Chaos-based S-box for lightweight block cipher

Conference Paper · October 2014

DOI: 10.1109/CCE.2014.6916765

CITATIONS
3

READS
226

3 authors, including:

Thang Manh Hoang
Hanoi University of Science and Technology, Hanoi, Vietnam
89 PUBLICATIONS **469** CITATIONS
SEE PROFILE

Dat Tran
University of Canberra
87 PUBLICATIONS **711** CITATIONS
SEE PROFILE

Chaos-based S-box for Lightweight Block Cipher

Ta Thi Kim Hue[1], Thang Manh Hoang[1,2], Dat Tran[2]
[1]School of Electronics and Telecommunications
Hanoi University of Science and Technology
No. 1 Dai Co Viet, Hai Ba Trung, Ha Noi, Vietnam
Email: kimhueta@ieee.org

[2] Faculty of Education, Science, Technology & Mathematics (ESTEM)
University of Canberra
University Drive, Bruce, ACT 2601 AUSTRALIA
Email: dat.tran@canberra.edu.au

***Abstract*—In this paper, design of chaos-based 4×4-bit substitution box (S-box) is presented. The chaotic 4×4-bit S-box provides good cryptographic properties and has hardware efficiency. The proposed chaotic 4×4-bit S-box is used for design of chaotic S-boxes chaining layer, which offers a highly secure level. The result of implementation shows that the proposed chaotic 4×4-bit S-box is suitable for the lightweight block cipher due to low resource utilization.**

I. Introduction

Nowadays, a new computing environment called Internet of Things (IoT) or Smart Object networks is pervasive, where a lot of constrained devices are connected to the internet. Many cheap devices interact with one another through the network and provide new experience to human. When enjoying this new environment, security of constrained end nodes is important. However, it is not easy to implement full cryptographic standards such as DES, AES, etc, on constrained devices due to the resource limit.

Lightweight cryptography is a relatively new field aimed to develop more efficient cryptographic implementations in response to typical constraints in the hardware used in IoT, i.e. computational power, battery, and memory. Lightweight cryptography is tailored for such constrained devices, with the goal of balancing the tradeoffs among low resource requirements, performance, and acceptable cryptographic strength.

Lightweight cryptographic algorithms are used in commercial products today, including SEA [1], DESL, PRESENT [2], KATAN/KTANTAN [3], HIGHT [4], PRINTcipher [5], LED [6], etc. For example, Keeloq is a 32-bit block-cipher developed in 1980s and used frequently in the auto industry. DST is a 40-bit block cipher using a 40-bit key, developed by Texas Instruments for RFID. Both of these algorithms have relatively small block, small key sizes and a large number of encryption rounds.

One of main properties of S-boxes in a common lightweight block cipher is small size (e.g. 4×4-bit S-box) and the form of look-up tables (LUT) are usually used. Those S-boxes are static [2], and substitution tables are fully defined. In addition, there is no strict criteria and no standard design for S-boxes. An S-box provides the confusion property, the core of cryptosystems as described by Shannon [7]. It is the only nonlinear component contributes the strength of cryptosystems. Therefore, a good S-box provides a significant concern of cryptosystems in terms of speed, performance and security by some a great extent.

Design of S-boxes in [1-7] is a direct consequence of their pursuit of hardware efficiency, however, its inverse S-box is almost linear and apparently, its confusion property cannot be ensured, e.g. [8]. In [9], Adam and Tavares described the criteria for a good $n \times n$-bit S-box which is widely accepted as the essential properties of S-boxes. So far, few design of S-boxes for the lightweight block cipher consider criteria to become the "good" S-box as proposed by Adam and Tavares. By using chaotic maps, Jakimoski and Kocarev proposed a four-step method to create a S-box [10]. Along with that, a presented in [11]–[14], the methods for designing 8×8 S-boxes based on the different chaotic maps, such as Skew tent map, Tent map, Baker map, and Logistic map.

The design of "good" 4×4-bit S-box for the lightweight block cipher is proposed, which is trade-off between the performance criteria and the hardware efficiency. This is a dynamic S-box which is bijective, highly nonlinear, possession of the strict avalanche criterion, and equiprobable input/output XOR distribution. The chaotic 4×4-bit S-box is fulfilling the conditions to against differential and linear attacks. The result of hardware implementation shows that the proposed S-box is very suitable for the lightweight block cryptography.

II. Proposed chaotic 4×4-bit S-box

In this section, a new method to obtain a good chaotic 4×4-bit S-box is generated, which is suited for hardware implementation on 8-bit processors.

A. Chosen chaotic map

In [11], [13], some important properties of skew tent map was demonstrated, which are essential for "good" cryptographic S-boxes. Therefore, the discretized skew tent map is employed for obtaining the 4×4-bit S-box. It is defined in

978-1-4799-5051-5/14/$31.00 ©2014 IEEE

Eq. (1) as below

$$F_K^1(X) = \begin{cases} ceil\left(M \times \frac{X}{K}\right) \ if \ 1 \le X \le K \\ floor\left(M \times \frac{M-X}{M-K}\right) + 1 \ if \ K < X \le M \end{cases} \tag{1}$$

The inverse function of the discretized skew - tent map is used to create the inverse S-box in the decryption. The inverse of F_K is given as

$$F_K^{-1}(Y) = \begin{cases} X_1, & if \ m(Y) = Y \ and \ \frac{X_1}{K} > \frac{M-X_2}{M-K} \\ X_2, & if \ m(Y) = Y \ and \ \frac{X_1}{K} \le \frac{M-X_2}{M-K} \\ X_1, & if \ m(Y) = Y + 1 \end{cases} \tag{2}$$

where

$$X_1 = \left\lfloor M^{-1}KY \right\rfloor; X_2 = \left\lceil (M^{-1}K - 1)Y + M \right\rceil \tag{3}$$

$$m(Y) = Y + \left\lfloor M^{-1}KY \right\rfloor - \left\lceil M^{-1}KY \right\rceil + 1 \tag{4}$$

It is clear that $F_K^1(X)$ is an one-to-one map as M is a positive integer $M \ge 2$. In general, this kind of S-box takes n input bits and produces n output bits, the input value can be any possible value in a closed interval $X = (0, 1, 2, ..., 2^n - 1)$ with $M = 2^n$. X is represented in bits as $X = (x_1, x_2, x_3, x_4)$, where $x_i \in \{0, 1\}$. For given $n = 4$, it is obvious that $M = 16$ is obtained. The S-box with k iterations is described by

$$S_K(X) = F_K^k(X + 1) - 1, \tag{5}$$

and the inverse S-box is in the following form

$$S_K^{-1}(X) = F_K^{-k}(X + 1) - 1. \tag{6}$$

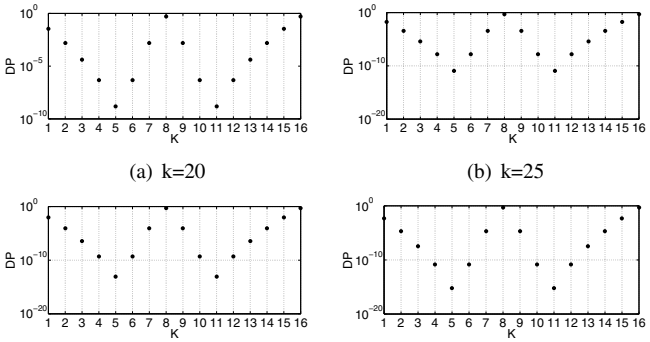
where $S_K : G_2^4 \to G_2^4, G_2^4 = GF\left(2^4\right)$ is the Galois field.

B. Chosen value of parameters

The value of parameters is chosen, and the value set is seen as part of the secret key $K \in \{1, 2, 3, ..., M\}$. In [15], a necessary number of iterating skew tent map is $k \ge 2.39 log_2(M) + 15$. Table I shows the sixteen dynamic S-boxes constructed using different secret keys K with the number of iterations $k = 25$ and M =16.

The differential cryptanalysis in [16] and the linear cryptanalysis in [17] are two typically basic attacks, denoted by the differential probability (DP) and the linear probability (LP), respectively. LP and DP measure the immunity of the S-box S_K against attacks on the cryptosystems. The authors of [18] computed lower bounds for differential and linear probabilities, then LP and DP get asymptotically close to their greatest lower bounds $\frac{1}{2^n}$ and $\frac{1}{2^{n-1}}$, respectively. Calculating LP and DP of these S-boxes and comparing with above mentioned lower bounds will tell us what suitable value of K and k are chosen. Specifically, DP is defined as

$$DP = max_{\Delta X \ne 0, \Delta Y} DP_S, \tag{7}$$



(a) k=20 (b) k=25

(c) k=30 (d) k=35

Fig. 1. The different probability for $S_K(X)$ with respect to the number of iterations.

where ΔX is the input difference, ΔY is the output difference, and DP_S is

$$DP_S = \frac{\#\left|\left\{X \in G_2^4 | S_K(X) \oplus S_K(X \oplus \Delta X) = \Delta Y\right\}\right|}{16}. \tag{8}$$

For a S-box, the output changes can be gained from the knowledge of the input changes. Actually DP is the maximum probability of output difference ΔY. By employing Eq. (7), values of DP with respect to K and different number of iterations are given in Fig. 1. The linear approximation probability LP_S is defined as

$$LP = max_{\alpha \ne 0, \beta \ne 0} LP_S, \tag{9}$$

where

$$LP_S = 4 \times \left(\frac{\#\left|\left\{X \in G_2^4 | X \circ \alpha = S_K(X) \circ \beta\right\}\right|}{16} - 1/2\right)^2. \tag{10}$$

The operation $\oplus$ denotes XOR, and $X \circ \alpha = x_1\alpha_1 \oplus x_2\alpha_2 \oplus x_3\alpha_3 \oplus x_4\alpha_4$ is the parity of the bitwise product of α and X (and analogously for $S_K(X) \circ \beta$). The parity of input bits selected by the mask α is equal to that of the output bits selected by the mask β. It is clear that the smaller the values of LP are, the more secure the S-boxes are against linear cryptanalysis. LP is obtained by numerical simulation as shown in Fig. 2.

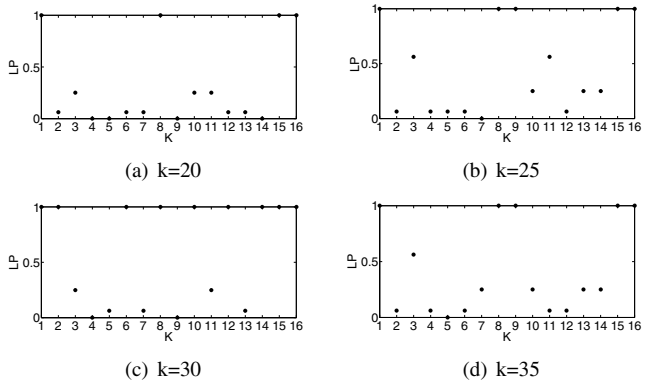
Figures 1 and 2 indicate that the $LP \le 2^{-3}$ and $DP \le 2^{-4}$ are achieved with the same values $k = 25$ and $K = \{2, 4, 5, 6, 7, 12\}$. With respect to any value of k, it should avoid $K = 1, 8, 16$ because F_K with $K = 1$ or 16 is nearly the identity map, whereas F_K with $K = 8$ is mostly equivalent to the orthodox tent map [13].

III. Cryptographic properties of proposed 4×4-bit S-box

According to the property of highly sensitive dependence on system parameters and initial condition of chaotic maps, it is easy and convenient to obtain a class of "good" S-box by choosing suitable value of K and k. To verify and demonstrate

TABLE I
AN EXAMPLE 4×4-BIT DYNAMIC S-BOX IS PRODUCED BY ITERATING THE CHAOTIC MAP 25 TIMES

X	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}
0	15	13	15	3	0	6	2	0	4	10	3	9	9	1	9	0
1	14	12	14	12	2	10	1	1	8	13	5	13	12	2	10	1
2	13	11	13	11	10	14	6	2	3	4	8	8	15	3	11	2
3	12	10	12	15	3	2	12	3	15	5	2	11	0	4	12	3
4	11	9	11	10	4	15	4	4	11	7	13	3	1	5	13	4
5	10	0	0	13	6	8	10	5	7	3	4	15	8	6	14	5
6	9	1	10	1	9	13	15	6	12	9	12	5	2	7	15	6
7	8	2	9	4	14	1	7	7	0	12	6	0	11	9	0	7
8	7	8	8	9	11	12	3	8	9	14	7	14	3	10	1	8
9	6	14	7	8	7	9	5	9	5	6	0	7	14	11	2	9
10	5	15	1	14	5	7	13	10	14	0	9	1	13	12	3	10
11	4	7	6	5	1	4	11	11	2	15	10	4	4	13	4	11
12	3	6	5	7	12	5	9	12	6	8	15	12	5	14	5	12
13	2	5	4	2	8	0	8	13	10	1	11	10	10	15	6	13
14	1	4	3	6	13	3	14	14	1	2	1	2	6	8	7	14
15	0	3	2	0	15	11	0	15	13	11	14	6	7	0	8	15



(a) k=20 (b) k=25

(c) k=30 (d) k=35

Fig. 2. The linear probability for $S_K(X)$ with respect to the number of iterations.

TABLE II
EXAMPLE FOR S-BOX S_4 WITH $K = 4$ AND $k = 25$

S_4	f_1	f_2	f_3	f_4
3	0	0	1	1
12	1	1	0	0
11	1	0	1	1
15	1	1	1	1
10	1	0	1	0
13	1	1	0	1
1	0	0	0	1
4	0	1	0	0
9	1	0	0	1
8	1	0	0	0
14	1	1	1	0
5	0	1	0	1
7	0	1	1	1
2	0	0	1	0
6	0	1	1	0
0	0	0	0	0

the properties of the proposed S-box, the bijection, nonlinearity property and strict avalanche, independence of output bits are calculated.

A. Bijective property

A 4×4-bit S-box $S : G_2^4 \to G_2^4$ can be decomposed into the sequence $S = [f_1, f_2, f_3, f_4]$ of Boolean functions such that

$$S(x_1, x_2, x_3, x_4) = [f_i(x_1, x_2, x_3, x_4)]; i = 1, 2, 3, 4 \quad (11)$$

The method was introduced to check the bijective property in [19]. If the Boolean function $f_i (1 \leq i \leq n)$ of a S-box is with the Hamming weight $wt(\sum_{i=1}^{n} a_i f_i) = 2^{n-1}$, where $a_i \in \{0, 1\}$ and a_i are non-zero simultaneously. An example with $K = 4$ and $k = 25$ generating the S-box S_4 is as in Tab. II.

Each 4-bit S-box contains four Boolean functions as in the columns of Tab. II. It is easy to observe that the Boolean function $f_i, i = \{1, 2, 3, 4\}$ has $0/1$ balanced. By computation, all the Hamming weight of these S-boxes are equal to 8, in other words, the corresponding S-boxes are bijective.

B. Nonlinearity property

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

$$N_f = 2^{n-1}\left(1 - 2^{-n} max_{\omega \in GF(2^n)} \left|S_{\langle f \rangle}(\omega)\right|\right). \quad (12)$$

The Walsh spectrum of $f(x)$ is defined as

$$S_{\langle f \rangle}(\omega) = \sum_{x \in GF(2^n)} (-1)^{f(x) \oplus x \bullet \omega}, \quad (13)$$

where $\omega \in GF(2^n)$. $x \bullet \omega$ denote the inner product of x and ω. Adams and Tavares give an equation in [9] to calculate the maximum achievable nonlinearity. If the Boolean functions of the 4×4-bit S-box are maximally nonlinear

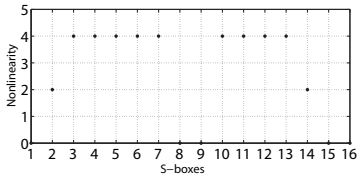


Fig. 3. The nonlinearities of the S-boxes

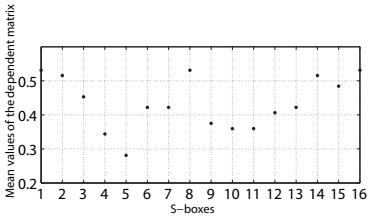


Fig. 4. The mean value of the dependence matrix

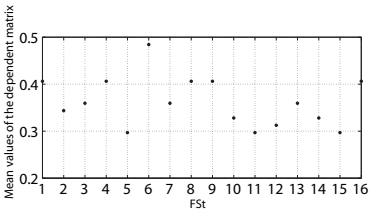


Fig. 5. The mean value of the dependence matrix of S_{FS}

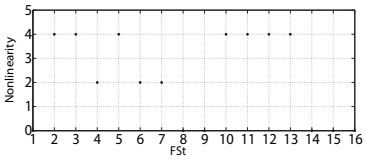


Fig. 6. The mean value of nonlinearity of S_{FS}

then $N_f = 4$. Figure 3 shows that these S-boxes have high nonlinear property. In [20], the linearity of f is in the following form of

$$Lin(f) = max_{\omega \in GF(2^n)} \left| S_{\langle f \rangle}(\omega) \right|. \quad (14)$$

By computation of the Walsh spectra for all of the 16 S-boxes, values of $Lin(f)$ is obtained as shown in Tab. III. It is easy to see that $Lin(f) \geq 8$. According to G. Leander [20], a 4×4-bit S-box is optimal if $Lin(f) = 8$, the S-box is against linear cryptanalysis. The value $Lin(f)$ is large if and only if f is close to a linear or affine function. Therefore, the smaller the value $Lin(f)$ means the more nonlinearity in the S-box. Clearly, as above mentioned, the proposed chaotic 4×4-bit S-boxes satisfy the conditions to become the optimal ones.

C. Strict avalanche criterion (SAC)

In order to determine whether a cryptographic transformation f fulfills the strict avalanche criterion (SAC), the efficient method in [21], [22] is used. By using this method, the dependence matrices of the proposed S-boxes are computed and shown in Fig. 4. If the mean value of the matrix is close to the ideal value 0.5, the S-box is considered as nearly fulfills the SAC. The result leads to the conclusion that S-boxes approximately satisfy the SAC.

D. The output bit independence criterion (BIC)

The independence of output bits ensures that any two output bits i and j act "independently" of each other. A S-box fulfills the requirement of BIC then the Boolean functions in the 4×4-bit S-boxes are $\{f_1, f_2, f_3, f_4\}$. If the (mod 2) sum of any two Boolean functions $FS_t = f_i \oplus f_j$, $(i \neq j, 1 \leq i, j, t \leq 4)$ then $S_{FS} = [FS_t], t = 1, 2, 3, 4$ should be highly nonlinear and satisfies SAC. Therefore, BIC can be verified by calculating SAC and the nonlinearity of S_{FS}. The mean values of dependence matrix and nonlinearites of S_{FS} are plotted in Figs. 5 and 6, respectively. It is easy to see from these results, the proposed S-boxes have a good property of BIC.

IV. Design of Chaotic S-boxes Chaining Layer

Chaining block mode is CPA (Chosen Plaintext Attack) secure. The proposed S-boxes are employed in the design of S-boxes chaining layer as shown in Fig. 7. The design of substitution boxes for lightweight block cipher is built in the form of chaining block network. In this scheme, one block is defined to be 64 bits $X = x_{63}x_{62}...x_b...x_1x_0$, where $x_b \in \{0, 1\}$, that is considered as 16 sub-blocks of 4 bits X_i, where $X_i = x_{4\times i+3}||x_{4\times i+2}||x_{4\times i+1}||x_{4\times i}$ for $i = \{0, 1, 2...15\}$. Sixteen dynamic 4×4-bit S-boxes are randomly generated as in Eq. (5) by choosing different values of parameters K and k. The input to S-box is XORed of the current input X_i and the preceding output Y_{i-1} to from a chain. There is a dummy initial input block C_0 known as the initialization vector (IV). The last output block of the S-boxes layer depends on all of input blocks. Thus, changes in the message will affect all ciphertext blocks. It can be seen in Eqs. (15)- (16).

$$Y_0 = S_K(K, [X_0 \oplus IV]). \quad (15)$$

$$Y_m = S_K(K, [X_m \oplus Y_{m-1}]); \qquad m = 1, 3...15. \quad (16)$$

Where S_K is the dynamic S-box as it was already mentioned in Subsection II-A. Output of any blocks is influenced by initialization vector (IV) and each of S-box has properties as explained as given in Subsection III. In order to consider the resistance of chaotic S-boxes layer to differential and linear

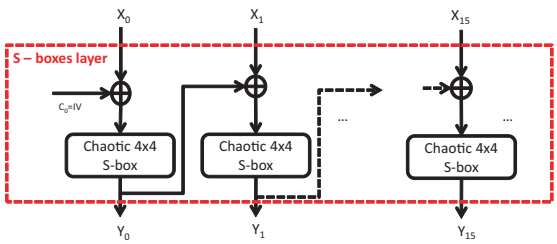


Fig. 7. The proposed scheme of S-boxes layer

TABLE III
WALSH SPECTRA FOR ALL OF THE 16 S-BOXES WHICH CITE IN TAB. I

S_K	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}	S_{16}
$Lin(f)$	16	12	8	8	8	8	8	16	16	8	8	8	8	12	16	16

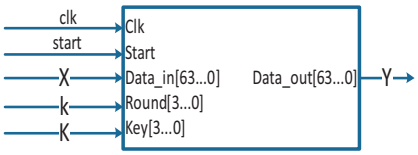


Fig. 9. I/O interfaces of the chaotic S-boxes layer

TABLE IV
PERFORMANCE AND DEVICE'S RESOURCE UTILIZATION

S-box	Device's resource utilization			
	CLKs	Total logic elements	Total registers	I/O pins
4×4	16	316(1%)	111(1%)	138

cryptanalysis, the number of active S-boxes involved in a differential (or linear) characteristic are computed.

Theorem.1 *Any one-layer differential (or linear) characteristic of chaotic S-boxes chaining scheme has sixteen active S-boxes.*

Proof. Let $S_j : G_2^4 \rightarrow G_2^4$ and $S_{j+1} : G_2^4 \rightarrow G_2^4$ be two active S-boxes, where j is j^th S-box of one-layer. Let $X_j, X_{j+1} \in G_2^4$ be the two input sub-blocks. Then $Y_j = S_j(X_j \oplus Y_{j-1})$ and $Y_{j+1} = S_{j+1}(X_{j+1} \oplus Y_j)$ can be rewritten as $Y_{j+1} = S_{j+1}(X_{j+1} \oplus S_j(X_j \oplus Y_{j-1}))$. It is easy to observed that there are two active S-boxes to obtaining a pair of output sub-blocks. This mean that 16 output sub-blocks in one-layer come from 16 different active S-boxes. The theorem follows.

There are $16! \approx 2^{44}$ permutations of the 4×4-bit S-boxes. We can restrict to good S-boxes fulfilling $S_K(X) = X$ or $S_K(X) = X'$ for $K = 1, 8, 16$. This observation reduced the space to only $13! \approx 2^{32}$. The set of active S-boxes in one-layer is a 16 combinations of the set $S = 13!$. The number of sets of active S-boxes are calculated by $(13!)^{16} \approx 2^{512}$. It is also strong enough to resist brute-force attack because the number alternative layers are $2^{512} \approx 1.34 \times 10^{54}$. Suppose that time required at decryption of one-chaotic S-boxes chaining layer is $1\mu s$ and $10^{-6}\mu s$, time for brute-force attack is also calculated as 2.58×10^{142} and 2.58×10^{136} years, respectively. Therefore, the chaotic S-boxes chaining layer is a robust encryption scheme.

V. EXPERIMENTAL RESULT

Hardware implementation is to create thousands of dynamic S-boxes which are more effective security than using look-up tables. The main design goals of the chaotic S-boxes layer described in Section IV are considered the following scenarios: Low cost smart devices with the limits of area, energy, and speed. For different application scenarios there exist different demands on the implementation and the optimization goals. The structure as illustrated in Fig. 7 is implemented on the low-cost FPGA. FPGA implementation provides more flexible solutions than ASICs while exploiting the hardware efficiency for the chaining chaotic S-box layer.

Implementation using VHDL on the FPGA core Cyclone II EP2C35F484C7 of Altera DE2 is displayed in Fig. 8, with S-boxes entities of 316 logic elements. Table IV lists the requirements of the chaotic S-box layer.

Chaotic 4×4-bit S-box shows significant decrease in critical path delay due to routing as compared to the S-box implementation with Look-Up Tables (LUTs). Two implementation options for the the chaotic S-boxes layer were taken in consideration in order to optimize the efficiency of the cipher. Using LUTs for substitution is the most obvious one and was implemented first but LUTs are used for the static (or fixed) substitution table. That is, each LUT is fully defined before starting encryption, the content of each LUT remains unchanged so that hardware implementation of dynamic LUTs is ineffective. Therefore, hardware implementation of the chaotic S-box function is the most feasible option. Tab.V summarizes the hardware implementations of chaotic S-boxes chaining layers.

VI. CONCLUSION

The S-box is one of the major components in block cipher. Many methods generating the 4×4-bit S-box for the lightweight block cipher have been suggested in recent years. A common feature of these methods is using the Boolean minimization tool or simple nonlinear functions to obtain Look-Up Tables of the static S-box. Unlike the existing algorithm, the structure of dynamic 4×4-bit S-box based on chaos has been proposed. The 4×4-bit S-boxes in this study have fulfill the cryptographic properties of the "good" ones. The chaotic S-box chaining layer has more effective security than sBoxLayer of the current lightweight block ciphers. The chaotic S-boxes layer using the proposed chaotic 4×4-bit S-boxes has been implemented on the Altera DE2 FPGA, in which a small resource is required.

ACKNOWLEDGMENT

This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.02-2012.27

REFERENCES

[1] F.-X. Standaert, G. Piret, N. Gershenfeld, and J.-J. Quisquater, "Sea: A scalable encryption algorithm for small embedded applications," in *Smart Card Research and Advanced Applications*, ser. Lecture Notes in Computer Science, J. Domingo-Ferrer, J. Posegga, and D. Schreckling, Eds. Springer Berlin Heidelberg, 2006, vol. 3928, pp. 222–236.

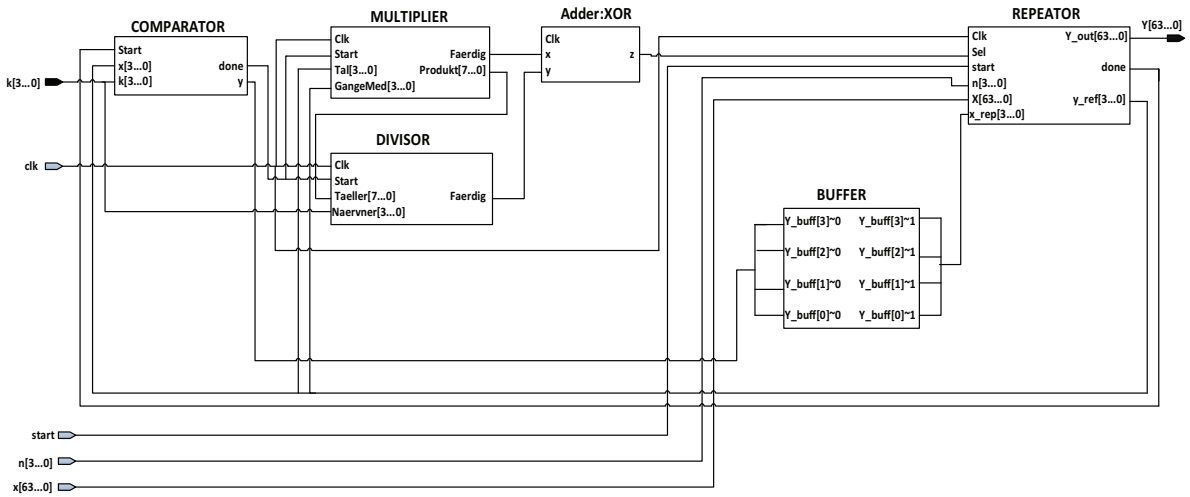


Fig. 8. Register Transfer Level (RTL) of the chaotic S-boxes layer

TABLE V
PERFORMANCE AND DEVICE'S RESOURCE UTILIZATION

One-Chaotic S-boxes chaining layer	Device's resource utilization		
	Total logic elements	Total registers	I/O pins
16 4×4-bit LUTs	$246(1\%)$	$64(1\%)$	135
16 Chaotic 4×4-bit S-boxes	$301(1\%)$	$92(1\%)$	135

[2] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New lightweight des variants," in *Fast Software Encryption*, ser. Lecture Notes in Computer Science, A. Biryukov, Ed. Springer Berlin Heidelberg, 2007, vol. 4593, pp. 196–210.

[3] C. Cannire, O. Dunkelman, and M. Kneevi, "Katan and ktantan a family of small and efficient hardware-oriented block ciphers," in *Cryptographic Hardware and Embedded Systems - CHES 2009*, ser. Lecture Notes in Computer Science, C. Clavier and K. Gaj, Eds. Springer Berlin Heidelberg, 2009, vol. 5747, pp. 272–288.

[4] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, "Hight: A new block cipher suitable for low-resource device," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, ser. Lecture Notes in Computer Science, L. Goubin and M. Matsui, Eds. Springer Berlin Heidelberg, 2006, vol. 4249, pp. 46–59.

[5] L. Knudsen, G. Leander, A. Poschmann, and M. Robshaw, "Printcipher: A block cipher for ic-printing," in *Cryptographic Hardware and Embedded Systems, CHES 2010*, ser. Lecture Notes in Computer Science, S. Mangard and F.-X. Standaert, Eds. Springer Berlin Heidelberg, 2010, vol. 6225, pp. 16–32.

[6] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The led block cipher," in *Cryptographic Hardware and Embedded Systems CHES 2011*, ser. Lecture Notes in Computer Science, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 326–341.

[7] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[8] M.-J. Saarinen, "Cryptographic analysis of all 4 4-bit s-boxes," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, A. Miri and S. Vaudenay, Eds. Springer Berlin Heidelberg, 2012, vol. 7118, pp. 118–133.

[9] C. Adams and S. Tavares, "The structured design of cryptographically good s-boxes," *Journal of Cryptology*, vol. 3, no. 1, pp. 27–41, 1990.

[10] G. Jakimoski and L. Kocarev, "Chaos and cryptography: block encryption ciphers based on chaotic maps," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 48, no. 2, pp. 163–169, Feb 2001.

[11] G. Tang and X. Liao, "A method for designing dynamical s-boxes based on discretized chaotic map," *Chaos, Solitons & Fractals*, vol. 23, no. 5, pp. 1901 – 1909, 2005.

[12] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining s-boxes based on three-dimensional chaotic baker maps," *Chaos, Solitons & Fractals*, vol. 31, no. 3, pp. 571 – 579, 2007.

[13] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: from theory to practical algorithms," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 53, no. 6, pp. 1341–1352, June 2006.

[14] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "A novel method to design s-box based on chaotic map and genetic algorithm," *Physics Letters A*, vol. 376, no. 67, pp. 827 – 833, 2012.

[15] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on*, vol. 49, no. 1, pp. 28–40, Jan 2002.

[16] E. Biham and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*. London, UK, UK: Springer-Verlag, 1993.

[17] M. Matsui, "Linear cryptanalysis method for des cipher," in *Advances in Cryptology EUROCRYPT 93*, ser. Lecture Notes in Computer Science, T. Helleseth, Ed. Springer Berlin Heidelberg, 1994, vol. 765, pp. 386–397.

[18] J. Szczepanski, J. Amigo, T. Michalek, and L. Kocarev, "Cryptographically secure substitutions based on the approximation of mixing maps," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 52, no. 2, pp. 443–453, Feb 2005.

[19] J. Detombe and S. Tavares, "Constructing large cryptographically strong s-boxes," in *Advances in Cryptology AUSCRYPT '92*, ser. Lecture Notes in Computer Science, J. Seberry and Y. Zheng, Eds. Springer Berlin Heidelberg, 1993, vol. 718, pp. 165–181.

[20] G. Leander and A. Poschmann, "On the classification of 4 bit s-boxes," in *Arithmetic of Finite Fields*, ser. Lecture Notes in Computer Science, C. Carlet and B. Sunar, Eds. Springer Berlin Heidelberg, 2007, vol. 4547, pp. 159–176.

[21] A. Webster and S. Tavares, "On the design of s-boxes," in *Advances in Cryptology CRYPTO 85 Proceedings*, ser. Lecture Notes in Computer Science, H. Williams, Ed. Springer Berlin Heidelberg, 1986, vol. 218, pp. 523–534.

[22] R. Forri, "The strict avalanche criterion: Spectral properties of boolean functions and an extended definition," in *Advances in Cryptology CRYPTO 88*, ser. Lecture Notes in Computer Science, S. Goldwasser, Ed. Springer New York, 1990, vol. 403, pp. 450–468.