A Novel Method for Designing Dynamical Key-Dependent S-Boxes based on Hyperchaotic System

Jun Peng, Shangzhu Jin, Liang Lei, Rong Jia
1School of Electrical and Information Engineering
Chongqing University of Science and Technology, Chongqing, China
pengjun70@126.com, gogcq@163.com, cqlei.l@163.com
*Corresponding author
2Office of Finance and Accounting, Chongqing University of Science and Technology, Chongqing, China, jiarong70@126.com

Abstract

The substitution box (S-box) is found in many block cipher, and it is a very important component. Since the chaotic system has several significant advantageous properties desirable for cryptosystem, the design of S-box using chaos has attracted a great deal of attention in recent years. In this paper, a novel method for designing key-dependent S-boxes based on a four-dimensional hyperchaotic Chen system has been presented. The design process for constructing S-boxes is described in detail and the results of numerical analysis indicate that all the criteria for S-boxes including bijection, nonlinearity, SAC, BIC and differential approximation probability can be fulfilled. Furthermore, the S-box's sensitivity to the secret key is also conducted. All the results in this paper have shown that the presented method is a good candidate for designing dynamical S-boxes that can be widely used in block cipher.

Keywords: Hyperchaotic System, Dynamical S-Box, Block Cipher, Key-Dependence

1. Introduction

Since the advantageous properties such as the ergodic, mixing and random-like behavior of chaos in constructing cryptosystems, the design of chaos-based cipher using chaos has attracted a great deal of attention over the past years [1-7]. In the meanwhile, as the substitution boxes (S-boxes) are core and only nonlinear component of block cryptosystems, recent research shows that it is a promising direction to use chaos to design S-boxes. Tang and Liao et al [8] presented a method to obtain cryptographically strong dynamic S-boxes based on the iterating discretized chaotic map. Fatih [9] presented a design methodology for S-boxes based on continuous-time chaotic Lorenz system. Wang et al [10] presented a method for designing S-boxes based on chaotic neural network which has sixteen and eight neurons in two layers. After that, Wang et al [11] studied a novel method to design S-box using chaotic map and genetic algorithm, where the problem of constructing S-box was transformed to a traveling salesman problem. In [12], Xu et al proposed a new method to obtain cryptographically strong S-boxes based on spatiotemporal chaotic system, in which the discretized Baker map and affine transformation are used orderly by an algorithm to shuffle the table generated by the spatiotemporal chaotic system.

In this paper, a novel method for generating dynamical key-dependent S-boxes based on iterating a four-dimensional hyperchaotic Chen system is presented. One of the main motivations for using hyperchaos is that we want to achieve a more sophisticated chaotic sequence to generate the S-box.

The remaining part of the paper is organized as follows. The several cryptographic properties that are required to design a “good” S-box are firstly described. Then, a novel method for generating dynamical key-dependent S-box is presented. Following that, theoretical analyses and simulation test are provided. Finally, conclusions are drawn.

2. Cryptographic properties of s-boxes

In general, the following cryptographic properties are widely accepted as the essential properties for “good” S-boxes and can be used to evaluate the S-box.
2.1. Bijection property

For an S-box, the following method is presented to check the bijective property [4]. The boolean function \( f(x) = (f_1, f_2, \ldots, f_n) \) is bijective if it satisfies

\[
wt\left(\sum_{i=1}^{n} a_i f_i\right) = 2^{n-1}
\]

(1)

where the \( a_i \in \{0,1\} \), \( (a_1, a_2, \ldots, a_n) \neq (0,0,\ldots,0) \) and \( wt(\cdot) \) is the Hamming weight. The above condition for the boolean function \( f(x) \) to be bijective guarantees that any linear combination of \( f_i \) has Hamming weight \( 2^{n-1}(i = 1,2,\ldots,n) \).

2.2. Nonlinearity property

The nonlinearity of the boolean function \( f(x) \) can be represented by the Walsh spectrum:

\[
N_f = 2^{n-1} \left(1 - 2^{-n} \max_{\omega \in GF(2^n)} |S_f(\omega)|\right)
\]

(2)

where \( N_f \) is the nonlinearity of \( f(x) \) and the Walsh spectrum of \( f(x) \) is defined as

\[
S_f(\omega) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega}
\]

(3)

where \( \omega \in GF(2^n) \) and \( x \cdot \omega \) denotes the dot-product of \( x \) and \( \omega \).

2.3. Strict avalanche criterion (sac)

In [6], the dependence matrix is constructed to ascertain whether a given S-box satisfies the strict avalanche criterion. If an S-box is said to satisfy the SAC, each of the output bits should change with a probability of one half whenever a single input bit is complemented. It is expected that the mean value of the dependence matrix is close to one half if the S-box satisfies the SAC.

2.4. Output bit independence criterion (bic)

The output bit independence is another important property that should be satisfied for S-boxes. This criterion is firstly presented by Webster and Tavares [14] and means that all avalanche variable couples must be independent for the set of avalanche vectors generated by the inverse of the bits of a single plaintext [9]. Assume the boolean functions in the \( 8 \times 8 \) S-box are \( f_1, f_2, \ldots, f_8 \). If \( f_j \) and \( f_k \) satisfy BIC, \( F_i = f_j \oplus f_k \) \((j \neq k, 1 \leq j, k \leq 8)\) should also satisfy nonlinearity and SAC.

2.5. Differential approximation probability

For a S-box, it should ideally have differential uniformity, which means that an input differential \( \Delta x \) should uniquely map to an output differential \( \Delta y \), thereby ensuring a uniform mapping probability for each \( x \). The differential approximation probability is a measure for differential uniformity and is defined as [15]

\[
DP_f = \max_{\Delta y \in GF(2^n)} \left(\frac{\# \{ x \in X | f(x) \oplus f(x \oplus \Delta x) = \Delta y \}}{2^n}\right)
\]

(4)

where \( X \) is the set of all possible input values, and \( 2^n \) is the number of its elements.
3. The method of designing s-boxes

3.1. Hyperchaotic chen system

Compared with the simple chaotic map, a hyperchaotic system has stronger spatiotemporal complexity and mixture property because of having more than one positive Lyapunov exponent. The inherent merits of hyperchaos form the solid theoretical foundation for excellent S-boxes construction.

Research results in [16, 17] indicate that Chen system is a three-order system which can be easily implemented by circuits, and has better three-dimensional dynamical properties in phase space than Lorenz system and Chua's system. Chen system is described by the following system of differential equations [18]:

\[
\begin{align*}
\dot{x} &= a(y - x), \\
\dot{y} &= (b - a)x - xz + by, \\
\dot{z} &= xy - cz.
\end{align*}
\]

where \((x, y, z)\) are the state variables, and \((a, b, c)\) are control parameters, and when \(a = 35, b = 28, c = 3\), the system is chaotic. By introducing a nonlinear feedback controller to the first equation of system (5), the following hyperchaotic system (6) is obtained:

\[
\begin{align*}
\dot{x} &= a(y - x) + u, \\
\dot{y} &= dx - xz + by, \\
\dot{z} &= xy - cz, \\
\dot{u} &= yz + ru.
\end{align*}
\]

where \((x, y, z, u)\) are the state variables, and \((a, b, c, d, r)\) are control parameters. When \(a = 35, b = 12, c = 3, d = 7, 0 \leq r \leq 0.085\), the system (6) is chaotic, and when \(a = 35, b = 12, c = 3, d = 7, 0.085 < r < 0.798\), is hyperchaotic. In [19], the author show that the system (6) has a hyperchaotic attractor with two positive Lyapunov exponents \(\lambda_1 = 0.56, \lambda_2 = 0.11\) when \(a = 35, b = 12, c = 3, d = 7, r = 0.5\). The hyperchaotic attractors with initial conditions \((0.35, 0.35, 0.35, 0.35)\) are shown in Figure 1 (a) - (f). The results show that the system (6) has a strong ability of generating complex hyperchaotic attractors via some simple control inputs. We believe that the S-boxes generated by using the hyperchaotic system (6) should have the desirable cryptographic properties.
3.2. Description of designing key-dependent 8x8 s-boxes

In this section, we present an approach to construct 8x8 S-box with a 64-bits key. Firstly, the secret key is mapped to the initial condition and control parameter for the hyperchaotic system (6); secondly, iterate the system (6) to generate a hyperchaotic sequence which is subsequently used to construct the S-box. In the system (6), we make sure that parameter $r$ is located within (0.085,0.798) to obtain hyperchaotic sequences. The detail description of designing S-box is as follows:

**Step 1.** Randomly given a 64-bits key $K = K_1 K_2 ... K_8$, calculate the following initial condition $(x_0, y_0, z_0, u_0)$ and parameter $r$ of the system (6):

\[
x_0 = \frac{K_1^{\epsilon \delta} \oplus K_2^{\epsilon \delta}}{256}
\]

\[
y_0 = \frac{K_3^{\epsilon \delta} \oplus K_4^{\epsilon \delta}}{256}
\]

\[
z_0 = \frac{K_5^{\epsilon \delta} \oplus K_6^{\epsilon \delta}}{256}
\]

\[
u_0 = \frac{K_7^{\epsilon \delta} \oplus K_8^{\epsilon \delta}}{256}
\]

\[
r = d_1 + \frac{\left( K_1 \oplus K_2 \oplus K_3 \oplus K_4 \right)^{\epsilon \delta} \oplus \left( K_5 \oplus K_6 \oplus K_7 \oplus K_8 \right)^{\epsilon \delta} \cdot (d_2 - d_1)}{256}
\]

where $d_1 = 0.085$, $d_2 = 0.798$, $g = (K_1 + K_2 + \cdots + K_8) \mod 8$, symbol $W^{\epsilon \delta}$ and $W^{\epsilon \delta}$ means cyclic left-shift and right-shift by $g$ bits of $W$, respectively. Besides, the iteration times of the system (6) from the initial value is defined as:

\[
N = [(K_1 + K_2 + \cdots + K_8) \mod 256]^{\epsilon \delta}
\]

**Step 2.** Define an integer array $S$ with no items in its initial state.
Step 3. Iterate the system (6) for $N$ times from the initial value $(x_0, y_0, z_0, u_0)$ by using fourth-order Runge-Kutta methods. Here, to avoid the transient effect, the first 50 iterations are considered.

Step 4. Assume $(x_N, y_N, z_N, u_N)$ denotes the $N$-th iteration value of the system (6), and let $S' = \text{floor}(x_N^2 + y_N^2 + z_N^2 + u_N^2) \mod 256$.

Step 5. If $S'$ is not in $S$, add $S'$ into $S$. If $S$ has 256 items, translate $S$ into $8 \times 8$ S-box and the process is finished. Otherwise, let $(x_N, y_N, z_N, u_N)$ act as new initial value $(x_0, y_0, z_0, u_0)$ and repeat Step 3 to Step 5.

As we know, the chaotic system (6) is extremely sensitive to the initial values and control parameters which are determined by the secret key. Hence, a great deal of completely different S-boxes can be generated with a tiny change in the secret key.

3.4. Properties analysis of the s-boxes

In this section, we construct a key-dependent S-box with a random key “Pg4fvT8n”. According to the algorithm described in above section, an $8 \times 8$ S-box is generated and shown in Table 1.

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

Then, we randomly select 200 different keys to obtain 200 S-boxes and the properties test results are as follows:

(1) All the S-boxes are bijective.

(2) Maximum, minimum and mean nonlinearity of the S-boxes is 110, 92 and 103.47, respectively (please see Figure 2). Especially, of the 93.00% of the S-boxes whose nonlinearity are among [100, 108], only 2.00% are among [92, 95], indicating that most of the S-boxes have a high nonlinearity property.
(3) The dependence matrix of the S-box in Table 1 is calculated by using the method proposed in [14] and shown in the following, the mean value is 0.4990.

\[
\begin{bmatrix}
0.4844 & 0.4688 & 0.4531 & 0.4688 & 0.4219 & 0.4375 & 0.4375 & 0.5000 \\
0.5469 & 0.4688 & 0.5781 & 0.5000 & 0.5156 & 0.5000 & 0.4688 & 0.4688 \\
0.5000 & 0.4531 & 0.5625 & 0.4844 & 0.4844 & 0.4688 & 0.5000 & 0.4844 \\
0.5313 & 0.5156 & 0.4688 & 0.5313 & 0.5000 & 0.4063 & 0.4688 & 0.5313 \\
0.5156 & 0.5156 & 0.4375 & 0.5313 & 0.5625 & 0.5156 & 0.3750 & 0.4844 \\
0.5156 & 0.5156 & 0.5313 & 0.5000 & 0.5000 & 0.5156 & 0.4844 & 0.5313 \\
0.4844 & 0.5000 & 0.5938 & 0.5156 & 0.4844 & 0.4688 & 0.5156 & 0.5156 \\
0.5156 & 0.4844 & 0.5781 & 0.5156 & 0.4844 & 0.5469 & 0.5625 & 0.5313
\end{bmatrix}
\]

We found that all the mean values of the dependence matrices of 200 S-boxes are located within [0.48, 0.52] (see Figure 3), which are close to the ideal value 0.5, indicating that all the S-boxes have excellent SAC property.

(4) The mean values of nonlinearities of $f_j \oplus f_k$ are greater than 100 and the mean value of dependence matrices of $f_j \oplus f_k$ are close to 0.5, indicating that all the S-boxes approximately fulfill the requirement of BIC property.
(5) Most of the maximum values of $DP_f$ are smaller than 5%, indicating that these S-boxes can resist the differential cryptanalysis to some extent.

(6) In order to investigate the S-box’s sensitivity to the secret keys, the correlation coefficients between the S-boxes with key1 and key2 are calculated. In here, key1 is set to “Pg4fvT8n” and key2 is set to “Qg4fvT8n”, where only the first letter ‘P’ of key1 is changed to ‘Q’. The S-boxes generated by key1 and key2 are shown in Table 1 and Table 2, respectively, and the correlation coefficient between them is -0.0157, indicating that the S-boxes are very sensitive to the keys.

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

4. Conclusion

S-box is a very important component of block cipher. In this paper, a novel method for generating dynamical key-dependent S-boxes based on hyperchaotic Chen system is presented. The results of numerical analysis on these S-boxes have shown that all the cryptographic properties such as bijection, nonlinearity, SAC, BIC and differential approximation probability for a strong S-box are approximately fulfilled, and the S-box’s sensitivity to the secret key is also satisfied. Furthermore, since a great deal of S-boxes can be obtained easily by the presented method, it is also suitable for designing block cipher with dynamical S-boxes.

5. Acknowledgements

The work described in this paper was supported by the Natural Science Foundation Project of CQ CSTC under Grant No. 2010BB2284; the First Batch of Supporting Program for University Excellent Talents in Chongqing; and Research Project of Chongqing University of Science and Technology under Grant No. CK2011Z17. The authors would like to thank the anonymous reviewers for their valuable suggestions.

6. References