S-box design method based on improved one-dimensional discrete chaotic map

Dragan Lambić a,b

aDepartment for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam; bFaculty of Mathematics & Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam

ABSTRACT
A new method for obtaining random bijective S-boxes based on improved one-dimensional discrete chaotic map is presented. The proposed method uses a new special case of discrete chaotic map based on the composition of permutations, in order to overcome the problem with potentially short length of the orbits. The proposed special case is based on the composition of permutations and sine function and has a larger minimum length of the orbits compared to the previous special case of the discrete-space chaotic map. The results of performance test show that the example of S-box generated by the proposed method has good cryptographic properties. The proposed method can achieve large key space, which makes it suitable for generation of larger S-boxes, and the process of generation of S-boxes is not affected by approximations of any kind. Also, proposed method has potential to operate at greater speed and with smaller memory requirements than previous S-box generation method based on discrete space chaotic map, which can be particularly useful for lightweight devices such as wireless sensor networks.

1. Introduction
Cryptographic algorithms used for encryption are divided into two main categories: stream and block ciphers. Stream ciphers are designed to encrypt one bit at the time while block ciphers operate on a group of bits of fixed length which is called a block. Shannon’s property of confusion is essential for block ciphers because it obscures connection between secret key used for encryption and encrypted bits. Substitution box (S-box) is important nonlinear component used in block ciphers to achieve confusion property. S-box have some number of bits as an input and transform these bits to some number of output bits. Although number of input and output bits is not necessarily the same, recent block ciphers mostly use such S-boxes. From mathematics perspective, an $m \times m$ S-box is a nonlinear mapping $S : \{0, 1\}^m \rightarrow \{0, 1\}^m$, where $\{0, 1\}^m$ is the vector space of $m$ elements from GF(2).
Besides confusion, secure block cipher should possess diffusion characteristics in order to resist linear and differential cryptanalysis. These basic characteristics of cryptography overlaps with the properties of chaos such as mixing, random-like behaviour, ergodic behaviour and sensitivity to initial conditions. In recent years, chaotic maps such as logistic map, exponential map, 2D Baker map, Chebyshev map, Tent map, Lorenz system, 3D four-wing autonomous chaotic system, chaotic scaled Zhongtang system, logistic-sine map, fractional-order chaotic Chen system etc. are widely used for random S-box design (Belazi, Khan, Abd El-Latif, & Belghith, 2016; Cavusoglu, Zengin, Pehlivan, & Kacar, 2016; Chen, 2008; Jakimoski & Kocarev, 2001; Lambić, 2014; Liu, Yang, Liu, & Dai, 2015; Ozkaynak, Celik, & Ozer, 2016; Ozkaynak & Ozer, 2010; Wang, Wong, Liao, & Xiang, 2009). Besides these, there are many other methods for the generation of random S-boxes based on various chaotic maps, which to our knowledge all have continuous space domain, except for the method presented in Lambić (2017).

However, implementation of continuous space domain chaotic systems on computers and other digital devices causes dynamical degradation (Wang et al., 2016). Taking into account the high sensitivity to initial conditions of the chaotic maps, small differences caused by the use of approximations has a great influence on the obtained S-boxes. Method presented in Lambić (2017) uses discrete chaotic map based on the composition of permutations which represents fully digital approach, so there is no need for discretization of continuous values (Lambić, 2015). Therefore, the process of generation of S-boxes is not affected by approximations of any kind. However, special case of chaotic map presented in paper Lambić (2015) has a drawback of relatively short orbit lengths. For that reason it must be used with caution, using greater number of elements of the permutation, which decreases speed and increases memory requirements.

Previously mentioned drawbacks significantly affect the usability of this chaotic map (Lambić, 2015) in lightweight devices such as wireless sensor networks which have limited memory and computational resources (Tong, Wang, & Zuo, 2012; Zaibi, Peyrard, Kachouri, Fournier-Prunaret & Samet, 2014). In order to overcome this problem, a new special case of one-dimensional discrete chaotic map (Lambić, 2015), which is based on the composition of permutations and sine function is presented. This special case also represents fully digital approach. Proposed map has a longer minimal length of the orbits compared to special case of chaotic map presented in paper Lambić (2015) and therefore mitigates possible negative effects of shorter orbits.

In this paper, a new method to obtain random chaotic S-boxes based on proposed special case of discrete chaotic map is presented. Because proposed method uses chaotic map with significantly greater length of periodic orbits than method presented in paper Lambić (2017), it has potential to function properly with a smaller number of elements of the permutation, which could result in greater speed and smaller memory requirements.

The rest of this paper is organized as follows. In Section 2, a proposed special case of discrete chaotic map based on the composition of permutations is presented. In Section 3, the method of S-box design based on proposed chaotic map and an example of the S-box generated by this method are presented. Criteria used to measure quality of S-boxes are introduced in Section 4, and the performance of the example S-box is evaluated and compared with other random bijective chaos-based S-boxes. In Section 5, performance analysis of the proposed method is presented. Conclusions are drawn in Section 6.
2. New discrete chaotic map

In this section special case of discrete chaotic map based on the composition of permutations is proposed. This special case can be considered as improvement of chaotic map presented in paper Lambić (2015), because it was developed with the aim of extending minimum length of the orbits.

2.1. Notation

Let $P = p_0p_1 \cdots p_{n-2}p_{n-1}$ denote a permutation of the set $\{0, 1, \ldots, n-1\}$ and $P' = p_{n-1}p_{n-2} \cdots p_0$ denote the reverse permutation of the permutation $P$.

The composition $h = f \circ g$ of two permutations $f$ and $g$ of the same set $A$, is the permutation mapping each $x \in A$ into $h(x) = f (g(x))$.

Let $S_n$ denote the set of all permutations of the set $\{0, 1, \ldots, n-1\}$. Lehmer code (1960) is a bijective function $l : S_n \rightarrow \{0, 1, 2, \ldots, n! - 1\}$. Define function $l(P) = \sum_{0 \leq i < n} c_i \cdot (n-1-i)!$ where $P \in S_n$ and $c_i$ is the number of elements of the set $\{j > i \mid p_j < p_i\}$. Inverse Lehmer code is a bijective function $l^{-1} : \{0, 1, 2, \ldots, n! - 1\} \rightarrow S_n$.

Let $\text{floor}(y)$ denote a function which map a real number $y$ to the largest integer less than or equal to $y$. Let $\sin(y)$ denote implementation of trigonometric sine function in C++ programming language. Let $\pi \approx 3.1415926535897932$ denote the constant which represents the value of $\pi$ rounded to 16 decimal places.

2.2. Proposed map

In paper Lambić (2015) a one-dimensional discrete chaotic map is proposed by

$$X_{i+1} = X_i \circ f (X_i, C), \tag{1}$$

where $X_i, C \in S_n$ and $f : S_n \rightarrow S_n$. If $x_i = l(X_i)$ and $c = l(C)$, this map can also be represented as

$$X_{i+1} = l[l^{-1}(x_i) \circ f (l^{-1}(x_i), l^{-1}(c))], \tag{2}$$

where $x_i, c \in \{0, 1, 2, \ldots, n! - 1\}$ and $f : S_n \rightarrow S_n$. In this paper, we consider the special case when

$$f (x_i, c) = l^{-1} \left( \text{floor} \left( \sin \left( \frac{\pi}{2} \left( \frac{x_i}{n! - 1} + \frac{c + 1}{n! + 1} \right) \right) \right) \right). \tag{3}$$

On the basis of Equations (1) and (3) we obtain map $F_n : \{0, 1, 2, \ldots, n! - 1\} \rightarrow \{0, 1, 2, \ldots, n! - 1\}$ by:

$$F_n(x) = l \left[ l^{-1}(x) \circ l^{-1} \left( \text{floor} \left( \sin \left( \frac{\pi}{2} \left( \frac{x}{n! - 1} + \frac{c + 1}{n! + 1} \right) \right) \right) \right) \right]. \tag{4}$$

In the following text, we will deal with the dynamical properties of the proposed map. Bearing in mind that the proposed map is a special case of map presented in paper Lambić (2015), proof that this map is discrete chaotic will be omitted, because it is exactly the same as in paper Lambić (2015). Denote by $Id = l^{-1}(0)$ identical
permutation. The proposed map (Equation (4)) does not have fixed points because 

$$-\sin\left(\frac{\pi}{2}\left(x_i/(n! - 1) + (c + 1)/(n! + 1)\right)\right) * (n! - 1) > 1 \text{ for all } x_i, c \in \{0, 1, 2, \ldots, n! - 1\}, n>1 \text{ and therefore } f(X_i, C) \neq Id.$$ 

Figure 1 shows the frequency of appearance of each output value $x$ of the proposed map for different values of the parameter $c$, when $n=6$. Darker shade indicates increased probability of the output $x$ acquiring corresponding value on the vertical axis for the given value of the parameter $c$.

In order to demonstrate qualitative behaviour of proposed map, cobweb plot diagrams for $n = 6$, $c = 3$, $x_0 = 9$ and $n = 8$, $c = 1$, $x_0 = 8307$ are shown (Figures 2 and 3).

If we consider the proposed map when $c=1$, for $n=6$ map has periodic orbit of minimal length 5. When $c=3$, for $n=6$ the minimum length of the orbit is 29, which is much greater than 2, which is the maximum length of the orbits of examples for $n=6$ presented in the paper Lambič (2015). For that reason, it is recommended that the map proposed in Lambič (2015) is used for $n \geq 8$. On the other hand, special case proposed in this paper can be used for $n=6$ when great cycle lengths are not required. Proposed special case can

---

**Figure 1.** The frequency of appearance of output values of the proposed map for $n=6$. 
be very useful in situations when speed and memory are a priority, because when \( n \) (number of elements of the permutation) increases, periodic orbits of the discrete chaotic map have a greater length, but the process of converting the permutations to the Lehmer code becomes more demanding.

3. Proposed S-box generation method

In this section, the proposed simple algorithm for generation of \( m \times m \) S-boxes which uses discrete chaotic map based on the composition of permutations and sine function (Equation (4)) is described. Set the initial state of S-box \( S_b \) to identical permutation, \( S_b[j] = j \) for all \( 0 \leq j < 2^m \), and chose the initial value \( x_0 \) of chaotic map from the set \( \{0, 1, 2, \ldots, n! - 1\} \). For each \( 0 \leq i < 2^m \) calculate index \( j = \lfloor x_i / n! \cdot 2^m \rfloor \), swap values of \( S_b[2^m - 1 - i] \) and \( S_b[j] \), and iterate chaotic map (Equation (4)) one time in order to obtain value \( x_{i+1} = F_n(x_i) \). One S-box can be generated by the following pseudocode:

```plaintext
for 0 \leq i < 2^m
    swap values of Sb[2^m - 1 - i] and Sb[floor(x_i/n! \cdot 2^m)]
    x_{i+1} = F_n(x_i)
end for
```

Proposed S-box generation method returns the \( m \times m \) S-box \( S_b \). For example, if \( n = 8 \), \( c=17 \) and \( x_0 = 12, 294 \) then the \( 8 \times 8 \) S-box from Table 1 is obtained.

4. Performance analysis of the generated S-box

A block cipher is generally considered secure if the S-boxes satisfy a number of criteria, such as bijection, nonlinearity, strict avalanche criterion, output bits independence criterion, equiprobable input/output XOR distribution and maximum expected linear probability.

Example of S-box generated by proposed approach was compared with some representative random bijective chaos-based S-boxes presented in papers (Cavusoglu et al., 2016; Chen, 2008; Lambić, 2014, 2017; Liu et al., 2015; Ozkaynak & Ozer, 2010). In Lambić & Živković (2013) several random S-box generation methods based on chaotic

| 208 | 165 | 65 | 228 | 68 | 44 | 150 | 170 | 87 | 172 | 74 | 157 | 133 | 22 | 255 |
| 105 | 53 | 75 | 225 | 156 | 173 | 58 | 131 | 216 | 117 | 158 | 27 | 152 | 235 | 61 | 250 |
| 51 | 36 | 37 | 177 | 176 | 238 | 88 | 223 | 77 | 20 | 98 | 236 | 135 | 66 | 3 | 45 |
| 39 | 231 | 179 | 229 | 163 | 34 | 80 | 28 | 185 | 41 | 48 | 128 | 112 | 237 | 7 | 52 |
| 100 | 224 | 193 | 31 | 96 | 169 | 190 | 219 | 251 | 144 | 120 | 81 | 14 | 76 | 64 | 201 |
| 181 | 142 | 171 | 16 | 6 | 57 | 29 | 202 | 115 | 32 | 102 | 130 | 24 | 217 | 189 | 113 |
| 182 | 191 | 203 | 227 | 132 | 252 | 106 | 108 | 30 | 79 | 239 | 35 | 0 | 199 | 154 | 40 |
| 73 | 247 | 200 | 213 | 214 | 93 | 222 | 11 | 84 | 166 | 134 | 54 | 209 | 25 | 101 | 137 |
| 33 | 242 | 63 | 141 | 9 | 123 | 248 | 183 | 104 | 62 | 233 | 245 | 143 | 19 | 148 | 243 |
| 103 | 119 | 55 | 221 | 125 | 59 | 70 | 50 | 94 | 124 | 186 | 12 | 5 | 118 | 232 | 178 |
| 90 | 194 | 138 | 109 | 153 | 151 | 13 | 92 | 121 | 212 | 204 | 127 | 136 | 164 | 220 | 188 |
| 149 | 175 | 71 | 234 | 167 | 43 | 116 | 47 | 139 | 160 | 21 | 114 | 23 | 72 | 42 | 95 |
| 241 | 69 | 67 | 78 | 97 | 174 | 83 | 184 | 56 | 155 | 146 | 187 | 159 | 180 | 107 | 196 |
| 91 | 206 | 210 | 246 | 207 | 82 | 215 | 162 | 226 | 99 | 254 | 18 | 10 | 15 | 8 | 218 |
| 49 | 192 | 253 | 1 | 85 | 111 | 205 | 240 | 89 | 230 | 147 | 197 | 86 | 60 | 38 | 211 |
| 26 | 46 | 249 | 145 | 161 | 244 | 110 | 198 | 129 | 126 | 4 | 2 | 17 | 122 | 168 | 195 |
maps were compared. Bounds for criteria used to measure quality of S-boxes presented in that paper will also be used for comparison.

S-box generated by the proposed method have all different output values from interval $[0, 255]$ so it satisfies the requirement of bijectivity (Lambić, 2017).

The nonlinearity of generated S-box is calculated according to formula presented in paper Cusick & Stanica (2009). The nonlinearities of eight output bits are 106, 108, 108, 106, 106, 106, 106, 106. Minimum nonlinearity is used as an indicator of the quality of S-box, because the chain is only as strong as its weakest link. Minimum nonlinearity of generated S-box is better than most of random chaotic S-box examples from Table 2.

Strict avalanche criterion is described in paper Webster & Tavares (1986). The dependence matrix of the generated S-box is presented in Table 3. The average offset of the dependence matrix elements of generated S-box is 0.02954 and the mean value is 0.4978, which is very close to the ideal value of 0.5. Some S-boxes have a mean value close to 0.5, although elements of the dependence matrix significantly deviate from this ideal value. For this reason, the offset is a better indicator of the SAC characteristics of the S-box. S-box generated by proposed method satisfies bound for SAC criteria set in Lambić & Živković (2013).
BIC criteria is presented in paper Webster & Tavares (1986). If S-box satisfies BIC, all pairs of output bits should be highly nonlinear and satisfy the avalanche criterion. Fulfillment of the SAC criterion of pairs of output bits can be tested with a dynamic distance (Chen, 2008). If the value of dynamic distance (DD) is a small integer close to zero, S-box satisfies the SAC. The data regarding output bits independence criterion of the generated S-box are shown in Tables 4 and 5. The minimum value of BIC nonlinearity is 100 and maximum value of DD is 10.

**Figure 3.** Cobweb plot diagram for \( n = 8, c = 1, x_0 = 8307. \)

**Table 2.** Comparison of the random bijective chaotic S-boxes.

| Scheme                          | Min. nonlinearity | SAC offset | Min. BIC-nonlinearity | Max. XOR | MELP     |
|---------------------------------|-------------------|------------|-----------------------|----------|----------|
| Scheme in ref. Lambić (2014)    | 108               | 0.02954    | 104                   | 8        | 0.035156 |
| Scheme in ref. Cavusoglu et al. (2016) | 104               | 0.03809    | 98                    | 10       | 0.0791   |
| Scheme in ref. Liu et al. (2015) | 104               | 0.03027    | 98                    | 10       | 0.0625   |
| Scheme in ref. Lambić (2017)    | 106               | 0.02441    | 100                   | 10       | 0.070557 |
| Scheme in ref. Ozkaynak & Ozer (2010) | 100               | 0.03125    | 100                   | 10       | 0.070557 |
| Scheme in ref. Chen (2008)      | 102               | 0.03174    | 100                   | 10       | 0.088135 |
| Bounds in ref. Lambić & Živković (2013) | 106               | 0.03      | 100                   | 10       | 0.079    |
| The proposed scheme             | 106               | 0.02954    | 100                   | 10       | 0.070557 |
The equiprobable input/output XOR distribution criterion is also known as maximum expected differential probability (MEDP) and is calculated according to a formula presented in paper Biham & Shamir (1991). The equiprobable input/output XOR distribution of generated S-box is presented in Table 6. Maximal value in Table 6 is 10.

Definition of the maximum expected linear probability can be found in papers Keliher, Meijer, & Tavares (1997) and Keliher (2005). The maximal expected linear probability of the S-box presented in this paper is 0.070557, which satisfies bound set in Lambić & Živković (2013). The S-box generated in this paper satisfies all bounds set in Lambić & Živković (2013). For that reason, we can claim that S-box generation method presented in this paper can generate S-boxes with high performance.

5. Performance analysis of the proposed method

In this section, proposed method will be compared to previous fully digital S-box design method (Lambić, 2017). Speed and required memory are of critical importance when some cryptographic system with dynamic S-boxes is used in devices with very limited resources such as wireless sensor networks (Tong et al., 2012). Both of the aforementioned methods can be used for generation of dynamic S-boxes, so it is very important to establish minimum requirements for their normal functioning.

Previous fully discrete S-box generation method proposed in Lambić (2017) should be used for \( n \geq 8 \). For example, if \( n=6 \), that method is completely unusable, because the maximum length of the cycle of the chaotic map proposed in the paper Lambić (2015)
is only 2, and therefore all obtained S-boxes are almost completely linear. The minimum value of the parameter $n$ for which this discrete chaotic map has acceptable cycle length is 8, so we will consider S-box generation method proposed in Lambić (2017) for $n=8$. On the other hand chaotic map proposed in this paper has up to 15 times longer cycle for $n=6$ (for $c=3$ the minimum length of the orbit is 29) than chaotic map used in previous method (Lambić, 2015) for same value of $n$, which means that it can be used for $n=6$. Therefore, we will consider the proposed S-box generation method for $n=6$.

Since both methods are based on the Lehmer code which was implemented relying on the algorithm with time complexity $O(n^2)$, the ratio of the speed of these two methods is about $\frac{6^2}{8^2} = \frac{36}{64}$ which means that the proposed method is approximately 43\% faster.

S-box generation method proposed in Lambić (2017) requires $8 \cdot \log_2(8) = 24$ bits of memory for one permutation from the set $S_8$, and 16 bits for each of the parameters $x_i$, $c \in [0, 40319]$ because $\log_2(8! − 1) \approx 15.3$. Proposed method requires $6 \cdot \log_2(8) = 18$ bits of memory for one permutation from the set $S_6$, and 10 bits for each of the parameters $x_i$, $c \in [0, 719]$ because $\log_2(6! − 1) \approx 9.49$. In sum, proposed method requires only $18 + 2 \cdot 10 = 38$ bits of memory compared to $24 + 2 \cdot 16 = 56$ bits required by the previous approach, which is approximately 32\% less required memory space. This difference may be of crucial importance in lightweight devices such as wireless sensor networks.

### 6. Conclusion

In this paper a new method for obtaining random bijective S-boxes based on improved one-dimensional discrete chaotic map is presented. In order to overcome the problem with potentially short length of the orbits of the previous discrete-space chaotic map, a new special case based on the composition of permutations and sine function is proposed. Proposed map is defined over finite set which makes it suitable for use on digital computers. Although the trigonometric sine function has a real domain and the number $\pi$ is an irrational number, in the proposed map the implementation of sine function in C++ programming language and constant which represents the value of $\pi$ rounded to 16 decimal places are used. Therefore there is no need for approximations of any kind and this map is

| 6 | 6 | 10 | 6 | 8 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 |
|---|---|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 6 | 5 | 6 | 8 | 10 | 8 | 6 | 6 | 6 | 4 | 8 | 6 | 10 | 6 | 6 | 6 | 6 | 8 | 6 |
| 8 | 6 | 6 | 6 | 8 | 8 | 6 | 6 | 4 | 8 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 8 | 4 | 10 | 8 | 6 | 8 | 8 | 8 | 6 | 6 | 6 | 6 | 8 | 6 | 8 | 6 |
| 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 8 | 6 | 6 | 6 | 8 | 6 | 8 | 6 |
| 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 10 | 8 | 10 | 6 | 4 | 8 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 8 | 6 | 8 | 6 | 8 | 8 | 8 |
| 6 | 10 | 6 | 6 | 8 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 4 | 8 | 8 |
| 6 | 6 | 6 | 8 | 8 | 8 | 6 | 6 | 6 | 6 | 6 | 8 | 8 | 8 | 8 | 8 | 6 |
| 8 | 8 | 8 | 8 | 6 | 8 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 8 | 8 | 8 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 8 | 8 | 6 | 8 | 10 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 8 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 8 | 8 | 8 | 6 | 8 | 6 | 8 |
| 6 | 8 | 6 | 6 | 8 | 6 | 8 | 6 | 8 | 8 | 6 | 8 | 8 | 8 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 8 | 6 | 6 | 6 | 4 | 8 | 6 | 8 | 8 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 8 | 8 | 8 | 8 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |

| Table 6. Input/output XOR distribution table of S-box generated by the proposed method. | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 8 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
| 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |

| – | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| JOURNAL OF INFORMATION AND TELECOMMUNICATION | 189 |
particularly applicable in fields where fully digital approach is necessary. The proposed special case has a significantly greater length of periodic orbits which makes it more useful than the map presented in paper Lambić (2015), because it can achieve a decent length of orbits for small $n$.

The proposed special case of discrete chaotic map is used as the basis of the new method for generation of random chaotic S-boxes. The results of performance test show that the example of S-box generated by the proposed method has good cryptographic properties. The proposed method can achieve large key space, which makes it suitable for generation of larger S-boxes, and the process of generation of S-boxes is not affected by approximations of any kind. Also, because proposed method use chaotic map with significantly greater length of periodic orbits than method presented in paper Lambić (2017), it has potential to operate at greater speed and with smaller memory requirements than previous S-box generation method based on discrete space chaotic map, which can be particularly useful for lightweight devices such as wireless sensor networks.

**Disclosure statement**

No potential conflict of interest was reported by the author.

**Notes on contributor**

**Dragan Lambić** received the Ph.D. degree from the Faculty of Mathematics in Belgrade. His primary research areas are mathematics, computer science, cryptography, chaos, computer science education and mathematics education.

**ORCID**

Dragan Lambić [http://orcid.org/0000-0001-8611-353X](http://orcid.org/0000-0001-8611-353X)

**References**

Belazi, A., Khan, M., Abd El-Latif, A. A., & Belghith, S. (2016). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dynamics, 87*, 337–361.

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology, 4*, 3–72.

Cavusoglu, U., Zengin, A., Pehlivan, I., & Kacar, S. (2016). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dynamics, 87*, 1081–1094.

Chen, G. (2008). A novel heuristic method for obtaining S-boxes. *Chaos, Solitons and Fractals, 36*, 1028–1036.

Cusick, T., & Stanica, P. (2009). *Cryptographic Boolean functions and applications*. Amsterdam: Elsevier.

Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: Block encryption ciphers based on chaotic maps. *IEEE Transactions on Circuits and Systems I, 48*, 163–169.

Keliher, L. (2005). Refined analysis of bounds related to linear and differential and linear cryptanalysis for the AES. In H. Dobbertin et al. (Eds.), *Advanced encryption standard-AES ’04, Bonn, 2004, Lecture notes in computer science, 2005* (pp. 42–57).

Keliher, L., Meijer, H., & Tavares, S. (1997). A new substitution-permutation network cryptosystem using key-dependent s-boxes. In *Proceedings of SAC97*, Ottawa, Canada, 13–26.

Lambić, D. (2014). A novel method of S-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals, 58*, 16–21.
Lambić, D. (2015). A new discrete chaotic map based on the composition of permutations. *Chaos, Solitons & Fractals, 78*, 245–248.

Lambić, D. (2017). A novel method of S-box design based on discrete chaotic map. *Nonlinear Dynamics, 87*, 2407–2413.

Lambić, D., & Živković, M. (2013). Comparison of random S-box generation methods. *Publications de l’institut mathematique, 93*(107), 109–115.

Lehmer, D. H. (1960). Teaching combinatorial tricks to a computer. In *Proceedings of symposia in applied mathematics combinatorial analysis* (Vol. 10, pp. 179–193). American Mathematical Society, Providence, Rhode Island.

Liu, G., Yang, W., Liu, W., & Dai, Y. (2015). Designing S-boxes based on 3-D four-wing autonomous chaotic system. *Nonlinear Dynamics, 82*, 1867–1877.

Ozkaynak, F., Celik, V., & Ozer, A. B. (2016). A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image and Video Processing, 1–6*. DOI:10.1007/s11760-016-1007-1

Ozkaynak, F., & Ozer, A. B. (2010). A method for designing strong S-Boxes based on chaotic Lorenz system. *Physics Letters A, 374*, 3733–3738.

Tong, X. J., Wang, Z., & Zuo, K. (2012). A novel block encryption scheme based on chaos and an S-box for wireless sensor networks. *Chinese Physics B, 21*(2), 020506.

Wang, Y., Wong, K. W., Liao, X., & Xiang, T. (2009). A block cipher with dynamic S-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation, 14*, 3089–3099.

Wang, Q., Yu, S., Li, C., Lu, J., Fang, X., Guyeux, C., & Bahi, J. M. (2016). Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. *IEEE Transactions on Circuits and Systems I: Regular Papers, 63*(3), 401–412.

Webster, A., & Tavares, S. (1986). On the design of S-boxes. In *Advances in cryptology: Proceedings of CRYPTO’85, Lecture notes in computer science*, Berlin, 1986 (pp. 523–534).

Zaibi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., & Samet, M. (2014). Efficient and secure chaotic S-box for wireless sensor network. *Security and Communication Networks, 7*(2), 279–292.