Parallel multi-layer selector S-Box based on lorenz chaotic system with FPGA implementation

Mohamed Saber, Esam A. A. Hagras
Department of Communications and Computers, Faculty of Engineering,
Delta University for Science & Technology, Egypt

Article Info

Article history:

Received Jan 2, 2020
Revised Mar 5, 2020
Accepted Mar 19, 2020

Keywords:

Chaotic systems
FPGA
S-Box

ABSTRACT

The substitution box (S-Box) is the main block in the encryption system, which replaces the non-encrypted data by dynamic secure and hidden data. S-Box can be designed based on complex nonlinear chaotic systems that presented in recent papers as a chaotic S-Box. The hardware implementation of these chaotic systems suffers from long processing time (low speed), and high-power consumption since it requires a large number of non-linear computational models. In this paper, we present a high-speed FPGA implementation of Parallel Multi-Layer Selector Substitution Boxes based on the Lorenz Chaotic System (PMLS S-Box). The proposed PMLS chaotic S-Box is modeled using Xilinx System Generator (XSG) in 32 bits fixed-point format, and the architecture implemented into Xilinx Spartan-6 X6SLX45 board. The maximum frequency of the proposed PMLS chaotic S-Box is 381.764 MHz, with dissipates of 77 mwatt. Compared to other S-BOX chaotic systems, the proposed one achieves a higher frequency and lower power consumption. In addition, the proposed PMLS chaotic S-Box is analyzed based on S-Box standard tests such as; Bijectivity property, nonlinearity, strict avalanche criterion, differential probability, and bits independent criterion. The five different standard results for the proposed S-Box indicate that PMLSC can effectively resist crypto-analysis attacks, and is suitable for secure communications.

Corresponding Author:

Mohamed Saber,
Department of Communications and Computers,
Faculty of Engineering,
Delta University for Science & Technology,
Gamasa, Mansoura, Egypt.
Email: mohamed.saber@deltauniv.edu.eg

1. INTRODUCTION

Chaos theory in a complex system has been cited increasing in several different scientific areas, especially in engineering science such as cryptography and secure communication [1]. All Chaotic systems are sensitive to initial conditions, control parameters and unpredictable behaviors [2]. The chaotic maps are nonlinear dynamic systems that satisfy all the nonlinearities behaviors properties. In a cryptographic block cipher, the substitution Boxes are the only nonlinear component used in encryption systems such as advanced and data encryption standard [3]. Chaotic S-Box is a hybrid scheme to improve the nonlinearity of the S-Box based on chaos characteristics. In recent years, many chaotic S-boxes have been introduced [4-9]. The works in [10] design a chaotic S-Box by combining the chaotic Lorenz and Rossler systems. Also, a strong S-Box design based on 4D-4 Wing Hyperchaotic System [11].

Recently, Xilinx System Generator (XSG) for Digital Signal Processor (DSP) applications is a library integrated inside Simulink program permits to design, simulate, and produce a VHDL code for a digital hardware model of different computational and communication systems [12]. The main advantage of XSG is the simplicity of generating a VHDL code for complex hardware systems and provide the required synchronization between different parts of the model in the graphical user interface (GUI), which consider as a difficult task in complex digital systems [13-14]. Another advantage provided by XSG is hardware co-simulation in which a hardware model implemented into the FPGA board can be simulated in the MATLAB program environment. The design and FPGA implementation of the Lorenz chaotic system has been studied in [15-16].

The originality of our approach is that the hardware implementation of the proposed architecture allows a very useful and attractive trade-off between high speeds, low area cost and high nonlinearity of the PMLS S-Box. The main achievements of this paper are summarized as follows:

a) We propose a low power and high-speed XSG-FPGA implementation of proposed PMLS S-Box based on the Lorenz Chaotic System (381.764 MHz with dissipates of 77 mwatt).

b) We discuss the properties of the software and the XSG-FPGA implementation of the Lorenz chaotic system and investigate its chaotic behavior.

c) Standards security analysis is used to verify the performance of the implemented S-box, and it has good security results.

This paper organized as follows: Section 2 discussed the mathematical model of the Lorenz chaotic system and explained a new low power and high-speed architecture of PMLS S-Box. Next, Section 3 describes the FPGA Implementation of the Proposed PMLS S-Box. Proposed PMLS S-Box Hardwire Implementation Analysis has been introduced in Section 4. In Section 5, the proposed PMLS S-Box performance analysis has been considered. Results and security analysis for the proposed PMLS S-Box are given in Section 6. Finally, conclusions are presented.

2. PROPOSED PMLS S-BOX ARCHITECTURE

Lorenz chaotic system is an example of a three-dimensional nonlinear dynamical system, and can be described by the following equations [17]:

$$\dot{x} = \sigma * (y - x) \tag{1}$$

$$\dot{y} = r * x - y - x * z \tag{2}$$

$$\dot{z} = x * y - \beta * z \tag{3}$$

Where σ, r, β called the control parameters which are greater than zero and the values of σ, β, r are 10, 2.666 and r is varied, respectively and the output signals x, y, and z are a fractions numbers between 0 and 1. Figure 1 shows a bifurcation diagram for the Lorenz chaotic system at $\sigma = 10, \beta = 2.66, r = 28$ and initial conditions of $x_o = 10, y_o = 10,\ z_o = 10$. In this paper, we used the Runge Kutta algorithm (RG4) to solve the three-dimensional nonlinear dynamical equations [17].

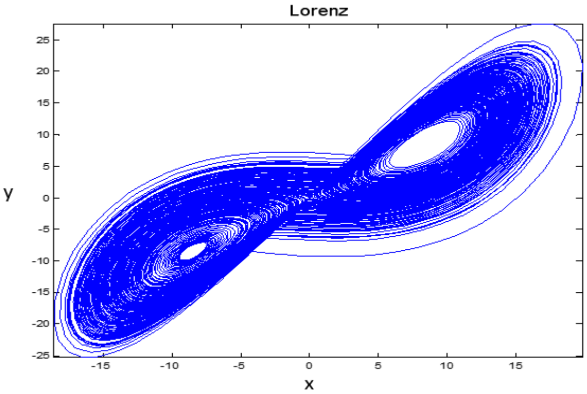

Figure 1. Bifurcation diagram of Lorenz chaotic map

The architecture of the proposed PMLS S-Box, as shown in Figure 2, consists of 3 main blocks. The first block is the 'Lorenz generator' block, which generates three random fractions numbers x, y and z according to the (1,2, and 3). The second block is ‘Mod (256)’ consists of three ‘Mod’ subblocks used to converts the Lorenz generator fraction output x, y and z into decimal integer numbers X, Y and Z from the range 0 to 255 values.

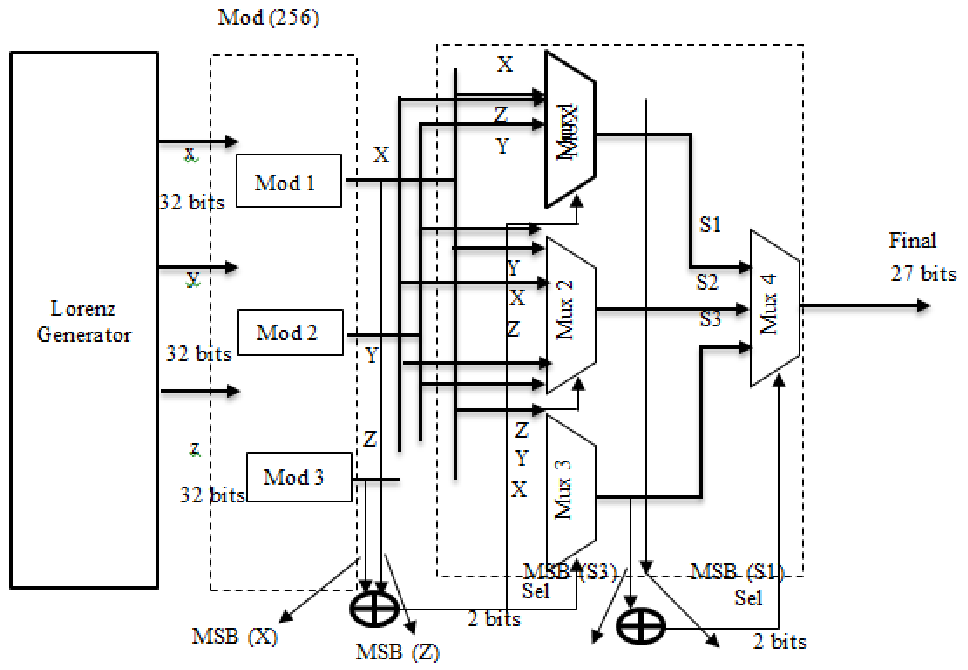

Figure 2. Block diagram of proposed PMLS S-Box

The second block is the ‘Parallel Multiplexers’ block which consists of 4 multiplexers ‘Mux’ subblocks, The ‘Mux’ blocks are organized in multilayer structure, the first layer uses a 3 blocks in parallel, each one of them receives the 3 numbers (X, Y, Z) in different order and generates a random one of them. The first multiplexer receives (X, Z, and Y) and generates (S1), the second multiplexer receives (Y, X, and Z) and generates (S2), while the last one receives (Z, Y, and X). and generates (S3). The selection bits used for the three multiplexers come from the ‘Select’ block. The second layer of multiplexers consists of one ‘Mux’ subblocks which receives the three random numbers S1, S2, S3, and selects only one output of them to represent the final output, the selection operation depends on the MSB of the input signals S1 and S3.

The ‘Sel’ signal is a two bits used to provide the selection for the first layer multiplexers (Mux 1, Mux 2, Mux 3) prepared by extraction the most significant bit (MSB) from the binary number X, and also the MSB from the number Z, adds the two MSBs together and the output considered as a selection bits for the 3 multiplexers. For the second layer multiplexers (Mux 4), the ‘Sel’ is prepared by extraction of MSBs from S1 and S3. The proposed PMLSC S-box operation algorithm can be summarized as follows:

1) Select initial parameters and values of $\sigma, \beta, r, x_o, y_o, z_o$
2) Calculate x, y , z where ($0 < x, y, z < 1$)
3) Generate 2^{14}values of x, y, z, and ignore the first 5000 values.
4) Calculate x=mod(x,256)
    - Multiply the fractional values of (x, y, z) by 2^{14}
    - Ignore the fraction part and consider only the integer part
    - Divide the integer by 256 (shift right eight places in a hardware implementation)
    - Ignore the fraction part and consider only the integer part.
    - The obtained integer part represents the X=mod (x, 256)
5) Repeat 2 to calculate Y=mod (y, 256)
6) Repeat 2 to calculate Z=mod(z, 256)
7) Multi Selector Mechanism
    - The multi-layer contains first layer selection to generate (S1, S2, S3), and the second layer generates the final output, which is a number S1 or S2 or S3.
    - Extract MSBs of X, and Z.

- A binary number is given by the summation of the two MSBs of each X, and Z.
- The binary number (Sel.) is used to control the three multiplexers selection.
- For the first multiplexer in the first layer with output S1.
- If sel = “00”, S1← X. - If sel = “01”, S1← Z.
- If sel = “10”, S1← Z. - If sel =”11”, S1←Y.
- For the second multiplexer in the first layer with output S2
- If sel = “00”, S2← Y. - If sel = “01”, S2 ← X.
- If sel = “10”, S2← X. - If sel=”11”, S2 ← Z.
- For the third multiplexer in the first layer with output S3
- If sel = “00”, S3← Z. - If sel = “01”, S3← Y.
- If sel = “10”, S3← Y. - If sel=”11”, S3 ← X.
- Extract MSBs of S1 and S3.
- A binary number is given by the summation of the two MSBs of each S1 and S3.
- The binary number (Sel.) is used to control the multiplexer selection.
- For the multiplexer in the second layer with output final
- If sel = “00”, final← S1. - If sel = “01”, final ← S2.
- If sel = “10”, final← S3.

8) Final S-Box Output
   - The S-Box Outputs are the last 256 decimal numbers selected from the multiplexer selector.
   - The obtained 256 decimal numbers of the S Box, all S Box are checked if there are repeated numbers, the process goes back to step 1 until there are no repeated numbers in the S Box.
   - The final multiplexer number selector is non-repeated numbers of 16x16 Chaotic S-Box Outputs.
   - Store the non-repeated numbers of 16x16 Chaotic S-Box Outputs.

3. FPGA IMPLEMENTATION OF PMLS S-BOX

The proposed PMLS S-Box is modeled using XSG, the architecture is implemented into the Xilinx Spartan-6 X6SLX45 board with a maximum frequency of 381.764 MHz and dissipates 77 *m*watt. The S-Box architecture is modeled using XSG in 32 fixed-point format because the system operates with real numbers (numbers with a fractional part). The speed of operation is the main feature of using the fixed-point format in arithmetic operations instead of using the floating-point format. In different applications where high accuracy is not required, the fixed-point format is used [18-20]. The fixed-point format of the model is $Q4.28$ where 4 is the number of bits representing the integer part, while 28 is the number of bits representing the fraction part. The proposed PMLS S-Box hardware model as in the XSG program is shown in Figure 3, and it represents the block diagram shown in Figure 2.

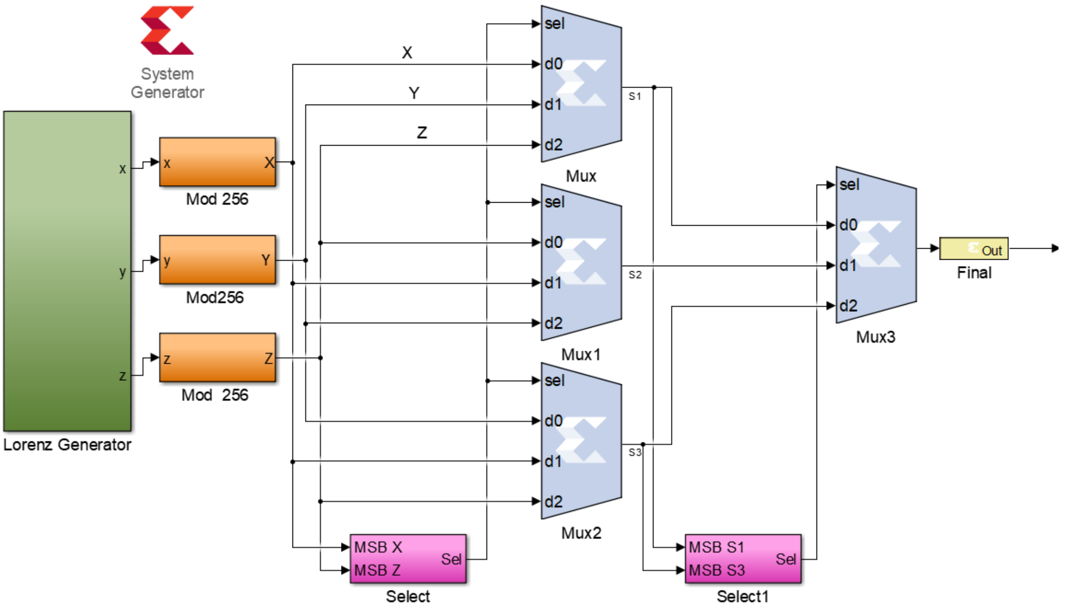

Figure 3. XSG hardware model of the proposed PMLS S-Box

The hardware model of Lorenz generator block is shown in Figure 4 while, Figure 5 shows the simulated and XSG implemented the bifurcation diagram for the Lorenz chaotic system. It is shown from Figure 5 that the Lorenz chaotic system has a random behavior, and these results are identical to those obtained using the numerical method in Figure 1.

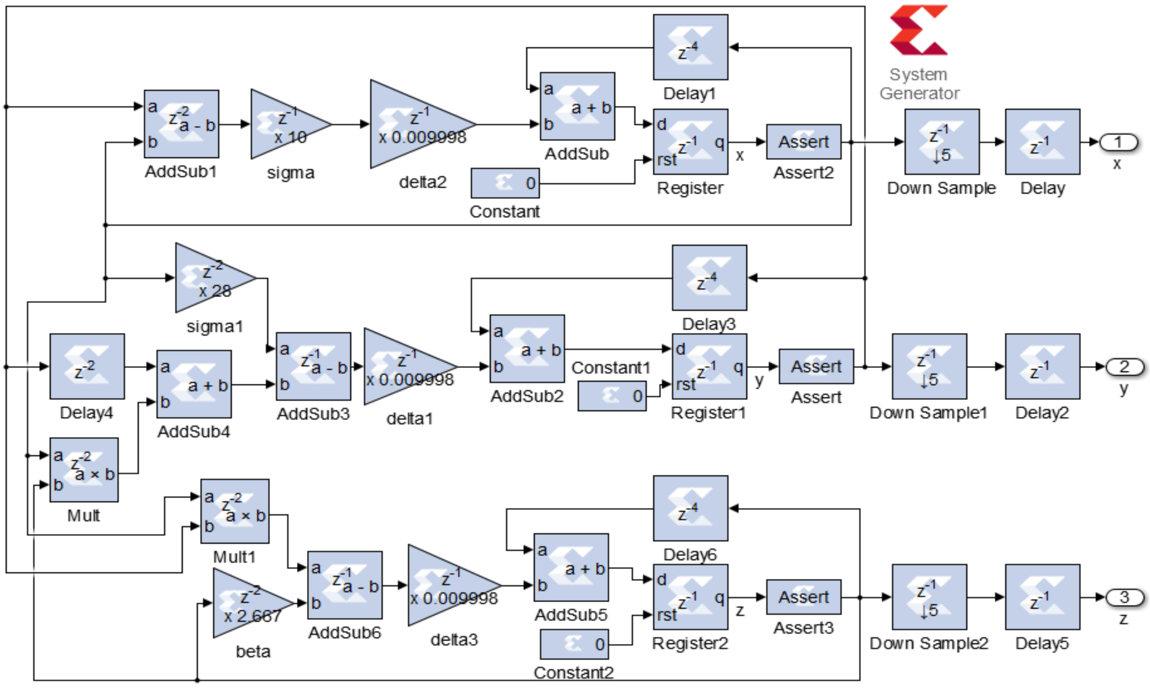

Figure 4. XSG hardware model of Lorenz generator block

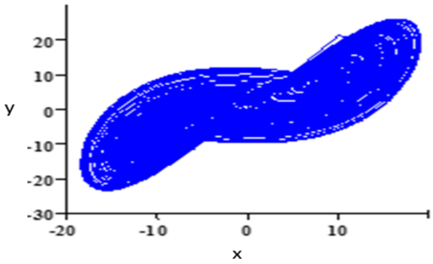

Figure 5. XSG bifurcation diagram for the hardware Lorenz generator model

4. PROPOSED PMLS S-BOX HARDWARE IMPLEMENTATION RESULTS

After the implementation of the model, the device utilization summary which indicates how much resources (Registers, LUT, LUT flip-flops) of the FPGA device are used to implement the proposed PMLS S-Box architecture is shown in Table 1.

Table 1 Device utilization report of the implementation of proposed PMLS S-Box

Resources	Utilization
Slice Registers	574/5476
LUTs	163/27288
Flip Flops	15/589
Multipliers	5
No. of Bonded IOBs	28/316
Max. Frequency	381.764 MHz
Power	77 mWatt

A hardware implementation comparison results between our work and the similar work in recent years are shown in Table 2. Indicates that the proposed method consumes the lower number of resources compared to different methods, with a high clock frequency and low power consumption.

Table 2. Comparison between proposed PMLS S-Box and similar works

Reference	Analysis method	Area Resources				Max. freq. (MHz)	Power (mW)
		Slice registers	LUTs	Bonded IOBs	Multipliers		
A. Akgul [21]	RK4	10630	17160	131	11	86.36	-
M. Azzaz [22]	RK4	1695	3251	-	78	38.86	321
S.Sadoudi [23]	RK4	1138	1969	11	40	22.850	-
M. Alcin [24]	RK4	86329	87207	195	-	266.429	-
I. Koyuncu [25]	RK4	42021	39309	133	-	373.094	-
M. Tuna [26]	RK4	45805	47273	131	-	390.067	-
K.Rajagopal[27]	RK4	94323	89129	195	-	325.759	-
E. Gerardo [28]	RK4	476	928	16	-	31.33	-
B. Karakaya[29]	Euler	165	311	3	22	59.492	-
Proposed system	RK4	154	163	28	7	381.764	77

5. PROPOSED PMLS S-BOX PERFORMANCE ANALYSIS

The substitution box is a nonlinear element widely used on cryptosystem; the mathematical model of S-Box cryptanalysis is presented in [30]. Five tests are used to measure the performance of S-Boxes; the bijective property, nonlinearity, distribution outputs Bit Independence Criterion (BIC), Strict Avalanche Criterion (SAC), and equiprobable input/output XOR. The final S-Box cryptanalysis results of the proposed PMLS S-Box are given in Table 3. In [31-33], a brief description of the five standard tests are reported. Comparison and the security analysis of the proposed PMLS S-Box and author S-Box methods are given in Table 4. The results shown in Table 4, indicate that the proposed PMLS S-Box can effectively resist the cryptanalysis attacks, and it is suitable for secure communications.

Table 3. The final PMLS S-Box results

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	133	153	173	177	197	217	237	241	5	25	45	49	69	89	109	113
1	6	26	46	50	70	90	110	114	134	154	174	178	198	218	238	242
2	135	155	175	179	199	219	239	243	7	27	47	51	71	91	111	115
3	8	28	48	52	72	92	112	116	136	156	176	180	200	220	240	244
4	137	157	161	181	201	221	225	245	9	29	33	53	73	93	97	117
5	10	30	34	54	74	94	98	118	138	158	162	182	202	222	226	246
6	139	159	163	183	203	223	227	247	11	31	35	55	75	95	99	119
7	12	32	36	56	76	96	100	120	140	160	164	184	204	224	228	248
8	141	145	165	185	205	209	229	249	13	17	37	57	77	81	101	121
9	14	18	38	58	78	82	102	122	142	146	166	186	206	210	230	250
A	143	147	167	187	207	211	231	251	15	19	39	59	79	83	103	123
B	16	20	40	60	80	84	104	124	144	148	168	188	208	212	232	252
C	129	149	169	189	193	213	233	253	1	21	41	61	65	85	105	125
D	2	22	42	62	66	86	106	126	130	150	170	190	194	214	234	254
E	131	151	171	191	195	215	235	255	3	23	43	63	67	87	107	127
F	4	24	44	64	68	88	108	128	132	152	172	192	196	216	236	256

Table 4 Comparison and the security analysis of different chaotic S-box and the proposed PMLS S-Box

		Nonlinearity			SAC		BIC-	BIC-	
S Box	Min.	Max.	Avg.	Min	Max	Avg.	SAC	Nonlin	DP
Proposed	104	110	106. 5	0.3750	0.6094	0.5010	0.5022	103.07	0.03905
Ref. [24]	104	108	106.75	0.4063	0.6250	0.4976	0.5022	103.57	0.03906
Ref. [25]	102	106	104	0.3750	0.6094	0.4980	0.4971	103.29	0.03906
Ref. [26]	100	106	103.25	0.4219	0.5938	0.5049	0.5010	103.71	0.03906
Ref. [27]	96	106	103	0.3906	0.6250	0.5039	0.5010	100.36	0.03906
Ref. [28]	102	108	104.75	0.3906	0.5056	0.5056	0.5022	104.07	0.04688
Ref. [29]	98	108	104.25	0.2813	0.6094	0.4954	0.5048	102.86	0.04688
Ref. [30]	100	106	104	0.3750	0.6250	0.4946	0.5019	103.21	0.03906
Ref. [31]	100	106	103	0.3906	0.5938	0.5020	0.4999	102.93	0.03906
Ref. [32]	84	106	100	0.1250	0.6250	0.4812	0.4967	101.93	0.06250
Ref. [33]	84	106	100	0.1250	0.6250	0.4812	0.4967	101.93	0.06250

5.1. Bijectivity

The Boolean function f is bijective if and only the linear sum of the Boolean function f_i of each component of a $n \times n$ S-box is 2^{n-1} [30]. The Bijectivity characteristic can be calculated based on $wt\,(\sum_{i=1}^{n} a_i\ f_i) = 2^{n-1}$,where a_i ∈ {0,1}, (a1 , a2 , ….. , an) ≠ (0 , 0 , ….. , 0) , wt () denotes humming weight. The proposed S Box is has the Bijectivity characteristic because the biject values is equal 128 equal to the ideal value.

5.2. Nonlinearity

Let $f(x)\colon \mathrm{f}_2^n\ \rightarrow f_2$ be a n Boolean function, the nonlinearity of $f(x)$ can be written as

$$N_f = \ {}_{1\in L_n}^{min} d_H\,(f,l) \tag{4}$$

Where $\mathrm{L_n}$ is a function set which contains all linear and affine functions, $\mathrm{d_H}$ (f, l) denotes the hamming distance between f and l.

The nonlinearity defined by Walsh spectrum is

$$N_f = 2^{-n}(1 - {}_{w\in Gf(2^n)}^{max} \left|s_{<f>}(\omega)\right|) \tag{5}$$

The nonlinearity of 8 output bits of the proposed S-Box is 104 minimum, 110 maximum, 106.5 average. Table 4 presents a comparison between the nonlinearity of the proposed PMLS S-Box and another S-Boxes. It is clear from Table 4, and the proposed PMLS S-Box can resist the linear cryptanalysis.

5.3. Strict avalanche criterion (SAC)

In SAC, if one bit in the input of the Boolean function changed, the changing probability of every bit in its output should be 0.5. The SAC of the proposed S Box is calculated based on the method given in [28]. The Min., Max., and average values of the SAC of the proposed S Box are 0.3750, 0.6094 and 0.5010, respectively. Table 4 gives a comparison for the Min., Max., and average values of the SAC of the proposed S Box and recent S Box generated by various algorithms. It is observed that the average values of the SAC of the proposed S-Box are very close to the ideal average values of the SAC (0.5000).

5.4. Differential probability

The Differential Probability (DP) is introduced in [32], and it is employed to reflect the XOR distribution of the input and output of the boolean function. The DP can be calculated as:

$$DP_f = max_{\Delta x\neq 0,\Delta y}\left(\frac{\#\{x\epsilon X|f(x)\theta f(x\theta\Delta x)=\Delta y\}}{2^n}\right) \tag{6}$$

where x represents the set of all possible input, 2^n is the number of elements in the set. This test is desired that the computed value is as small as possible. As shown in Table 4, the maximum value is equal to 0.03905, which indicates that the proposed S Box has a strong immunity to resist the differential attack.

5.5. Bit independent criterion (BIC)

Assume that for a given Boolean function, x_i, and $x_k (j \neq k)$ is a two bits output of an S-Box, if $x_i \oplus x_k$ is high nonlinear and satisfy the SAC, then the correlation coefficient of each output bit pair is approximately equal to 0 when one input bit is inversed. Therefore, we can check the BIC of the S-Box by verifying $x_i \oplus x_k$, $(j \neq k)$ of any two output bits of the S-Box achieves the nonlinearity and SAC. The BIC is similarly desired that the nonlinearity values are as high as possible and that the SAC is close to the ideal value of 0.5 [33].

5. CONCLUSION

In this paper, high speed and low power FPGA hardware implementation of a new design Parallel Multi-Layer Selector Substitution Boxes based on Lorenz Chaotic System (PMLS S-Box) is presented. The proposed PMLS S-Box architecture is implemented into the Xilinx Spartan-6 X6SLX45 board. The proposed architecture hardware model used 574 slice registers, 163 Luts, 15 flip-flops, and five multipliers as shown in the device utilization report. The maximum frequency of the proposed PMLS S-Box is 381.764 MHz and dissipates 77 $m$watt. A comparison between the proposed PMLS S-Box and similar work is presented and indicated that the proposed design consumes the lower number of resources compared to recent different methods, with a high clock frequency and low power consumption. The proposed PMLS S-Box achieved the values (104- 110- 106.5) as minimum, maximum, average respectively in nonlinearity tests. Also, for the SAC test, the proposed model archived (0.3750, 0.6094, 0.5010) as a minimum, maximum, average respectively. The five standard test results indicate that the proposed PMLS S-Box can effectively resist the crypto-analysis attacks and the proposed PMLS S-Box is suitable for secure communications applications

REFERENCES

[1] P. Zhen, G. Zhao, L. Min and X. Li, "A Survey of Chaos-Based Cryptography," 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, Guangdong, pp. 237-244. 2014.

[2] H. A Abdullah, H. N Abdullah, "FPGA implementation of color image encryption using a new chaotic map," *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 13, No. 1, pp. 129–137, 2019.

[3] F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, pp. 647-652. 2017.

[4] I. Hussain, T. Shah, M. Gondal, "A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm," *Nonlinear Dyn*, Vol. 70 (3), pp.1791–1794, 2012.

[5] Y. Wang, K. Wong, C. Li, Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys Letter A*, Vol. 376 (6), pp.827–833, 2012.

[6] D. Lambic, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn*, vol. 87, no. 4, pp. 2407–2413, 2017.

[7] A. Belazi, A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map". *Optik, Int., J Light Electron, Opt.*, vol. 130, pp. 1438–1444, 2017.

[8] M. Asim and V. Jeoti, "Efficient and simple method for designing chaotic S-boxes," *ETRI Journal*, vol. 30, no. 1, pp. 170–172, 2008.

[9] M. Khan, T. Shah, S. Batool, "Construction of S-box based on chaotic Boolean functions and its application in image encryption". *Neural Com., Appl.*, vol. 27(3), pp.677–685, 2017.

[10] M. Khan, T. Shah, H. Mahmood, M. Gondal, I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems", *Nonlinear Dyn.*, vol. 70 (3), pp. 2303–2311, 2012.

[11] U. Islam, G. Liu, "Designing S-Box Based on 4D-4Wing Hyperchaotic System," *3D Research*, vol. 8, 2017.

[12] Xilinx, Vivado, Design Suite User Guide: Model-Based DSP Design using System Generator, UG897, v2016.1 ed., Xilinx, Apr. 2018.

[13] Y. Yusuf, D. Mohd,N. Yaacob," Hardware simulation for exponential blind equal throughpout algorithm using system generator," *International Journal of Electrical and Computer Engineering*, Vol. 9, No.1, pp. 171-181, 2019.

[14] Xilinx, Inc., *Synthesis and Simulation Design Guide*, UG626 (v 14.5), 2012.

[15] M. Aseeri, M. I. Sobhy, and P. Lee, "Lorenz chaotic model using field programmable gate array (FPGA)," in *The 45th Midwest Symposium on Circuits and Systems*, vol. 1, 2002.

[16] L. Merah, A. Ali-Pacha, N. H. Said, and M. Mamat, "Design and FPGA implementation of Lorenz chaotic system for information security issues," *Applied Mathematical Sciences*, vol. 7, pp. 237–246, 2013.

[17] O. Fatih, B. Ahmet,"A method for designing strong S-Boxes based on chaotic Lorenz system", *Physics Letter A*, Vol. 374, pp. 3733-3738, 2010.

[18] Jr. Cgharles, H. Roth, Lizy, K. John, *Digital System Design Using VHDL*, Cengage Learning. 3rd Edition, 2017.

[19] Kadhiem Ayob, *Fundamental of Timing in FPGA*, Create Space Independent Publishing Platform, 2015.

[20] A. Rani, N. Grover, "An Enhanced FPGA Based Asynchronous Microprocessor Design using VIVADO and ISIM, " Bulletin of Electrical Engineering and Informatics, Vol. 7, No. 2, pp. 199-208, 2018.

[21] A. Akgul, H. Calgan, I. Koyuncu, I. Pehlivan, A. Istanbullu, "Chaos-based engineering applications with a 3D chaotic system without equilibrium points," *Nonlinear Dyn*, vol 84, pp 481-495, 2015.

[22] M.S. Azzaz, C. Tanougast, S. Sadoudi, R. Fellah, A. Dandache, "A new auto-switched chaotic system and its FPGA implementation," *Commun. Nonlinear Sci. Numer. Simul*, vol 18, pp 1792-1804, 2013.

[23] S. Sadoudi, M.S. Azzaz, M. Djeddou, M. Benssalah, "An FPGA Real-time Implementation of the Chen"s Chaotic System for Securing Chaotic Communications," *Int. J. Nonlinear Sci.*, vol. 7, pp 1749-3889, 2009.

[24] M. Alçın, İ. Pehlivan, İ. Koyuncu, "Hardware design and implementation of a novel ANN-based chaotic generator in FPGA," *Opt. - Int. J. Light Electron Opt*, vol 127, pp. 5500-5505, 2016.

[25] I. Koyuncu, A.T. Ozcerit, I. Pehlivan, "Implementation of FPGA-based real time novel chaotic oscillator," *Nonlinear Dyn.*, vol. 77, pp 49-59, 2014.

[26] M. Tuna, C.B. Fidan, "Electronic circuit design, implementation and FPGA-based realization of a new 3D chaotic system with single equilibrium point," *Opt. - Int. J. Light Electron Opt.*, vol 127, pp 11786-11799, 2016.

[27] K. Rajagopal, A. Akgul, S. Jafari, A. Karthikeyan, I. Koyuncu, "Chaotic chameleon: Dynamic analyses, circuit implementation, FPGA design and fractional-order form with basic analyses," *Chaos, Solitons & Fractals*, vol. 103, pp 476-487, 2017.

[28] L. Gerardo, E. Torres, E. Tlelo, C. Mancillas, " Hardware Implementation of Pseudo-random number generator based on chaotic maps," *Nonlinear Dynamics*, vol. 90, pp 1661-670, 2017.

[29] B. Karakaya, A. Gulten, M. Frasca, "A true random bit generator based on a memristive chaotic circuit: Analysis, design and FPGA Implementation," *Chaos, Solitons and Fractals*, vol. 119, pp. 143-149, 2018.

[30] G. Chen G, "A novel heuristic method for obtaining S-boxes," Chaos Solitons Fractals, vol. 36 (4), pp.1028–1036, 2008.

[31] V. M.S. Garcia, R. F. Carapia, C. R. Marquez, B. L. Benoso, M. A. Perez, " Substitution box generation using chaos: An image encryption application," *Applied Mathematics and computation*, vol. 332, pp 123-135, 2018.

[32] Y. Tian Ye, L. Zhimao, "Chaotic S-box: six dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling," *Nonlinear Dynamics*, vol. 94(3), pp 2155-2126, 2018.

[33] Y. Wang, Q. Xie, Y. Wu and B. Du, "A Software for S-box Performance Analysis and Test," *2009 International Conference on Electronic Commerce and Business Intelligence*, Beijing, 2009, pp. 125-128

BIOGRAPHIES OF AUTHORS

Mohamed Saber, born in Mansoura, Egypt on the 2nd of February 1979. Received BSc Degree In Communication and Electronics From Faculty of Engineering, Mansoura University 2001. He received MSc Degree In Electrical Communications Faculty of Engineering, Mansoura University in 2006. He received Ph.D. Degree In Informatics and Communications, Graduated School of Information Science and Electrical Engineering, Kyushu University, Japan, 2012. He works as an assistant professor at Delta university for science and Technology, Gamasa, Mansoura, Egypt. His research interests are: Digital signal processing, Design and implement digital communication systems on FPGA and DSP circuits, Synchronization (time, frequency, phase) in digital receivers.

Esam A. A. Hagras received a B.Sc. degree in Electrical Engineering from Alexandria University, Egypt in 1994, an M.Sc. degree in Electrical Engineering from Mansoura University, Egypt, in 2001 and the Ph.D. degree in Electrical Engineering from Alexandria University, in 2008. He has been Head of Electronics & Communication Research Center, Armed Forces, Cairo, Egypt from 2015 to 2018. He is currently an Assistant Professor with Communications and Computer Department, Faculty of Engineering, Delta University for Science and Technology, Gamasa, Mansoura, Dakahlia, Egypt. His current research interests include data protection in digital communication systems and developments of the new encryption algorithm