Generation and Optimization of Rijndael S-box Equation System

Jie Cui, Hong Zhong, Jiankai Wang and Runhua Shi
1School of Computer Science and Technology, Anhui University, Hefei, 230039, China
2School 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(2³) 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 secure 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 Daemen 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(2³). Cheon and Lee (2004) proposed a new system of multivariate quadratic equations over GF(2³) 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(2³) 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(2³), 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:

\[
I(x) = \begin{cases} 
(xy)^{25} & x \neq 0 \\
0 & x = 0 
\end{cases}
\]

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


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

\[ A(x) = Lx + x \cdot 63 \]

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

\[ S(x) = A \cdot I = A(I(x)) \]

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

\[ S(x) = 05x^F + 09x^{F^2} + F9x^{F^3} + 25x^{F^4} + F4x^{F^5} + 01x^{F^6} + B5x^{F^7} + 8Fx^2 + 63 \]

**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)→GF(2^8). We call these functions, respectively g and f and we call S = f ◦ 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 ¥ 0, i.e.:

\[
\begin{bmatrix}
\sum_{i=1}^{8} x_i^t
\end{bmatrix}
\begin{bmatrix}
\sum_{i=1}^{8} x_i^t
\end{bmatrix}
= \sum_{i=1}^{8} 0 \cdot t^i + 1
\]

Expanding the Eq. 1, we have:

\[
\sum_{i=1}^{8} \sum_{j=1}^{8} (x_i y_j) m_{00} (t^{i+j}) m_{00} = \sum_{i=1}^{8} 0 \cdot t^i + 1
\]

where, \( m(t) = t^4 + t^3 + t^2 + t + 1 \).

Comparing the both sides coefficients of \( t^k (0 \leq k \leq 8) \) in Eq. 1, we can obtain the 8 multivariate quadratic equations of inverse transformation. Since, \( y \rightarrow z \) 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 \( c_{0} , ..., c_{0} \) of \( t^k (0 \leq k \leq 8) \). Firstly, we give the computation process of the coefficients \( c_{0} , ..., c_{0} \).

We note \( (x_\gamma, x_\eta) = x, (y_\gamma, y_\eta) = y \) and \( (z_\gamma, z_\eta) = z \). i.e.:

\[
x = \sum_{i=1}^{8} x_i t^i, y = \sum_{i=1}^{8} y_i t^i \text{ and } z = \sum_{i=1}^{8} z_i t^i
\]

We have:

\[
x \cdot y \cdot t^i = (x_\gamma y_\gamma + x_\gamma y_\eta + x_\eta y_\gamma + x_\eta y_\eta) t^i + (x_\gamma y_\gamma + x_\eta y_\gamma + x_\gamma y_\eta + x_\eta y_\eta) t^i
\]

\[
\cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\eta + x_\gamma y_\eta) t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\eta + x_\gamma y_\eta) t^i
\]

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

**Step 1: x \cdot y \cdot t^i modulo:**

\[ x_\gamma y_\gamma \cdot t^i + x_\gamma y_\gamma \cdot t^i + x_\gamma y_\gamma \cdot t^i + x_\gamma y_\gamma \cdot t^i = R1 \]

**Step 2: R1 modulo:**

\[ (x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i = R2 \]

**Step 3: R2 modulo:**

\[ (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i = R3 \]

**Step 4: R3 modulo:**

\[ (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i + (x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma + x_\gamma y_\gamma) \cdot t^i = R4 \]

**Step 5: R4 modulo:**

\[ (x\dot{y} + x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^{10} \]

Step 6: R5 module:

\[ (x\dot{y} + x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^6 + (x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^6 = R5 \]

Step 7: R6 module:

\[ (x\dot{y} + x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^6 + (x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^6 = R6 \]

\[ R7 = (x\dot{y} + x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^6 + (x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^6 + (x_1 y_2 + x_2 y_3 + x_3 y_4 + x_4 y_5 + x_5 y_6 + x_6 y_7 + x_7 y_8 + x_8 y_9, y_9, y_10) \cdot t^6 = R7 \]

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:

\[ y = A^{-1}z + A^{-1} \cdot 63 = A^{-1}z^+05 \]

Where:

\[
\begin{bmatrix}
0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

Then we get:

\[
\begin{bmatrix}
y_1 = z_1 + z_2 + z_3 \\
y_2 = z_1 + z_2 + z_3 \\
y_3 = z_1 + z_2 + z_3 \\
y_4 = z_1 + z_2 + z_3 \\
y_5 = z_1 + z_2 + z_3 \\
y_6 = z_1 + z_2 + z_3 + 1 \\
y_7 = z_1 + z_2 + z_3 + 1 \\
y_8 = z_1 + z_2 + z_3 + 1
\end{bmatrix}
\]
Substituting Eq. 4 into 3, we obtain 8 multivariate quadratic equations of S-box as Eq. 5:

\[ \forall x \in \text{GF}(2^4), \quad x = y \times x^2 \]
\[ x^4 = y^4 \times x^4 \]
\[ x^{128} = y^{128} \times x^{256} = y^{128} \times x \]

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:

\[ x^{128} = y^{128} \times x \]
\[ y^{128} = x^{128} \times y \]

Then we have two equations over \( \text{GF}(2^4) \) 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:

\[ \forall x \in \text{GF}(2^4), \quad x = y \times x^2 \]
\[ x^4 = y^4 \times x^4 \]
\[ x^{128} = y^{128} \times x^{256} = y^{128} \times x \]

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:

\[ \forall x \neq 0, \quad x = x^y \]

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

\[ 0 = x^y + x^0 \]

From Eq. 7 and 8, we have 23 quadratic equations between \( x \) and \( z \) 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 $x_i$ or $z_i$ in the above 23 equations and the terms present in these equations are $t = 81$; these are $\{x_1z_2, x_2z_3, x_3z_4, x_4z_5, x_5z_6, x_6z_7, x_7z_8, x_8z_9, x_9z_{10}, x_{10}z_{11}\}$:

\[
\Gamma = ((t-r)\cdot n)^{\phi(n)}
\]

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:

\[
S(x) = A \cdot I \cdot A
\]

where, $A$ denotes the affine transformation and $I$ denotes the inverse transformation in $\mathbb{GF}(2^3)$.

**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:

\[
S'(x) = A \cdot F(A \cdot x)^{12} + A \cdot 26 \cdot x^{12} + 26 \cdot x^{12}
\]

\[
S'(x) = A \cdot F(A \cdot x)^{12} + A \cdot 26 \cdot x^{12} + 26 \cdot x^{12}
\]

where, $y_6 = x^{-1}$, $y_7 = (x^{-1})^2$, $y_8 = (x^{-1})^3$, $y_{22} = (x^{-1})^{22}$, $y_{23} = (x^{-1})^{23}$, $y_{24} = (x^{-1})^{24}$ and it can be denoted as $S(x) = g(y_6, y_7, y_8, y_{22}, y_{23}, y_{24})$.

We denote by $x_{(i,j)}^{(0)}$, the (j, k)th input byte variable of the $\mathcal{G}$th round S-box function. In consequence we denote the intermediate variable by $y_{(i,j)}^{(0)}, y_{(i,j)}^{(1)}, \ldots, y_{(i,j)}^{(255)}$ and the output variable by $y_{(i,j)}^{(255)}$. According to the algebraic expression of the new Rijndael S-box, the (j, k)th S-box transformation of the $\mathcal{G}$th round can be described as the following quadratic equations over $\mathbb{GF}(2^3)$:

\[
\begin{align*}
&x_{(i,j)}^{(0)} = 1 \\
&y_{(i,j)}^{(0)} = y_{(i,j)}^{(0)} (0 \leq m \leq 255, \text{where } m+1 \text{ mod } 254) \\
&\psi_{(i,j)}^{(0)} = g(y_{(i,j)}^{(0)}, y_{(i,j)}^{(1)}, \ldots, y_{(i,j)}^{(255)})
\end{align*}
\]

where, $0 \leq i, j, k \leq 3$.
Table 1: Coefficients of algebraic expression of the new Rijndael S-box

<table>
<thead>
<tr>
<th>C (mm)</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>FA</td>
<td>A6</td>
<td>A9</td>
<td>ES</td>
<td>DE</td>
<td>5A</td>
<td>65</td>
<td>FB</td>
<td>5C</td>
<td>AA</td>
<td>64</td>
<td>CB</td>
<td>A1</td>
<td>87</td>
<td>6A</td>
</tr>
<tr>
<td>1</td>
<td>E4</td>
<td>87</td>
<td>93</td>
<td>6A</td>
<td>76</td>
<td>65</td>
<td>69</td>
<td>43</td>
<td>0C</td>
<td>91</td>
<td>92</td>
<td>03</td>
<td>8F</td>
<td>63</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>54</td>
<td>99</td>
<td>93</td>
<td>30</td>
<td>EE</td>
<td>BF</td>
<td>F2</td>
<td>E6</td>
<td>71</td>
<td>4E</td>
<td>90</td>
<td>D5</td>
<td>18</td>
<td>85</td>
<td>45</td>
</tr>
<tr>
<td>3</td>
<td>7E</td>
<td>73</td>
<td>0E</td>
<td>13</td>
<td>8B</td>
<td>5B</td>
<td>0B</td>
<td>8D</td>
<td>C8</td>
<td>3B</td>
<td>6A</td>
<td>10</td>
<td>87</td>
<td>09</td>
<td>FB</td>
</tr>
<tr>
<td>4</td>
<td>28</td>
<td>AF</td>
<td>C5</td>
<td>20</td>
<td>0B</td>
<td>BD</td>
<td>7D</td>
<td>74</td>
<td>59</td>
<td>37</td>
<td>19</td>
<td>C9</td>
<td>2A</td>
<td>4F</td>
<td>02</td>
</tr>
<tr>
<td>5</td>
<td>91</td>
<td>F1</td>
<td>50</td>
<td>83</td>
<td>9B</td>
<td>42</td>
<td>87</td>
<td>4A</td>
<td>42</td>
<td>F2</td>
<td>74</td>
<td>0C</td>
<td>4F</td>
<td>2D</td>
<td>49</td>
</tr>
<tr>
<td>6</td>
<td>DA</td>
<td>25</td>
<td>64</td>
<td>58</td>
<td>CD</td>
<td>FE</td>
<td>1B</td>
<td>D2</td>
<td>7D</td>
<td>F8</td>
<td>66</td>
<td>A8</td>
<td>6D</td>
<td>2A</td>
<td>A9</td>
</tr>
<tr>
<td>7</td>
<td>21</td>
<td>C3</td>
<td>3F</td>
<td>D2</td>
<td>AC</td>
<td>EC</td>
<td>9C</td>
<td>7A</td>
<td>AC</td>
<td>0D</td>
<td>CC</td>
<td>7F</td>
<td>D3</td>
<td>35</td>
<td>C2</td>
</tr>
<tr>
<td>8</td>
<td>BF</td>
<td>86</td>
<td>07</td>
<td>91</td>
<td>SE</td>
<td>C5</td>
<td>75</td>
<td>4E</td>
<td>C1</td>
<td>83</td>
<td>F8</td>
<td>CA</td>
<td>9D</td>
<td>7E</td>
<td>7E</td>
</tr>
<tr>
<td>9</td>
<td>05</td>
<td>1E</td>
<td>9F</td>
<td>01</td>
<td>89</td>
<td>DC</td>
<td>75</td>
<td>7A</td>
<td>05</td>
<td>4F</td>
<td>1E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
<td>7E</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Notation</th>
<th>Equation system</th>
<th></th>
<th>Equation system</th>
<th></th>
<th>Equation system</th>
<th></th>
<th>First equation system</th>
<th></th>
<th>Second equation system</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of terms of each S-box</td>
<td>T</td>
<td></td>
<td>41.0</td>
<td></td>
<td>34.0</td>
<td></td>
<td>28.0</td>
<td>8I</td>
<td>510</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Size of the S-box</td>
<td>s</td>
<td></td>
<td>8.0</td>
<td></td>
<td>0.0</td>
<td></td>
<td>8.0</td>
<td>0.0</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resistance of algebraic attacks of the S-box</td>
<td>r</td>
<td></td>
<td>9.6</td>
<td></td>
<td>9.6</td>
<td></td>
<td>2.0</td>
<td>2**0.5</td>
<td>2**0.5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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: \( y_{x_{i},y_{j}}^{(0)}, \ldots, y_{x_{i},y_{j}}^{(0)} \), \( y_{x_{i},y_{j}}^{(0)} \), \( (y_{x_{i},y_{j}}^{(0)})^2 \), \( y_{x_{i},y_{j}}^{(0)} \), \( y_{x_{i},y_{j}}^{(0)} \), \( y_{x_{i},y_{j}}^{(0)} \), \( y_{x_{i},y_{j}}^{(0)} \), \( y_{x_{i},y_{j}}^{(0)} \).

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 \( G = 31.875^{15} = 2^{160} \).

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) and the equation system (Li and Chen, 2004) comprises 17 quadratic equations of 34 terms over GF(2) while our equation system comprises 255 quadratic equations of 510 terms over GF(2). 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**, respectively. However, our equation system has the following property: \( G = 2^{160} \). Cheon and Lee (2004) pointed out that should be greater than 2 to 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**k) 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**k) 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 Chinchhen Chang and the anonymous referees for their detailed comments and suggestions regarding this study.
REFERENCES


