Dijlah Journal of Engineering Sciences (DJES) **Vol. 1, No. 3, Dec., 2024, pp. 22-32**
ISSN: Printed: 3078-9656, Online: 3078-9664, paper ID: 013

Implement of Substitution Boxes for DES Based Field Programming Gate Array and VHDL

Jabbar S. Jahlool[1], Nazar J. Hussain[2], Ali M. Kadhim[3], Ali Alsalhi[4]
[1,2,3] Department of computer engineering techniques, University of Dijlah, Baghdad, Iraq
jabbar.shatti@duc.edu.iq, nazar.jabar@duc.edu.iq, ali.alsalihy@duc.edu.iq

Article Info

Article history:

Received Oct., 2, 2024
Revised Nov., 13, 2024
Accepted Dec. 20, 2024

Keywords:

DES
FPGAs
S-Box
VHD
Block Cipher

ABSTRACT

Nowadays the implementation of a cryptographic system based on traditional means is a late topic due to the development and multiplicity of detection methods, intrusion and hacking. Therefore, it is necessary to resort to more modern methods, such as the use of programmed digital electronic circuits like Field Programmable Gate Arrays (FPGAs). The objective of this paper is to design substitution box (S-Box) for Data Encryption Standard (DES) using Very High Speed Hardware Description Language (VHDL). As a result, S-box VHDL code was designed and written then by using the capabilities of the Xilinx Design Suite ISE the design was checked, analyzed, simulated and then a file called bit stream will be generated. The resulting file was downloaded to the FPGA circuit and the equivalent physical digital circuit representing the S-box was obtained.

Corresponding Author:

Jabbar S. Jahlool
Department of Computer Engineering Techniques, University of Dijlah
Almasafi street, Baghdad, Iraq
Email: jabbar.shatti@duc.edu.iq

1. INTRODUCTION

In today's world, encrypt has become the main aspect of life. Therefore, the focus in this aspect is on secure communication, which has become the main requirement for every organization. This can be achieved through various techniques such as encryption, password and biometrics. In general, encryption is the process of translating data into unknown data or a secret code that hides the true meaning of the information. The encryption process is done using one or more mathematical techniques to ensure that the information is protected from hacking, eavesdropping, theft, or any other means that distorts the data from its true meaning [1],[2].

In any cryptographic algorithm, S-box is considered to be the important part. Regardless of size of S-box, its properties makes it to be the best part in any cryptographic algorithm [3]. An important part of the encryption process is replacing the characters of the plain text with specific characters. It may be a mechanism to replace one or more characters of the plain text with specific rules, which is a mathematical algorithm designed for this purpose [4],[5]. To improving the Enhancing Secure Data Encryption Standard (ES-DES) against cryptanalysis attacks, this is possible by improving DES security by expanding S-Boxes as well as increasing key size [6].

Based on FPGA and features that proved faster and increasingly adjustable arrangement, the triple key AES whose design and implemented [7]. Effective calculations require relying on high-performance devices at the same time fast, and these electronic devices are FPGA. By creating parallel processing elements (PEs) called virtual processors, these devices allow the ability to perform parallel computing. Any system implemented by FPGAs provides more accurate and faster results than those implemented using computers, even when parallel processing techniques are based on computers [8],[9]. Design of AES S-Box depend on the a quicker, more customizable

hardware solution by FPGA and VHDL, this hardware implementation give efficiency of speed, security , size and power consumption [10].

Four different methods of S-box are discussed, S-box based on ROM or lookup table, modified lookup table that uses multiplexers and decoders makes total substitution faster, computational method has composite field structure to compute the substitution byte and a combination of arithmetic and lookup table method where previously computed inverse multiplication values are stored in lookup table [11],[12].

Implemented and tested DES algorithm depend on flexible, low cost and efficient encryption hardware solution by using FPGA. Method of iteration of loop, with128 bits key size and realized by lookup table based on S-box [13]. By researchers at IBM, the DES block cipher algorithm was developed and fine-tuned by the National Security Agency (NSA), government agencies, and the National Institute of Standards and Technology (NIST). The DES standard has been adopted as the federal standard for encryption of commercial and sensitive data by the American National Standards Institute (ANSI) standard. This is defined in the Federal Information Processing Standards (FIPS 46, 1977) and published by NIST [14],[15].

In this paper, a new simplified S-box design for DES using VHDL code and an FPGA digital device is demonstrated and implemented. After downloading the output design file (bit stream) to the FPGA, an equivalent digital S-box circuit was obtained which was checked and ensured that it worked for the purpose for which it was designed.

2. BRIEF CONCEPT OF DES

In short, the DES cipher system as shown in Figure 1 consists of 64-bit input data text encrypted with a 64-bit input key and output 64-bits cipher data. However, the key is actually 56-bit (effective bits), and 8 bit as parity check bits which are 8th, 16th, 24th, 32th, 40th, 48th, 56th and 64th bits. data text, first divided into blocks, each block is 64-bits, and then 64-bits data text is input to initial permutation function for initially permuting data text; two halves of transformed block are generated by initial permutation which are the left plain text (L) and right plain text (R), and each them plains is encrypted for 16 rounds and has its own key as shown in Figures 1 and 2.

Finally, the left and right plain text are re-connected together, for the purpose of performing the final permutation on the composed blocks; the result of this process is a 64-bit cipher text [16]-[20].

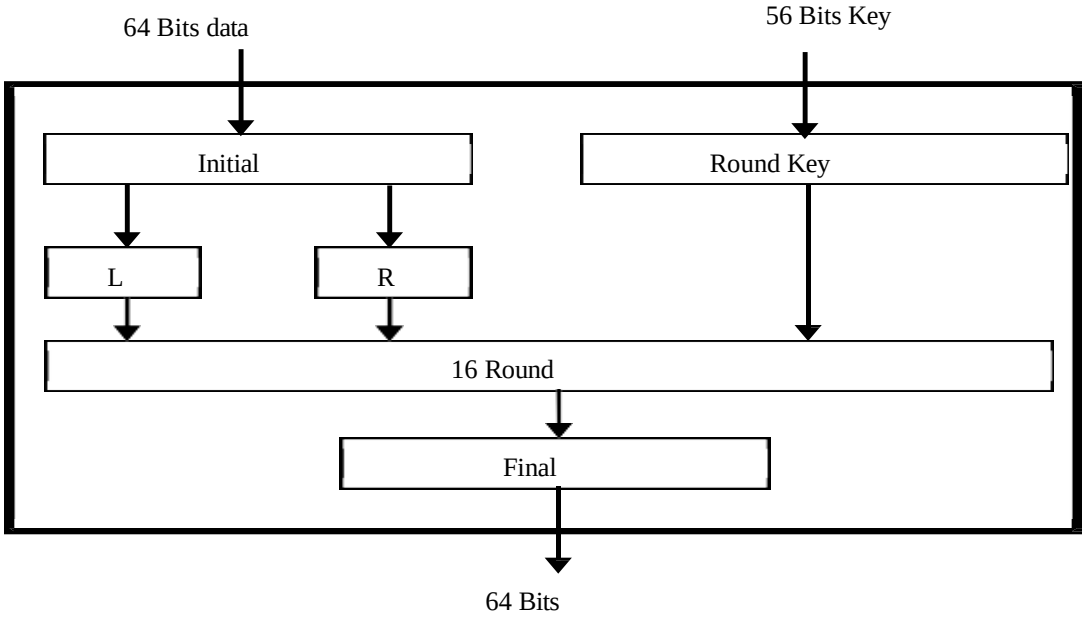

Figure 1. Block Diagram of DES Algorithm

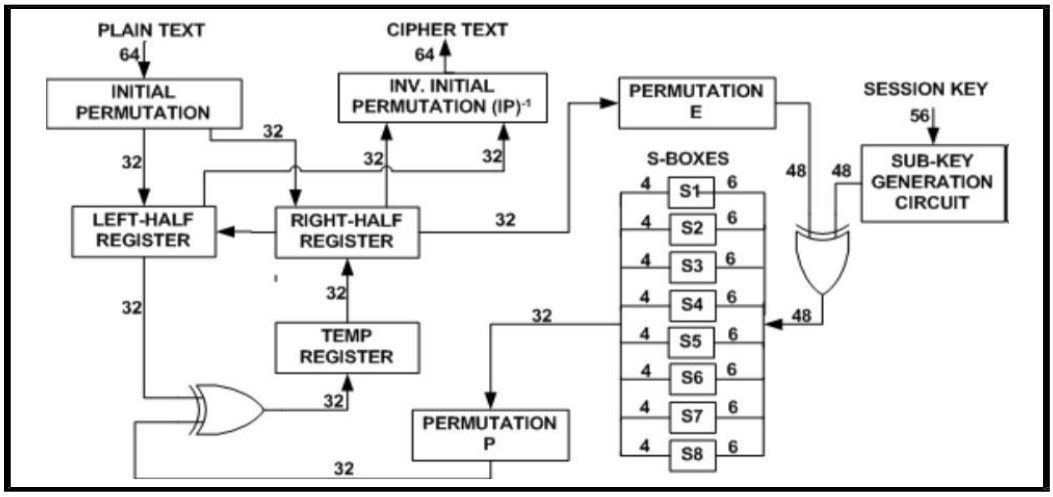

Figure 2. More Details Block Diagram of DES System

3. CLARIFY THE WORK OF S-BOXES

The S-box part, which is referred to as the F function of the DES algorithm, is the most important and the only non-linear operational part of this algorithm. Simply this part receives 48 bits and outputs 32 bits. As shown in the Figure 3 the 48 bits long input to the S-boxes is arranged into 8 blocks each of one is 6 bit denoted as (b1, b2, b3, b4, b5, b6). There are 8 S-boxes denoted as (S1, S2, . . . , S8) each of S-box accepts one of the 6 bit blocks as input. The S-box output of each is a 4 bit number [21].

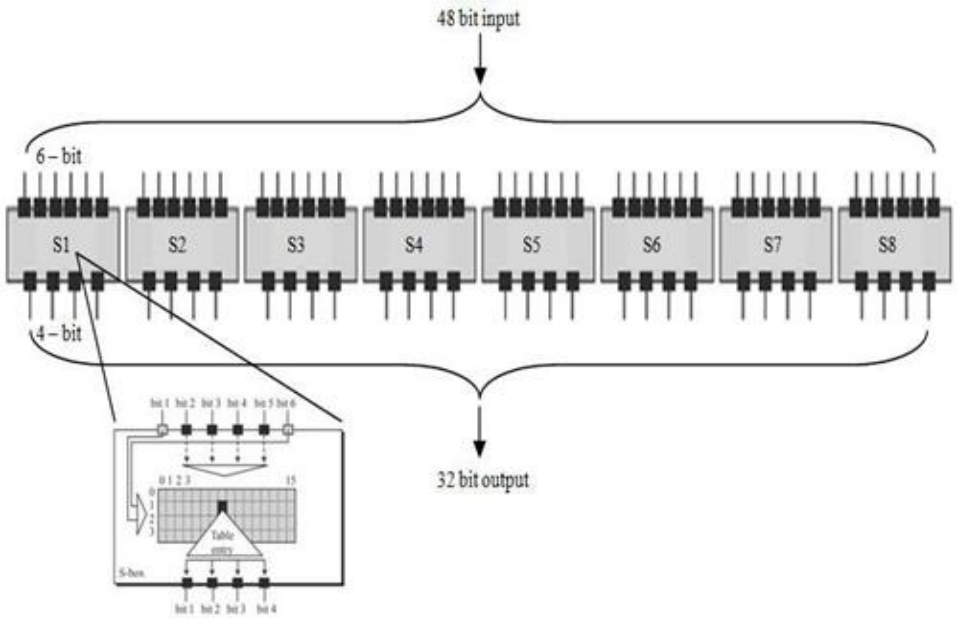

Figure 3. Blocks of S-box of DES Algorithm

Each of the 8 S-boxes can be thought of as a 4×16 matrixes as shown in the Table 1, it is the matrix of S-box S1. The contents of each box are calculated according to the following assumptions: Assume that each block of S-boxes is a matrix. Therefore each matrix cell is identified by a coordinate pair (i, j), where $0 \leq i \leq 3$ and $0 \leq j \leq 15$. The value of (i) is taken as the decimal representation of the first and last bits of the input to each

S-box, i.e. Dec(b1b6) = i and the value of (j) is take from the decimal representation of the inner four bits that remain, i.e. Dec(b2b3b4b5) = j. From this it is clear that, each cell within the S-box matrices contains a 4-bit number which is output once that particular cell is selected by the input.

Table 1. S1 Matrix Contents

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Or in another way, it is possible to explain how to calculate the contents of the boxes. If S1 is the function defined in Table 1 and B is a block of 6 bits, then S1(B) is determined as follows: The first and last bits of B represent in base 2 a number in the range 0 to 3. Let that number be i. The middle 4 bits of B represent in base 2 a number in the range 0 to 15. Let that number be j. Look up in the table the number in the i'th row and j'th column. It is a number in the range 0 to 15 and is uniquely represented by a 4 bit block. That block is the output S1(B) of S1 for the input B. For example, for input 011011 the row is 01, that is row 1, and the column is determined by 1101, that is column 13. In row 1 column 13 appears 5 so that the output is 0101. By the same mechanism, the contents of the others boxes are calculated and found as shown in tables (Tables 2 to 8 respectively).

Table 2. Contents of S2

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

Table 3. Contents of S3

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

Table 4. Contents of S4

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Table 5. Contents of S5

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Table 6. Contents of S6

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

Table 7. Contents of S7

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

Table 8. Contents of S8

Row No.	Column No.															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

In general the basic of S-boxes is as follows:

- Each S-box has six input bits and four output bits.
- The DES algorithm's strength comes from the nonlinear elements which are the S-boxes. This is because there is no output bit of an S-box too near to a linear function of the input bits.
- All possible outcomes must be included in each "row" of the S-box. (This characteristic makes the output random)
- The outputs of the S-box must differ by at least two bits when the difference two bits of the inputs of the S-box.

4. METHODOLOGY OF THE PROPODED DESIGN

The proposed code is written using VHDL language and by Xilinx ISE (Integrated Software Environment) digital system design software which is used to program Xilinx's digital circuits. The design is implemented using an FPGA electronic circuit. The FPGAs' device contains a number of features like it can programmable in the field i.e. outside the factory, reprogramming after manufacturing and installing in the fields.

The FPGA device usually consisting of an three programmable tools which are interconnect switches, logic blocks and input/output pins [22],[23]. VHDL is a design language that provides all the capabilities needed to describe a logic circuit. Intended logical circuit or system is any circuit or system used to process or store digital information. The VHDL also provides the possibility to build a model in which all tests or simulations can be performed to reach the desired goal, and then it can be used to create an actual working circuit. Magically and by means of software tools it is interpreted VHDL in a way that creates actual digital circuits in a process known as synthesis [24].

In order to build the required VHDL code, you must first understand and analyze the components of the S-box and know every bit of the cells of this S-box. As mention above the S-box consists of 8 blocks, each one has 6 bits input and 4 bits output as shown in the Figure 4. These bits denoted as 6 bits as address input and 4 bits as data input.

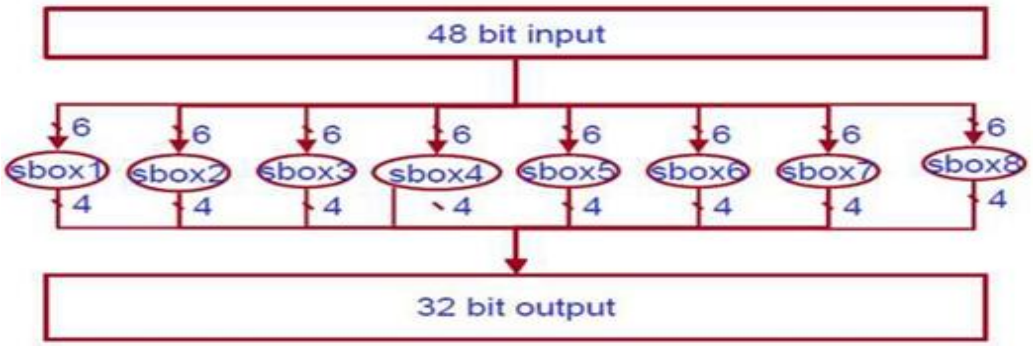

Figure 4. Blocks of S-Box Distribution

In other word each S-box is a two dimensional array as clear in Figure 5. Six address bits (b5b4b3b2b1b0), two row select bits (b5b0) and four bits (b4b3b2b1) for column select. The output of each block consists of 4 data bits (d3d2d1d0).

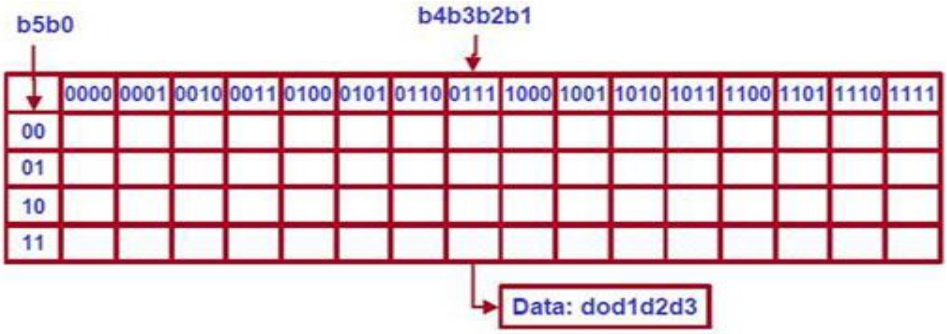

Figure 5. Bits Distribution of Each S-Box Block

S-Boxes represent only the non-linear part of (DES) so in brief we can explain the work of each S-box as shown in Figure 6.

Figure 6. S-Box Representation

And the expression of each box as follows:

S = matrix 4x16, values from 0 to 15
• B (6 bit long) = b1b2b3b4b5b6
– b1b6 r = row of the matrix (2 bits: 0,1,2,3)
– b2b3b4b5 c = column of the matrix (4 bits:0,1,…15)
• C (4 bit long) = Binary representation of S(r, c)

Depending on the mechanism of formation and installation of each S-Box, it is possible to use the VHDL code to represent this process and then upload the resulting file to a physical digital circuit (FPGA) for implement S-Box part by hardware tools. This is to achieve high speed, low cost and more secure in implementing this part. The start of the VHDL code shown below which represents the components of the S1-Box and so on for the other boxes

```
-- Design VHDL Code of S-box library IEEE;
use IEEE.std_logic_1164.all;
use IEEE.std_logic_arith.all;
entity S_box is
port ( In48 : in std_logic_vector(47 downto 0); Out32: out std_logic_vector(31 downto 0) );
end S_box;
architecture concurrent of S_box is
subtype data is std_logic_vector(3 downto 0); type Sbox_type is array (0 to 3,0 to 15) of data;
constant Sbox1 : Sbox_type := Sbox_type '(
("1110","0100","1101","0001","0010","1111","1011","1000",
"0011","1010","0110","1100","0101","1001","0000","0111"),
("0000","1111","0111","0100","1110","0010","1101","0001",
"1010","0110","1100","1011","1001","0101","0011","1000"),
("0100","0001","1110","1000","1101","0110","0010","1011",
"1111","1100","1001","0111","0011","1010","0101","0000"),
("1111","1100","1000","0010","0100","1001","0001","0111",
"0101","1011","0011","1110","1010", "0000", "0110", "1101"));
("1111","1100","1000","0010","0100","1001","0001","0111",
"0101","1011","0011","1110","1010","0000","0110","1101"));
```

5. TESTS AND RESULTS

Executing VHDL code and uploading it to the FPGA circuit will generate an integrated circuit inside the FPGA to implement each part of S-Box. The schematic diagram circuit of one cell S-box as shown in Fig. 7. The cell components consist of ROM, multiplexer (MUX) and input summing circuit.

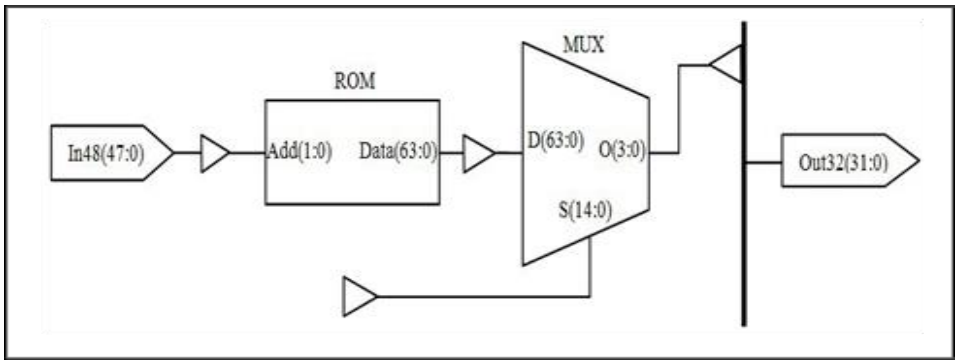

Figure 7. Schematic Diagram of One Cell of S-Box Circuit

The function from one look of S-box is clear shown in Figure 8 so that the input has 48-bit and output of 32 bit; this is one of the jobs of S-box. In fact, the process of writing and executing the proposed VHDL code for S-

boxes leads to generate of a file called bit stream. Downloading this file to FPGA circuit, leads to production of a digital electronic circuit, which represents the equivalent hardware design of the S-boxes, as shown in the Figure 8.

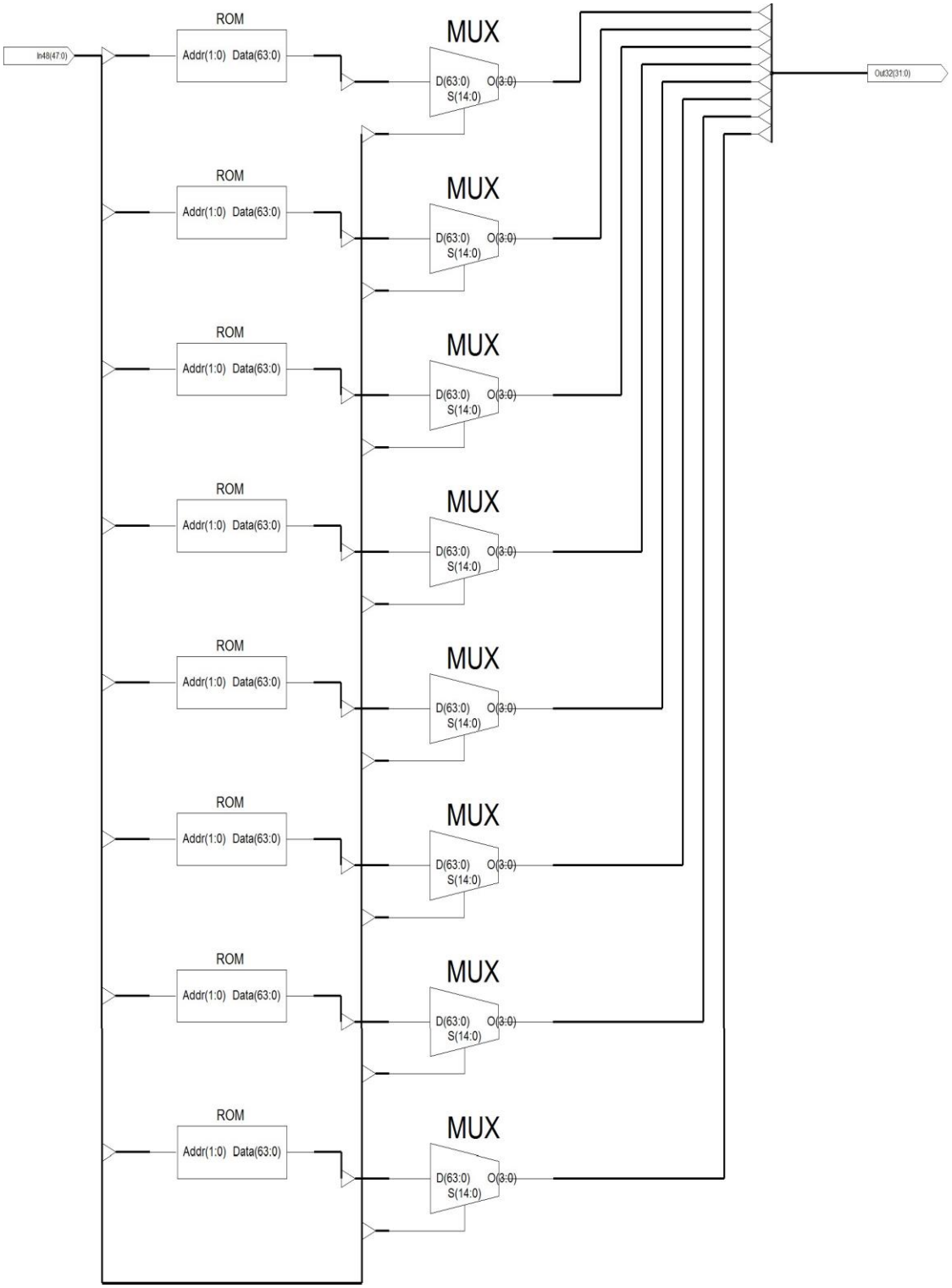

Figure 7. Block Diagram of the function of S-Box

The overall components of schematic circuit of S-box consists of 8 ROM, 8 MUX and 8-input summing circuit, this is shown of Figure 9.

Figure 9. Schematic Diagram of All S-Box Circuit After Execute VHDL Code

Each ROM have 2 input addresses bit and 64 data bit as shown in Figure 10.

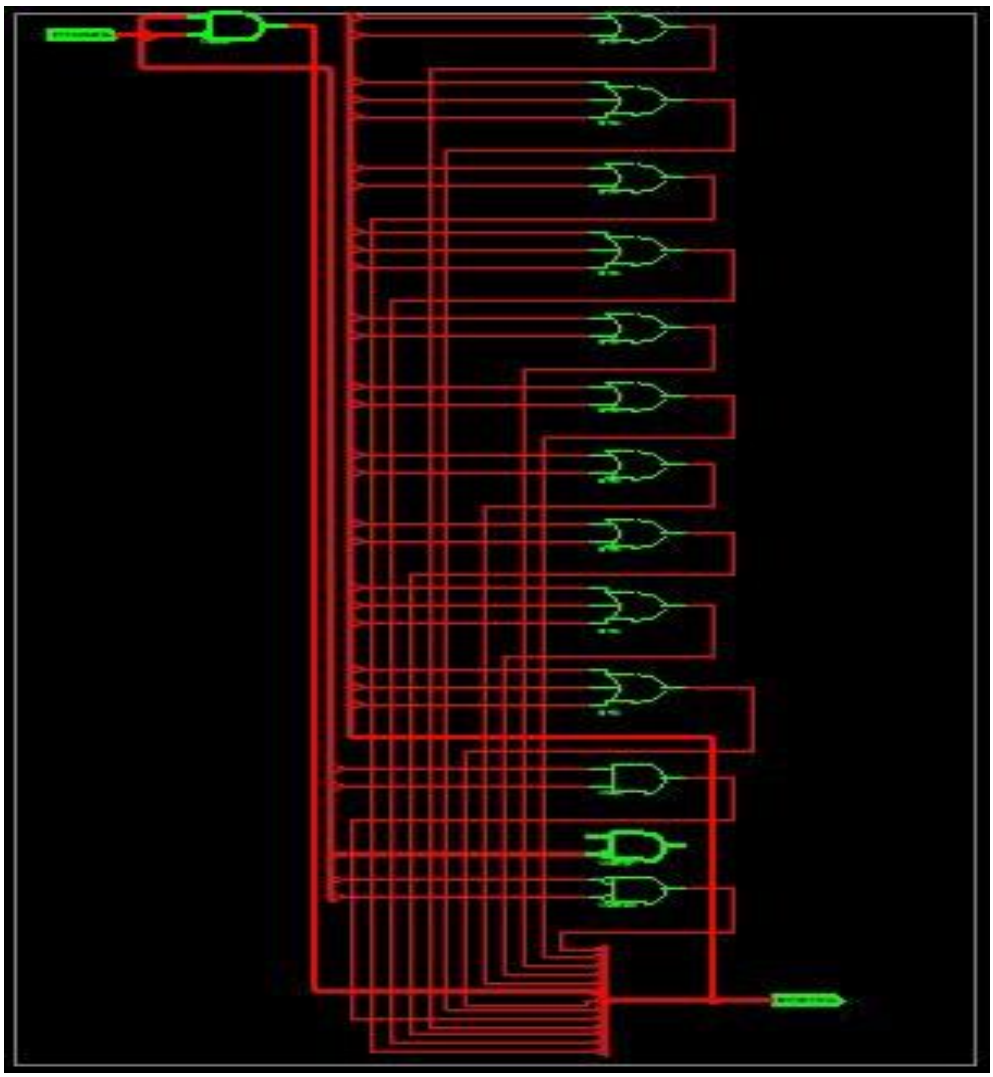

Figure 10. Components of Each ROM in S-Box

The output of each ROM connected to input of MUX which output 4-bit of each MUX then summing the output of all eight MUXs result 32 bit as the final outputs of S-box. Figure 11 represent the schematic diagram MUXs circuits.

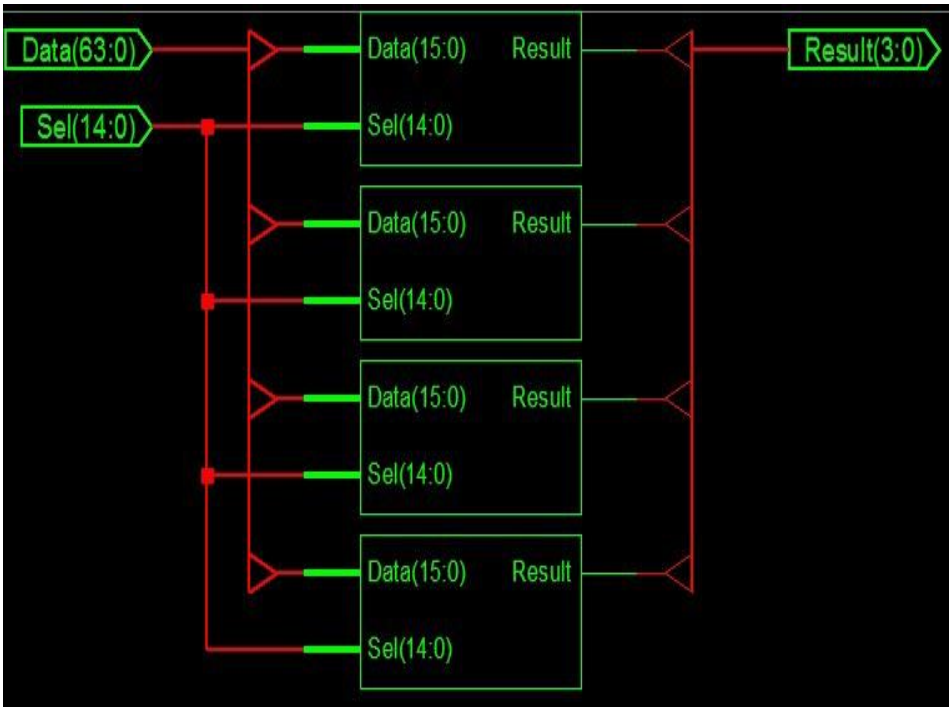

Figure 11. Schematic Diagram of Each MUX of S-Box

6. CONCLUSION

Another method provided by the proposed S-Box design is to implement devices other than a composite field to represent sub- byte transformation. As a result, the proposed design reduces as much as possible the hardware by avoiding the use of inverse multiplication in the Galois field. Compared with the Composite Field and the LUT, the S-Box results in a smaller area with an average or acceptable delay. An improved and compliable VHDL code is developed to implement the S-box part of DES process. Therefore, the design of the S-box can be implemented with an acceptable efficiency.

REFERENCES

[1] A. A. Yazdeen, S. R. M. Zeebaree, M. A. M. Sadeeq, S. F. Kak,. O. M. Ahmed, and R. R Zebari,''FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review," Qubahan Academic Journal, vol. 1, no. 2, pp. 8-16, March 2021.

[2] K. Lata, "An Approach Towards Resisting Side-Channel Attacks for Secured Testing of Advanced Encryption Algorithm (AES) Cryptochip," Third Conference on Security and Privacy (ISEA-ISAP), pp. 155-16, 2020.

[3] R. Sh. Jenny, and R. Sudhakar ,M. Karthikpriya, "Design of Compact S Box for Resource Constrained Applications" Journal of Physics: Conference Series, ICDIIS 2020, 1767 (2021) 012059, doi:10.1088/1742- 6596/1767/1/012059

[4] M. Syahrizal, M. Murdani, S. D. Nasution, M. Mesran, R. Rahim, and A. P. U. Siahaan, "Modified Playfair Cipher Using Random Key Linear Congruent Method," J. Online Jar. COT POLIPD, vol. 10, no. 2, pp. 45–49, 2017.

[5] A. Singh, M. Marwaha, B. Singh, and S. Singh, "Comparative Study of DES, 3DES, AES and RSA," Internation Journal Computer Technology, vol. 9, no. 3, pp. 1162–1170, Dec. 2010.

[6] T. K. Sivakumar, Dr. T. Sheela, Dr. R. Kumar, and Dr. K. Ganesan, "Enhanced Secure Data Encryption Standard (ES-DES) Algorithm Using Extended Substitution Box (S-Box)", International Journal of Applied Engineering Research, vol. 12, no. 21 , pp.11365-11373, 2017.

[7] F. Noorbasha, Y. Divya, M. Poojitha, K. Navya, A. Bhavishya, K. K. Rao, and K H. Kishore, "FPGA Design and Implementation of Modified AES Based Encryption and Decryption Algorithm," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 65, pp. 132-136, April 2019.

[8] S. R. M. Zeebaree, A. B. Sallow, B. K. Hussan, and S. M. Ali, "Design and Simulation of High-Speed Parallel/Sequential Simplified DES Code Breaking Based on FPGA," International Conference on Advanced Science and Engineering (ICOASE), IEEE Xplore, pp. 76-81, 2019.

[9] S. R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, no. 2, pp. 774-781 May 2020.

[10] Ch. Savalam, and P. Korapati, "Implementation and Design of AES S-Box on FPGA," International Journal of Research in Engineering and Science (IJRES), vol. 3, no. 1, pp. 1-6, Jan. 2015.

[11] A. Kumar, and S. Tejani, "S-BOX Architecture" In book: Futuristic Trends in Network and Communication Technologies, pp. 17-27, Publisher: Springer January 2019.

[12] K. Kazlauskas, R. Smaliukas, and G. Vaicekauskas, "A Novel Method to Design S-Boxes Based on Key Dependent Permutation Schemes and its Quality Analysis," International Journal of Advanced Computer Science and Applications, vol. 7, no. 4, pp. 93-99, 2016.

[13] C. Liua, J. Jia, and Zi. Liua, "Implementation of DES Encryption Arithmetic based on FPGA," Science Direct, AASRI Conference on Parallel and Distributed Computing Systems, AASRI Procedia 5 (2013), pp. 209 – 213.

[14] ANSI, "Triple Data Encryption Algorithm Modes of Operation," American National Standards Institute X9.52-1998, American Bankers association, Washington DC, July 29, 1998.

[15] FIPS, "Data Encryption Standard," Federal Information Processing Standards Publication 46-3, October 1999.

[16] G. Singh, and Supriya, "Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications, vol. 67, no. 19, pp. 33-38, 2013.

[17] H. D. Tsague, F. V. Nelwamondo, and N. Msimang "An Advanced Mutual-authentication Algorithm Using 3DES for Smart Card Systems," Second International Conference on Cloud and Green Computing. IEEE Computer Society, pp. 660-666 2012:,

[18] R. Zhang, "Analysis and Comparison on DES and 3-DES Algorithms," Information Engineering Research Institute, USA. Proceedings of 2012 2nd International Conference on Advanced Materials and Information Technology Processing AMITP 2012, vol.34.

[19] V. Tasril, M. B. Ginting, Mardiana, and A. P. U. Siahaan, "Threats of Computer System and its Prevention," Int. J. Sci. Res. Sci. Technol., vol. 3, no. 6, pp. 448–451, 2017.

[20] W. Fitriani, R. Rahim, B. Oktaviana, and A. P. U. Siahaan, "Vernam Encypted Text in End of File Hiding Steganography Technique," Int. J. Recent Trends Eng. Res., vol. 3, no. 7, pp. 214–219, Jul. 2017.

[21] F. H. Khan, R. Shams, A. Hasan, and N. Hasan, " Implementation of Data Encryption Standard (DES) on FPGA," Journal of Computer Science of Newports Institute of Communications and Economics vol. 5, Issue- 2014, pp. 47-59..

[22] S. Q. Mohammed, "Implementation of Simplified Data Encryption Standard on FPGA using VHDL," Kurdistan Journal of Applied Research (KJAR), vol. 7, no. 1, pp. 9- 20, - June 2022.

[23] I. Grout, "Digital systems design with FPGAs and CPLDs" book : 1st Edition - March 26, 2008.

[24] B. Mealy, and F. Tappero "Free Range VHDL," Book : 21 June 2013 : http://www.freerangefactory.org

BIOGRAPHIES OF AUTHORS

Jabbar Shatti Jahlool was born in Iraq in 1964. He received the B.Sc. and M.Sc. degree in Electrical Engineering from University of Technology, Baghdad, Iraq, in 1988 and 2001 respectively. From 2001 to 2014, he was electronic hardware designer, director of the technology transfer and scientific research in the Ministry of Industry. Since 2015 he has been a university lecturer with Department of Computer Techniques Engineering, Dijlah University College, Baghdad, Iraq. His research interests include hardware electrical and electronic circuits design, FPGA design, microcontroller's research and design project, power system analysis and control, and power electronics circuits. He can be contacted at email: jabbar.shatti@duc.edu.iq.

r. Nazar Jabbar Hussain, Received His Msc. degree in the in Electronic Engineering from University of Technology Baghdad – Iraq in 2005 and Doctor of philosophy in video encryption and compression from University of Buckingham UK -2016. He has been a full-time lecturer in computer engineering techniques Department/ Dijlah University College, Baghdad, Iraq, since December 2018. He also worked as senior researcher in the Iraqi Center of Development and Research since 1994., Currently, he has a head of computer engineering techniques Department/ Dijlah University College/ Baghdad/ Iraq since 2017. It can be contacted at email: nazar.jabar@duc.edu.iq.

Ali M. Kadhim, Received His Higher Diploma degree in the computing science from University of East Anglia / England – UK in 1990 and MSc in computer science from University of Technology –Baghdad Iraq - 1992. He has been a full-time lecturer and head of computer science and engineering technique departments in Al_Salam College university, Baghdad, Iraq ,for 10 years since Nov. 2003. Currently, he is a full-time lecturer in computer engineering techniques Department/ Dijlah University College/ Baghdad/ Iraq since 2013, ongoing He can be contacted at email: ali.alsalihy@duc.edu.iq.

الخلاصة

في الوقت الحاضر، يعد تنفيذ نظام تشفير يعتمد على الوسائل التقليدية موضوعًا متأخرًا بسبب تطور وتعدد طرق الكشف والاختراق والقرصنة. لذلك، من الضروري اللجوء إلى طرق أكثر حداثة، مثل استخدام الدوائر الإلكترونية الرقمية المبرمجة مثل مصفوفات البوابات القابلة للبرمجة ميدانيًا (FPGAs).الهدف من هذه الورقة هو تصميم صندوق الاستبدال (S-Box) لمعيار تشفير البيانات (DES) باستخدام لغة وصف الأجهزة عالية السرعة (VHDL).ونتيجة لذلك، تم تصميم وكتابة كود S-box VHDL ثم باستخدام إمكانياتXilinx Design Suite ISE ، تم فحص التصميم وتحليله ومحاكاته ثم سيتم إنشاء ملف يسمى تدفق البتات. تم تنزيل الملف الناتج إلى دائرة FPGA وتم الحصول على الدائرة الرقمية الفيزيائية المكافئة التي تمثل S-box.