y = g(x)$, obviously $xy = 1$ when $x \neq 0$. i.e.:

$$\left(\left(\sum_{i=0}^{7}x_it^i\right)\left(\sum_{j=0}^{7}x_jt^j\right)\right)_{m(t)}=\sum_{k=1}^{7}0\cdot t^k+1 \quad (1)$$

Expanding the Eq. 1, we have:

$$\sum_{i=0}^{7}\sum_{j=0}^{7}(x_iy_j)_{m(t)}(t^{i+j})_{m(t)}=\sum_{k=1}^{7}0\cdot t^k+1 \quad (2)$$

where, $m(t) = t^8+t^4+t^3+t+1$.

Comparing the both sides coefficients of $t^k(0\leq k<8)$ in Eq. 1, we can obtain the 8 multivariate quadratic equations of inverse transformation. Since, $y\mapsto z$ is linear, we can obtain 8 multivariate quadratic equations of Rijndael S-box.

Now, we give the generation principle of Rijndael S-box equation system. Multiplying x by y and the multiplication result modulo m(t), we can obtain the coefficients $c_7,..., c_0$ of $t^k(0\leq k<8)$. Firstly, we give the computation process of the coefficients $c_7,..., c_0$.

We note $(x_7,..., x_0) = x$, $(y_7,..., y_0) = y$ and $(z_7,..., z_0) = z$. i.e.,:

$$x=\sum_{i=0}^{7}x_it^i,\ y=\sum_{i=0}^{7}y_it^i \text{ and } z=\sum_{i=0}^{7}z_it^i$$

We have:

$$\begin{gathered}x\otimes y = x_7y_7\bullet t^{14}+(x_7y_6+x_6y_7)\bullet t_{13}+(x_7y_5+x_6y_6+x_5y_7)\bullet t_{12}+\\(x_7y_4+x_6y_5+x_5y_6+x_4y_7)\bullet t^{11}+(x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7)\\\bullet t^{10}+(x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7)\bullet t^9+\\(x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7)\bullet t^8+\\(x_7y_0+x_6y_1+x_5y_2+x_4y_3+x_3y_4+x_2y_5+x_1y_6+x_0y_7)\bullet t^7+\\(x_6y_0+x_5y_1+x_4y_2+x_3y_3+x_2y_4+x_1y_5+x_0y_6)\\\bullet t^6+(x_5y_0+x_4y_1+x_3y_2+x_2y_3+x_1y_4+x_0y_5)\bullet t^5+\\(x_4y_0+x_3y_1+x_2y_2+x_1y_3+x_0y_4)\bullet t^4+(x_3y_0+x_2y_1+x_1y_2+x_0y_3)\\\bullet t^3+(x_2y_0+x_1y_1+x_0y_2)\bullet t^2+(x_1y_0+x_0y_1)\bullet t+x_0y_0\end{gathered}$$

The multiplication result modulo m(t) one by one and we give the process in detail as follows:

Step 1: $x\otimes y$ modulo:

$$x_7y_7\bullet t^{14}+x_7t_7\bullet t^{10}+x_7y_7\bullet t^9+x_7y_7\bullet t^7+x_7y_7\bullet t^6 = R1$$

Step 2: R1 modulo:

$$\begin{gathered}(x_7y_6+x_6y_7)\bullet t^{13}+(x_7y_6+x_6y_7)\bullet t^9+(x_7y_6+x_6y_7)\bullet t^8+(x_7y_6+x_6y_7)\bullet\\t^6+(x_7y_6+x_6y_7)\bullet t^5 = R2\end{gathered}$$

Step 3: R2 modulo:

$$\begin{gathered}(x_7y_5+x_6y_6+x_5y_7)\bullet t^{12}+(x_7y_5+x_6y_6+x_5y_7)\bullet t^8+\\(x_7y_5+x_6y_6+x_5y_7)\bullet t^7+(x_7y_5+x_6y_6+x_5y_7)\bullet t^5+(x_7y_5+x_6y_6+x_5y_7)\\\bullet t^4 = R3\end{gathered}$$

Step 4: R3 modulo:

$$\begin{gathered}(x_7y_4+x_6y_5+x_5y_6+x_4y_7)\bullet t^{11}+(x_7y_4+x_6y_5+x_5y_6+x_4y_7)\bullet t^7+\\(x_7y_4+x_6y_5+x_5y_6+x_4y_7)\bullet t^6+(x_7y_4+x_6y_5+x_5y_6+x_4y_7)\bullet t^4+\\(x_7y_4+x_6y_5+x_5y_6+x_4y_7)\bullet t^3 = R4\end{gathered}$$

Step 5: R4 modulo:

$$
\begin{gathered}
(x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+x_7y_7)\bullet t^{10}+\\
(x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+x_7y_7)\bullet t^{6}+\\
(x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+x_7y_7)\bullet t^{5}+\\
(x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+x_7y_7)\bullet t^{3}+\\
(x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+x_7y_7)\bullet t^{2} = R5
\end{gathered}
$$

Step 6: R5 modulo:

$$
\begin{gathered}
(x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_7+\\
x_7y_6+x_6y_7)\bullet t^9+(x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+\\
x_2y_7+x_7y_7+x_7y_6+x_6y_7)\bullet t^5+(x_7y_2+x_6y_3+\\
x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_7+x_7y_6+x_6y_7)\bullet t^4+(x_7y_2+\\
x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_7+x_7y_6+x_6y_7)\bullet\\
t^2+(x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_7+x_7y_6+x_6y_7)\bullet\\
t = R6
\end{gathered}
$$

Step 7: R6 modulo:

$$
\begin{gathered}
(x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+x_7y_6+\\
x_6y_7+x_7y_5+x_6y_6+x_5y_7)\bullet t^8+(x_7y_1+x_6y_2+\\
x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+\\
x_7y_6+x_6y_7+x_7y_5+x_6y_6+x_5y_7)\bullet t^4+(x_7y_1+\\
x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+\\
x_7y_6+x_6y_7+x_7y_5+x_6y_6+x_5y_7)\bullet t^3+(x_7y_1+\\
x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+x_7y_6+\\
x_6y_7+x_7y_5+x_6y_6+x_5y_7)\bullet t+(x_7y_1+x_6y_2+x_5y_3+\\
x_4y_4+x_3y_5+x_2y_6+x_1y_7+x_7y_6+x_6y_7+\\
x_7y_5+x_6y_6+x_5y_7) = R7
\end{gathered}
$$

$$
\begin{gathered}
R7 = (x_7y_0+x_6y_1+x_5y_2+x_4y_3+x_3y_4+x_2y_5+x_1y_6+\\
x_0y_7+x_7y_7+x_7y_5+x_6y_6+x_5y_7+x_7y_4+x_6y_5+x_5y_6+\\
x_4y_7)\bullet t^7+x_6y_0+x_5y_1+x_4y_2+x_3y_3+x_2y_4+x_1y_5+x_0y_6+\\
x_7y_6+x_6y_7+x_7y_4+x_6y_5+x_5y_6+x_4y_7+x_7y_3+\\
x_6y_4+x_5y_5+x_4y_6+x_3y_7)\bullet t^6+(x_5y_0+x_4y_1+x_3y_2+x_2y_3+\\
x_1y_4+x_0y_5+x_7y_5+x_6y_6+x_5y_7+x_7y_3+x_6y_4+x_5y_5+x_4y_6\\
+x_3y_7+x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7)\bullet t^5+(x_4y_0+\\
x_3y_1+x_2y_2+x_1y_3+x_0y_4+x_7y_4+x_6y_5+x_5y_6+x_4y_7+\\
x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_7+x_7y_1+x_6y_2+\\
x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7)\bullet t^4+(x_3y_0+x_2y_1+x_1y_2+\\
x_0y_3+x_7y_4+x_6y_5+x_5y_6+x_4y_7+x_7y_3+x_6y_4+x_5y_5+x_4y_6\\
+x_3y_7+x_7y_7+x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+\\
x_7y_6+x_6y_7+x_7y_5+x_6y_6+x_5y_7)\bullet t^3+(x_2y_0+x_1y_1+x_0y_2+x_7y_3+x_6y_4+\\
x_5y_5+x_4y_6+x_3y_7+x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_6+x_6y_7)\\
\bullet t^2+(x_1y_0+x_0y_1+x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+\\
x_7y_7+x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+x_7y_5+\\
x_6y_6+x_5y_7)\bullet t+(x_0y_0+x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+\\
x_7y_6+x_6y_7+x_7y_5+x_6y_6+x_5y_7)
\end{gathered}
$$

Now we obtain the coefficients $c_7,\dots, c_0$ from R7 as Eq. 3.

$$
\begin{cases}
\begin{aligned}
c_7 = {} & x_7y_0+x_6y_1+x_5y_2+x_4y_3+x_3y_4+x_2y_5+x_1y_6+x_0y_7\\
& +x_7y_7+x_7y_5+x_6y_6+x_5y_7+x_7y_4+x_6y_5+x_5y_6+x_4y_7\\
c_6 = {} & x_6y_0+x_5y_1+x_4y_2+x_3y_3+x_2y_4+x_1y_5+x_0y_6+x_7y_6\\
& +x_6y_7+x_7y_4+x_6y_5+x_5y_6+x_4y_7+x_7y_3+x_6y_4+\\
& x_5y_5+x_4y_6+x_3y_7\\
c_5 = {} & x_5y_0+x_4y_1+x_3y_2+x_2y_3+x_1y_4+x_0y_5+x_7y_5+x_6y_6\\
& +x_5y_7+x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+x_7y_2+x_6y_3\\
& +x_5y_4+x_4y_5+x_3y_6+x_2y_7\\
c_4 = {} & x_4y_0+x_3y_1+x_2y_2+x_1y_3+x_0y_4+x_7y_4+x_6y_5+x_5y_6+\\
& x_4y_7+x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_7+\\
& x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7\\
c_3 = {} & x_3y_0+x_2y_1+x_1y_2+x_0y_3+x_7y_4+x_6y_5+x_5y_6+x_4y_7+\\
& x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+x_7y_7+x_7y_1+x_6y_2+\\
& x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+x_7y_6+x_6y_7+x_7y_5+\\
& x_6y_6+x_5y_7\\
c_2 = {} & x_2y_0+x_1y_1+x_0y_2+x_7y_3+x_6y_4+x_5y_5+x_4y_6+x_3y_7+\\
& x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+x_7y_6+x_6y_7\\
c_1 = {} & x_1y_0+x_0y_1+x_7y_2+x_6y_3+x_5y_4+x_4y_5+x_3y_6+x_2y_7+\\
& x_7y_7+x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+\\
& x_7y_5+x_6y_6+x_5y_7\\
c_0 = {} & x_0y_0+x_7y_1+x_6y_2+x_5y_3+x_4y_4+x_3y_5+x_2y_6+x_1y_7+\\
& x_7y_6+x_6y_7+x_7y_5+x_6y_6+x_5y_7
\end{aligned}
\end{cases}
\quad (3)
$$

Then, we give the generation process of the 24 multivariate quadratic equations. According to the principle of Rijndael S-box, the relationship between z and y can be denoted as:

$$z = Ay+\text{‘63'}$$

We can get:

$$y = A^{-1}z+A^{-1}.\ \text{‘63'} = A^{-1}z+\text{‘05'}$$

Where:

$$
A = \begin{bmatrix}
1&1&1&1&1&0&0&0\\
0&1&1&1&1&1&0&0\\
0&0&1&1&1&1&1&0\\
0&0&0&1&1&1&1&1\\
1&0&0&0&1&1&1&1\\
1&1&0&0&0&1&1&1\\
1&1&1&0&0&0&1&1\\
1&1&1&1&0&0&0&1
\end{bmatrix}
\quad
A^{-1} = \begin{bmatrix}
0&1&0&1&0&0&1&0\\
0&0&1&0&1&0&0&1\\
1&0&0&1&0&1&0&0\\
0&1&0&0&1&0&1&0\\
0&0&1&0&0&1&0&1\\
1&0&0&1&0&0&1&0\\
0&1&0&0&1&0&0&1\\
1&0&1&0&0&1&0&0
\end{bmatrix}
$$

Then we get:

$$
\begin{cases}
y_7 = z_6+z_4+z_1\\
y_6 = z_5+z_3+z_0\\
y_5 = z_7+z_4+z_2\\
y_4 = z_6+z_3+z_1\\
y_3 = z_5+z_2+z_0\\
y_2 = z_7+z_4+z_1+1\\
y_1 = z_6+z_3+z_0\\
y_0 = z_7+z_5+z_2+1
\end{cases}
\quad (4)
$$

Substituting Eq. 4 into 3, we obtain 8 multivariate quadratic equations of S-box as Eq. 5:

$$\left\{\begin{array}{l}
0 = x_0z_6 + x_0z_4 + x_0z_1 + x_1z_0 + x_1z_5 + x_1z_3 + x_2z_7 + x_2z_4 + \\
\quad x_2z_2 + x_3z_6 + x_3z_3 + x_3z_1 + x_4z_0 + x_4z_6 + x_4z_5 + x_4z_4 + \\
\quad x_4z_1 + x_4z_2 + x_5z_0 + x_5z_6 + x_5z_7 + x_5z_5 + x_5z_3 + x_6z_6 + \\
\quad x_6z_7 + x_6z_5 + x_6z_4 + x_6z_2 + x_7z_5 + x_7z_3 + x_5 + x_7 \\
0 = x_0z_0 + x_0z_5 + x_0z_3 + x_1z_7 + x_1z_4 + x_1z_2 + x_2z_6 + x_2z_3 + \\
\quad x_2z_1 + x_3z_0 + x_3z_6 + x_3z_5 + x_3z_4 + x_3z_2 + x_3z_1 + x_4z_0 + \\
\quad x_4z_6 + x_4z_7 + x_4z_5 + x_4z_3 + x_5z_6 + x_5z_7 + x_5z_5 + x_5z_4 + \\
\quad x_5z_2 + x_6z_5 + x_6z_3 + x_7z_6 + x_7z_2 + x_7z_1 + x_4 + x_6 \\
0 = x_0z_7 + x_0z_4 + x_0z_2 + x_1z_6 + x_1z_3 + x_1z_1 + x_2z_0 + x_2z_6 + \\
\quad x_2z_5 + x_2z_4 + x_2z_2 + x_2z_1 + x_3z_0 + x_3z_6 + x_3z_5 + x_3z_7 + \\
\quad x_3z_3 + x_4z_2 + x_4z_6 + x_4z_7 + x_4z_5 + x_4z_2 + x_5z_5 + x_5z_3 + \\
\quad x_6z_6 + x_6z_2 + x_6z_1 + x_7z_5 + x_7z_1 + x_7z_0 + x_3 + x_5 + x_7 \\
0 = x_0z_6 + x_0z_1 + x_0z_3 + x_1z_6 + x_1z_4 + x_1z_2 + x_1z_5 + x_1z_1 + \\
\quad x_1z_0 + x_2z_6 + x_2z_3 + x_2z_5 + x_2z_7 + x_2z_0 + x_3z_7 + x_3z_6 + \\
\quad x_3z_5 + x_3z_4 + x_3z_2 + x_4z_5 + x_4z_3 + x_5z_6 + x_5z_2 + x_5z_1 + \\
\quad x_6z_5 + x_6z_1 + x_6z_0 + x_7z_6 + x_7z_7 + x_7z_1 + x_7z_0 + x_4 + \\
\quad x_6 + x_2 + x_7 \\
0 = x_0z_0 + x_0z_5 + x_0z_2 + x_1z_6 + x_1z_7 + x_1z_0 + x_2z_6 + x_2z_5 + \\
\quad x_3z_1 + x_3z_6 + x_3z_5 + x_4z_5 + x_4z_4 + x_4z_0 + x_5z_6 + x_5z_7 + \\
\quad x_5z_3 + x_5z_1 + x_6z_5 + x_6z_1 + x_6z_2 + x_6z_4 + x_6z_0 + x_7z_6 + \\
\quad x_7z_7 + x_7z_3 + x_7z_0 + x_3 + x_6 + x_1 \\
0 = x_0z_7 + x_0z_4 + x_0z_1 + x_1z_6 + x_1z_3 + x_1z_0 + x_2z_6 + x_2z_5 + \\
\quad x_2z_7 + x_2z_4 + x_2z_2 + x_2z_1 + x_3z_6 + x_3z_5 + x_3z_3 + x_3z_4 + \\
\quad x_3z_1 + x_3z_0 + x_4z_7 + x_4z_5 + x_4z_4 + x_4z_3 + x_4z_2 + x_4z_0 + \\
\quad x_5z_6 + x_5z_7 + x_5z_4 + x_5z_3 + x_5z_2 + x_5z_1 + x_6z_5 + x_6z_3 + \\
\quad x_6z_2 + x_6z_4 + x_6z_0 + x_7z_4 + x_7z_7 + x_7z_3 + x_7z_2 + x_7z_1 + \\
\quad x_0 + x_2 + x_7 \\
0 = x_0z_6 + x_0z_3 + x_0z_0 + x_1z_6 + x_1z_7 + x_1z_5 + x_1z_4 + x_1z_2 + x_1z_1 \\
\quad + x_2z_6 + x_2z_5 + x_2z_3 + x_2z_4 + x_2z_0 + x_2z_1 + x_3z_7 + x_3z_5 + \\
\quad x_3z_3 + x_3z_4 + x_3z_2 + x_3z_0 + x_4z_7 + x_4z_6 + x_4z_4 + x_4z_3 + \\
\quad x_4z_2 + x_4z_1 + x_5z_5 + x_5z_4 + x_5z_3 + x_5z_2 + x_5z_0 + x_6z_7 + \\
\quad x_6z_3 + x_6z_2 + x_6z_4 + x_6z_1 + x_7z_4 + x_7z_3 + x_7z_2 + x_7z_0 + \\
\quad x_6 + x_1 + x_7 \\
1 = x_0z_7 + x_0z_5 + x_0z_2 + x_1z_6 + x_1z_4 + x_1z_1 + x_2z_3 + x_2z_5 + \\
\quad x_2z_0 + x_3z_7 + x_3z_4 + x_3z_2 + x_4z_6 + x_4z_3 + x_4z_1 + x_5z_6 + \\
\quad x_5z_5 + x_5z_4 + x_5z_2 + x_5z_1 + x_5z_0 + x_6z_5 + x_6z_7 + x_6z_6 + \\
\quad x_6z_3 + x_6z_0 + x_7z_6 + x_7z_7 + x_7z_5 + x_7z_4 + x_7z_2 + x_0 + x_6
\end{array}\right. \tag{5}$$

Since, there is no nonzero const term in 7 of these equations in Eq. 5, for x = 0, these 7 equations are true with probability 1. The 8th equation is true when, $x \neq 0$, so this equation is true with probability 255/256.

Since, $xy = 1(\forall x \neq 0)$ we can get:

$$\forall x \neq 0 \quad x = x^2y$$

Obviously, this equation is also true when x = 0, so we have:

$$\forall x \in GF(2^8) \quad \begin{cases} x = y \times x^2 \\ x^2 = y^2 \times x^4 \\ \quad \vdots \\ x^{128} = y^{128} \times x^{256} = y^{128} \times x \end{cases} \tag{6}$$

We might as well choose the last equation in Eq. 6. It is symmetric with respect to the exchange of x and y, so we can obtain the following two equations:

$$\begin{cases} x^{128} = y^{128}x \\ y^{128} = x^{128}y \end{cases}$$

Then we have two equations over $GF(2^8)$ are true with probability 1. Because $x \mapsto x^{128}$ is linear, each of above two equations will give eight quadratic equations with eight variables. Similarly, we can obtain these sixteen equations as Eq. 7 and 8:

$$\left\{\begin{array}{l}
0 = x_0z_1 + x_0z_5 + x_0z_3 + x_0z_7 + x_1z_5 + x_1z_3 + x_1z_4 + x_1z_7 + x_1z_6 + x_2z_2 \\
\quad + x_2z_3 + x_2z_6 + x_2z_5 + x_3z_3 + x_3z_1 + x_3z_4 + x_3z_0 + x_4z_0 + x_4z_6 + \\
\quad x_4z_5 + x_4z_2 + x_4z_1 + x_4z_7 + x_4z_3 + x_5z_0 + x_5z_7 + x_5z_5 + x_5z_3 + x_6z_6 \\
\quad + x_6z_3 + x_6z_5 + x_6z_1 + x_7z_4 + x_7z_1 + x_7z_7 + x_7z_3 + x_5 + x_3 + x_6 + x_1 \\
0 = x_0z_6 + x_0z_5 + x_0z_3 + x_0z_4 + x_0z_7 + x_1z_5 + x_1z_3 + x_1z_2 + x_1z_6 + x_2z_4 + \\
\quad x_2z_3 + x_2z_1 + x_2z_0 + x_3z_0 + x_3z_6 + x_3z_5 + x_3z_3 + x_3z_2 + x_3z_1 + x_4z_0 + \\
\quad x_4z_3 + x_4z_7 + x_4z_5 + x_5z_6 + x_5z_1 + x_5z_5 + x_5z_3 + x_6z_4 + x_6z_3 + \\
\quad x_6z_7 + x_6z_1 + x_7z_1 + x_7z_2 + x_7z_5 + x_7z_7 + x_3 + x_6 + x_1 \\
0 = x_0z_6 + x_0z_5 + x_0z_3 + x_0z_2 + x_1z_4 + x_1z_3 + x_1z_1 + x_1z_0 + x_2z_0 + x_2z_6 + \\
\quad x_2z_5 + x_2z_7 + x_2z_2 + x_2z_1 + x_3z_0 + x_3z_5 + x_3z_7 + x_3z_3 + x_4z_1 + x_4z_6 + \\
\quad x_4z_3 + x_4z_5 + x_5z_7 + x_5z_3 + x_5z_1 + x_5z_4 + x_6z_5 + x_6z_2 + x_6z_1 + x_6z_7 + \\
\quad x_7z_6 + x_7z_1 + x_7z_4 + x_7z_7 + x_3 + x_5 + x_4 + x_1 \\
0 = x_0z_4 + x_0z_1 + x_0z_3 + x_0z_0 + x_1z_0 + x_1z_3 + x_1z_2 + x_1z_5 + x_1z_1 + x_1z_6 + \\
\quad x_1z_7 + x_2z_7 + x_2z_3 + x_2z_5 + x_2z_0 + x_3z_1 + x_3z_6 + x_3z_5 + x_3z_3 + x_4z_4 + \\
\quad x_4z_3 + x_4z_1 + x_4z_7 + x_5z_7 + x_5z_2 + x_5z_5 + x_5z_1 + x_6z_6 + x_6z_1 + x_6z_4 + \\
\quad x_6z_7 + x_7z_4 + x_7z_7 + x_7z_5 + x_7z_2 + x_4 + x_3 + x_1 \\
0 = x_0z_0 + x_0z_6 + x_0z_2 + x_1z_6 + x_1z_4 + x_1z_0 + x_2z_2 + x_2z_1 + x_3z_0 + x_3z_7 + \\
\quad x_4z_6 + x_4z_3 + x_4z_0 + x_5z_6 + x_5z_4 + x_5z_3 + x_5z_1 + x_5z_5 + x_5z_0 + x_6z_3 + \\
\quad x_6z_1 + x_6z_2 + x_6z_4 + x_6z_7 + x_6z_6 + x_7z_4 + x_7z_7 + x_7z_3 + x_7z_1 + x_7z_2 + \\
\quad x_2 + x_6 + x_1 + x_7 \\
0 = x_0z_7 + x_0z_4 + x_0z_1 + x_0z_6 + x_0z_5 + x_0z_3 + x_0z_0 + x_1z_6 + x_1z_3 + x_1z_2 + \\
\quad x_1z_5 + x_1z_4 + x_1z_7 + x_1z_1 + x_2z_6 + x_2z_5 + x_2z_7 + x_2z_3 + x_2z_0 + x_2z_2 + \\
\quad x_3z_6 + x_3z_4 + x_3z_1 + x_4z_7 + x_4z_4 + x_4z_2 + x_5z_6 + x_5z_5 + x_5z_4 + x_5z_0 \\
\quad + x_5z_2 + x_5z_1 + x_6z_5 + x_6z_7 + x_6z_2 + x_6z_4 + x_6z_6 + x_7z_6 + x_7z_2 + \\
\quad x_7z_1 + x_3 + x_2 + x_4 + x_5 + x_1 \\
0 = x_0z_7 + x_0z_5 + x_0z_2 + x_0z_6 + x_0z_4 + x_0z_1 + x_0z_3 + x_1z_6 + x_1z_5 + x_1z_0 + \\
\quad x_1z_3 + x_1z_2 + x_1z_7 + x_2z_4 + x_2z_1 + x_2z_6 + x_3z_7 + x_3z_4 + x_3z_2 + x_4z_6 + \\
\quad x_4z_4 + x_4z_1 + x_4z_5 + x_4z_0 + x_4z_2 + x_5z_6 + x_5z_5 + x_5z_4 + x_5z_2 + x_5z_7 + \\
\quad x_6z_2 + x_6z_1 + x_6z_6 + x_7z_6 + x_7z_1 + x_7z_7 + x_7z_0 + x_6 + x_0 + x_2 + x_3 + x_7 \\
0 = x_0z_6 + x_0z_1 + x_0z_2 + x_0z_0 + x_1z_1 + x_1z_5 + x_1z_3 + x_1z_7 + x_2z_4 + x_2z_7 + \\
\quad x_2z_6 + x_2z_3 + x_2z_5 + x_3z_3 + x_3z_6 + x_3z_5 + x_3z_2 + x_4z_3 + x_4z_4 + x_4z_1 + \\
\quad x_4z_0 + x_5z_6 + x_5z_5 + x_5z_1 + x_5z_2 + x_5z_3 + x_5z_0 + x_5z_7 + x_6z_5 + x_6z_3 + \\
\quad x_6z_0 + x_6z_7 + x_7z_6 + x_7z_3 + x_7z_1 + x_7z_5 + x_5 + x_3
\end{array}\right. \tag{7}$$

From Eq. 7 and 8, we have 23 quadratic equations between x_i and z_j that are true with probability 1. We have explicitly generated these equations have verified that they are all linearly independent and have also verified that there are no more such equations. It is easy to find that there is no terms in x_ix_j or z_iz_j in the above 23 equations and the terms present in these equations are t = 81: these are $\{x_1z_1,\ldots x_8z_8, z_1,\ldots z_8, x_1,\ldots x_8, 1\}$:

$$\begin{cases}
\begin{aligned}0 = {} & x_0z_6 + x_0z_4 + x_0z_1 + x_1z_5 + x_1z_0 + x_2z_5 + x_2z_3 + x_2z_0 + x_3z_4 + \\ & x_3z_7 + x_4z_2 + x_4z_4 + x_4z_7 + x_5z_1 + x_5z_4 + x_5z_3 + x_6z_6 + x_6z_3 \\ & + x_6z_1 + x_7z_0 + x_7z_2 + x_7z_3 + x_5 + x_7 + z_1 + z_3 + z_5 + z_7\end{aligned} \\
\begin{aligned}0 = {} & x_0z_0 + x_0z_5 + x_0z_3 + x_1z_4 + x_1z_7 + x_2z_4 + x_2z_2 + x_2z_7 + x_3z_3 + \\ & x_3z_4 + x_3z_1 + x_4z_1 + x_4z_3 + x_4z_6 + x_5z_2 + x_5z_0 + x_5z_3 + x_6z_5 + \\ & x_6z_0 + x_6z_2 + x_6z_4 + x_6z_6 + x_6z_1 + x_7z_1 + x_7z_2 + x_7z_7 + x_3 + x_5 \\ & + x_7 + z_7 + z_6 + z_5 + z_4 + z_3\end{aligned} \\
\begin{aligned}0 = {} & x_0z_6 + x_0z_5 + x_0z_3 + x_0z_2 + x_1z_4 + x_1z_3 + x_1z_1 + x_1z_0 + x_2z_0 + \\ & x_2z_6 + x_2z_5 + x_2z_7 + x_2z_2 + x_2z_1 + x_3z_0 + x_3z_5 + x_3z_7 + x_3z_3 + \\ & x_4z_1 + x_4z_6 + x_4z_3 + x_4z_5 + x_5z_7 + x_5z_3 + x_5z_1 + x_5z_4 + x_6z_5 + \\ & x_6z_2 + x_6z_1 + x_6z_7 + x_7z_6 + x_7z_1 + x_7z_4 + x_7z_7 + x_5 + x_3 + x_1 + \\ & x_6 + x_7 + z_6 + z_5 + z_3 + z_2\end{aligned} \\
\begin{aligned}0 = {} & x_0z_6 + x_0z_1 + x_0z_3 + x_1z_3 + x_1z_0 + x_1z_2 + x_2z_1 + x_2z_2 + x_2z_5 + \\ & x_2z_0 + x_2z_4 + x_2z_6 + x_3z_2 + x_3z_1 + x_4z_7 + x_4z_6 + x_4z_0 + x_4z_5 + \\ & x_4z_3 + x_5z_6 + x_5z_0 + x_5z_1 + x_6z_6 + x_6z_5 + x_6z_2 + x_6z_4 + x_6z_7 + \\ & x_7z_7 + x_7z_5 + x_7z_0 + x_5 + x_3 + x_1 + x_4 + z_4 + z_1 + z_3 + z_0\end{aligned} \\
\begin{aligned}0 = {} & x_0z_0 + x_0z_5 + x_0z_2 + x_1z_5 + x_1z_2 + x_1z_0 + x_1z_7 + x_1z_1 + x_2z_7 + \\ & x_2z_6 + x_3z_0 + x_3z_7 + x_3z_1 + x_3z_6 + x_3z_4 + x_4z_6 + x_4z_5 + x_5z_7 + \\ & x_5z_4 + x_5z_3 + x_5z_1 + x_5z_5 + x_5z_0 + x_6z_5 + x_6z_1 + x_6z_6 + x_7z_4 + \\ & x_7z_7 + x_7z_3 + x_7z_6 + x_7z_2 + x_7z_0 + x_2 + x_3 + x_6 + x_1 + x_5 + z_2 + \\ & z_0 + z_6\end{aligned} \\
\begin{aligned}0 = {} & x_0z_7 + x_0z_4 + x_0z_1 + x_1z_6 + x_1z_7 + x_1z_5 + x_1z_4 + x_1z_1 + x_2z_6 + \\ & x_2z_3 + x_2z_0 + x_3z_5 + x_3z_3 + x_3z_1 + x_3z_0 + x_4z_7 + x_4z_4 + x_4z_2 + \\ & x_4z_6 + x_4z_1 + x_4z_5 + x_5z_6 + x_5z_7 + x_5z_0 + x_5z_2 + x_5z_1 + x_6z_5 + \\ & x_6z_3 + x_6z_0 + x_6z_4 + x_6z_6 + x_6z_1 + x_7z_4 + x_7z_7 + x_7z_5 + x_7z_0 + \\ & x_3 + x_2 + x_7 + x_1 + z_7 + z_6 + z_5 + z_4 + z_3 + z_1 + z_0\end{aligned} \\
\begin{aligned}0 = {} & x_0z_6 + x_0z_3 + x_0z_0 + x_1z_1 + x_1z_5 + x_1z_3 + x_1z_0 + x_2z_4 + x_2z_7 + \\ & x_2z_6 + x_2z_2 + x_2z_1 + x_2z_5 + x_3z_1 + x_3z_6 + x_3z_0 + x_3z_2 + x_3z_7 + \\ & x_4z_3 + x_4z_4 + x_4z_6 + x_4z_1 + x_4z_5 + x_4z_0 + x_5z_4 + x_5z_5 + x_5z_0 \\ & + x_5z_7 + x_6z_5 + x_6z_3 + x_6z_0 + x_6z_2 + x_6z_4 + x_6z_7 + x_7z_7 + x_7z_3 \\ & + x_7z_1 + x_2 + x_3 + x_7 + x_1 + z_7 + z_6 + z_5 + z_4 + z_3 + z_2 + z_1 + 1\end{aligned} \\
\begin{aligned}0 = {} & x_0z_5 + x_0z_2 + x_0z_7 + x_1z_1 + x_1z_5 + x_1z_2 + x_1z_7 + x_1z_6 + x_2z_4 + \\ & x_2z_6 + x_2z_1 + x_3z_5 + x_3z_0 + x_4z_3 + x_4z_5 + x_4z_0 + x_5z_4 + x_5z_7 + \\ & x_6z_2 + x_6z_4 + x_6z_7 + x_7z_4 + x_7z_3 + x_7z_1 + x_0 + x_7 + x_1 + z_7 + \\ & z_6 + z_2 + z_1 + z_0 + 1\end{aligned}
\end{cases} \tag{8}$$

OPTIMIZATION OF RIJNDAEL S-BOX EQUATION SYSTEM

Definition 1: Cheon and Lee (2004). 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 study.

Definition 2: An Affine-Inverse-Affine (AIA) S-box is defined as follow:

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

where, A denotes the affine transformation and I denotes the inverse transformation in GF(2^8).

Equation system of the AIA structure rijndael S-box: In the Cui *et al.* (2011), we designed a new Rijndael S-box structure named Affine-Inverse-Affine (AIA) to increase the algebraic complexity of Rijndael S-box. Now we analyze the equation system of the new Rijndael S-box.

We obtain the coefficients of the algebraic expression of the new Rijndael S-box as Table 1.

From Table 1 and the algebraic expression of Rijndael S-box, it can be seen that the algebraic expression of Rijndael S-box is very simple (i.e., only 9 terms are involved) while the new Rijndael S-box involves 255 terms and is very complex.

From Table 1, it is easy to see that the algebraic expression of the new Rijndael S-box is as follow:

$$\begin{aligned} S'(x) &= Fax^{\infty}+A6x^{01}+A9x^{02}+\ldots+E7x^{FC}+26x^{FD}+12x^{FE} \\ &= FA+A6(x^{-1})^{254}+A9(x^{-1})^{253}+\ldots+E7(x^{-1})^{3}+26(x^{-1})^{2}+12x^{-1} \\ &= FA+A6y_{253}+A9y_{252}+\ldots+E7y_2+26y_1+12y_0 \end{aligned}$$

where, $y_0 = x^{-1}$, $y_1 = (x^{-1})^2$, $y_2 = (x^{-1})^3, \ldots, y_{252} = (x^{-1})^{253}$, $y_{253} = (x^{-1})^{254}$ and it can be denoted as $S(x) = g(y_0, y_1, \ldots, y_{252}, y_{253})$.

We denote by $x^{(i)}_{0,(j,k)}$ the (j, k)-th input byte variable of the -th round S-box function. In consequence we denote the intermediate variable by $y^{(i)}_{0,(j,k)}, y^{(i)}_{1,(j,k)}, \ldots, y^{(i)}_{253,(j,k)}$ and the output variable by $z^{(i)}_{0,(j,k)}$. According to the algebraic expression of the new Rijndael S-box, the (j, k)-th S-box transformation of the -th round can be described as the following quadratic equations over GF(2^8):

$$\begin{cases} x^{(i)}_{0,(j,k)} y^{(i)}_{0,(j,k)} = 1 \\ y^{(i)}_{m,(j,k)} y^{(i)}_{0,(j,k)} = y^{(i)}_{m+1,(j,k)}, (0 \le m \le 253, \text{where } m+1 \text{ is plus 1 mod 254}) \\ z^{(i)}_{0,(j,k)} = g(y^{(i)}_{0,(j,k)}, y^{(i)}_{1,(j,k)}, \ldots, y^{(i)}_{7,(j,k)}) \end{cases} \tag{9}$$

where, $0 \le i \le 9$, $0 \le j$, $k \le 3$.

Table 1: Coefficients of algebraic expression of the new Rijndael S-box

C (mn)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	FA	A6	A9	E5	DE	5A	05	FB	5C	AA	64	CB	A1	87	6A	6C
1	E4	87	93	6A	76	E5	66	09	43	0C	91	92	03	8F	63	30
2	54	99	E9	30	EE	BF	F2	E6	71	4E	90	D5	18	85	45	FA
3	7E	73	0E	13	8B	5B	08	8B	C8	3B	6A	10	87	09	FB	47
4	28	AF	C5	20	0B	8D	74	D5	59	37	19	C9	2A	4F	02	C1
5	91	F1	50	83	9B	42	87	4A	42	F2	74	0C	4F	2D	49	AE
6	DA	25	64	58	CD	FE	1B	D2	7D	F8	66	A8	6D	2A	A9	7E
7	21	C3	3F	D2	EC	C9	7A	AC	0D	CC	7F	D3	35	25	C2	6F
8	BF	86	07	91	5E	C5	75	4E	C1	83	E8	CA	B0	E9	75	B6
9	07	16	F8	7B	49	D5	FA	AD	5B	5F	C2	19	12	13	C5	20
A	99	B3	44	9F	F2	71	9B	38	7A	AE	A5	0D	48	C4	EF	1E
B	F4	09	8F	D1	2F	88	60	9B	E9	9F	75	66	69	7C	23	62
C	05	DE	30	DE	BB	D5	96	4D	52	AB	77	32	09	B4	3F	AB
D	FF	97	D6	FB	FE	59	DB	BA	15	1A	64	2D	02	F8	5D	3B
E	74	EE	1B	82	C8	63	F8	F4	BF	49	50	5A	7C	FC	46	47
F	C9	97	ED	52	59	D3	01	56	79	DB	C7	9A	E7	26	12	00

Table 2: Comparisons of equation systems of Rijndael S-box

Parameters	Notation	Equation system Murphy and Robshaw (2002)	Equation system Li and Chen (2004)	Equation system Xiao and Zhang (2008)	First equation system	Second equation system
No. of equations of each S-box	R	24.0	17.0	16	23	255
No. of terms of each S-box	T	41.0	34.0	28	81	510
Size of the S-box	s	8.0	8.0	3	8	8
Resistance of algebraic attacks of the S-box		9.6	9.6	2^8	$2^{22.9}$	2^{160}

The last linear equation can be seen as another linear transformation after S-box transformation. From the Eq. 9, it can be seen that each S-box has 255 quadratic equations. Then, the total 255 quadratic equations of the new Rijndael S-box are obtained.

These 255 quadratic equations comprise a total of 510 terms: $1, y^{(i)}_{0,(j,k)}, \ldots, y^{(i)}_{253,(j,k)}, x^{(i)}_{0,(j,k)}y^{(i)}_{0,(j,k)}, (y^{(i)}_{0,(j,k)})^2, y^{(i)}_{1,(j,k)}y^{(i)}_{0,(j,k)}, y^{(i)}_{2,(j,k)}y^{(i)}_{0,(j,k)}, \ldots, y^{(i)}_{253,(j,k)}y^{(i)}_{0,(j,k)}$.

For the new Rijndael S-box, it is easy to obtain that $t = 510$, $r = 255$, $n = 8$. According to the definition 1, it can be obtained that $\Gamma = 31.875^{32} \approx 2^{160}$.

Comparison with the existing equation systems: Table 2 shows the comparison results. As can be seen from Table 2 for each S-box, the equation system (Murphy and Robshaw, 2002) comprises 24 quadratic equations of 41 terms over GF(2^8) and the equation system (Li and Chen, 2004) comprises 17 quadratic equations of 34 terms over GF(2^8) while our equation system comprises 255 quadratic equations of 510 terms over GF(2^8).

According to the definition of RAA, we can obtain that the RAA of the equation system (Murphy and Robshaw, 2002; Li and Chen, 2004; Xiao and Zhang, 2008) are 9.6, 9.6 and 2^8, respectively. However, our equation system has the following property: $\Gamma = 2^{160}$. Cheon and Lee (2004) pointed out that should be greater than 2^{32} for secure ciphers.

This suggests that the complexity of solving our equation system is much more than that of solving other existing equation systems. Our work is helpful to improving the security of Rijndael cipher.

CONCLUSION

In this study, a new approach to generating the multivariate quadratic equation system over GF(2) is proposed and an equation system over GF(2^8) is proposed to describe the new Rijndael S-box. Firstly, the construction principle and the algebraic expression of Rijndael S-box are described. Secondly, a new approach to generating the multivariate quadratic equation system over GF(2) is proposed and the generation process of the multivariate quadratic equations is given explicitly. Finally, an equation system over GF(2^8) is proposed to describe the new Rijndael S-box and it suggest that the new equation system has stronger resistance against algebraic attacks than other existing equation systems.

ACKNOWLEDGMENT

The study was supported by the National Natural Science Foundation of China (No. 61173188, 61173187, 61272074), the Educational Commission of Anhui Province, China (No. KJ2013A017), the Research Fund for the Doctoral Program of Higher Education (No. 20133401110004) and the Doctoral Research Start-up Funds Project of Anhui University. The authors are very grateful to Chinchen Chang and the anonymous referees for their detailed comments and suggestions regarding this study.

REFERENCES

Chen, Q., Z. Tang, Y. Li, Y. Niu and J. Mo, 2011. Research on encryption algorithm of data security for wireless sensor network. J. Comput. Inform. Syst., 7: 369-376.

Cheon, J.H. and D.H. Lee, 2004. Resistance of S-Boxes Against Algebraic Attacks. In: Fast Software Encryption, Roy, B. and W. Meier (Eds.)., Springer-Verlag, Berlin, Heidelberg, pp: 83-93.

Courtois, N.T. and J. Pieprzyk, 2002. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. In: Advances in Cryptology, Zheng, Y. (Ed.). Volume 2501, Springer, Heidelberg Germany, ISBN: 978-3-540-00171-3, pp: 267-287.

Cui, J., L. Huang, H. Zhong, C. Chang and W. Yang, 2011. An improved AES S-Box and its performance analysis. Int. J. Innovative Comput. Inform. Control, 7: 2291-2302.

Demirci, H., M.S. Sagiroglu and M.O. Kulekci, 2013. A time-memory trade-off approach for the solution of nonlinear equation systems. Turkish J. Electrical Eng. Comput. Sci., 21: 186-197.

Ghosh, S. and A. Das, 2012. Improvements of algebraic attacks based on structured gaussian elimination. https://eprint.iacr.org/2012/176.pdf

Hussain, I., T. Shah, H. Mahmood and M.A. Gondal, 2013. A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Comput. Applic., 22: 1085-1093.

Kim, J., S. Hong and B. Preneel, 2007. Related-key rectangle attacks on reduced AES-192 and AES-256. Proceedings of the 14th International Workshop on Fast Software Encryption, March 26-28, 2007, Luxembourg, pp: 225-241.

Li, N. and W. Chen, 2004. A new system of multivariate quadratic equations for rijndael. J. Electron. Inform. Technol., 26: 1990-1995.

Murphy, S. and M.J.B. Robshaw, 2002. Essential algebraic structure within the AES. Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, August 18-22, 2002, London, pp: 1-16.

Xiao, H.P. and G.J. Zhang, 2008. The improvement on algebraic system of multivariate quadrtic equations for Rijndael. J. Electron. Inform. Technol., 30: 2459-2463.

Zhang, W., W. Wu, L. Zhang and D. Feng, 2007. Improved related-key impossible differential attacks on reduced-round AES-192. Proceedings of the 13th International Workshop on Selected Areas in Cryptography, August 17-18, 2006, Montreal, Canada, pp: 15-27.

Zhang, X., Q. Wang, B. Wang and H. Kan, 2011. A constructive method of algebraic attack with less Keystream bits. IEICE Trans. Fundamentals Electron. Commun. Comput. Sci., 94: 2059-2062.