

Secured Substitution Box of Advance Encryption Standards (AES) With Permutation

¹ C. PADMINI, ² JVR RAVINDRA

^{1, 2} Department of Electronics and Communication Engineering,

¹Jawaharlal Nehru Technological University, Hyderabad

²Vardhaman College of Engineering, Shamshabad, Hyderabad

ABSTRACT :Electronic gadgets such as mobile phones, laptops, IPad, home appliances and other gaming gadgets have become a part and parcel of our life and they have made the human life most comfortable. With the shirking of technology the gadgets have become handy and security of the devices is taken care by the field of cryptography. Cryptography plays a vital role in acquiring the software security of data. One of the best Cryptographic algorithm secured the data is Advanced Encryption Standard (AES) which is a combination of various steps involved by which the data was made secured. One of the major action involved in making the encryption is by Substitution of data with the help of Substitution box called as S Box. In this paper to improve the attack immunity a Sub Byte transformation called as S Box of AES is implemented with permutation applied at any independent steps of S Box. The attack immunity depends on number of iterations involved in cracking the Cryptosystem. The permutation incorporated will be known only to source and destination people for recovery and the possibility of attack gets reduced. The proposal is implemented and results are verified in Xilinx software 45nm technology. The design is also verified with respect to normal S- Box and the number of iterations are also verified.

KEY WORDS :: Cryptography, Advanced Encryption Algorithm, Substitution Box, Permutation, AES, S- Box; Cryptographic system.

Date of Submission: 09-06-2021

Date of acceptance: 23-06-2021

I. INTRODUCTION

In this era, life without electronic gadgets is like an incomplete one. World around is completely filled with different type of electronic gadgets. They could be in the form of mobile phones for various applications, RFID tags for authentication or IOT based network for controlling and communicating so on and so fore. All the gadgets are used by each and every person and for many of the devices security plays a vital role. It might be a security of mobile phone or RFID authentication, security plays an important role. The gadgets are made secured by securing the data in it. The data that gets processed while doing any transactions or communication might be hacked and this leads to threat for the device and data. To reduce this type of attacks data are made secured with the help of various cryptographic algorithms such as Rivert Shamir and Adleman (RSA) algorithm, Data Encryption Standard (DES), Triple DES (TDES) and final landed with Advance Encryption Standard (AES)[1]. This paper concentrated on improvisation of AES algorithm by replacing the regular Substitution Box[2] (S Box) with an improvised S Box which is implemented by introducing the permutation in S Box by which the number of iterations needed for cracking of AES[3] algorithm increases thereby minimizing the possibility of software and hardware [5] attack. The paper is organized in this manner as Section I Presents Introduction, section II gives the existing AES algorithm steps and S Box implementation. Section III presents the proposed S Box with Permutation and section IV gives the result obtained for the proposed technique and section V presents the conclusion and future scope followed by references

II. ADVANCE ENCRYPTION STANDARD (AES):

The security system for the electronic gadgets is taken care by cryptographic algorithms such as AES. AES is implemented with the help of four main steps such as Sub Bytes transformation, Shift Rows transformation, Mix Columns transformation, and Add Round Key transformation as shown in fig.1 in which the Sub Byte transformation is done by an important block called S Box as shown in Fig.2. S Box implies a Substitution Box which will provided the code data for for substitution in the encryption process of AES and at the decryption the reversal happens and the original data is retrieved. This way the data is made secured using the AES algorithm.

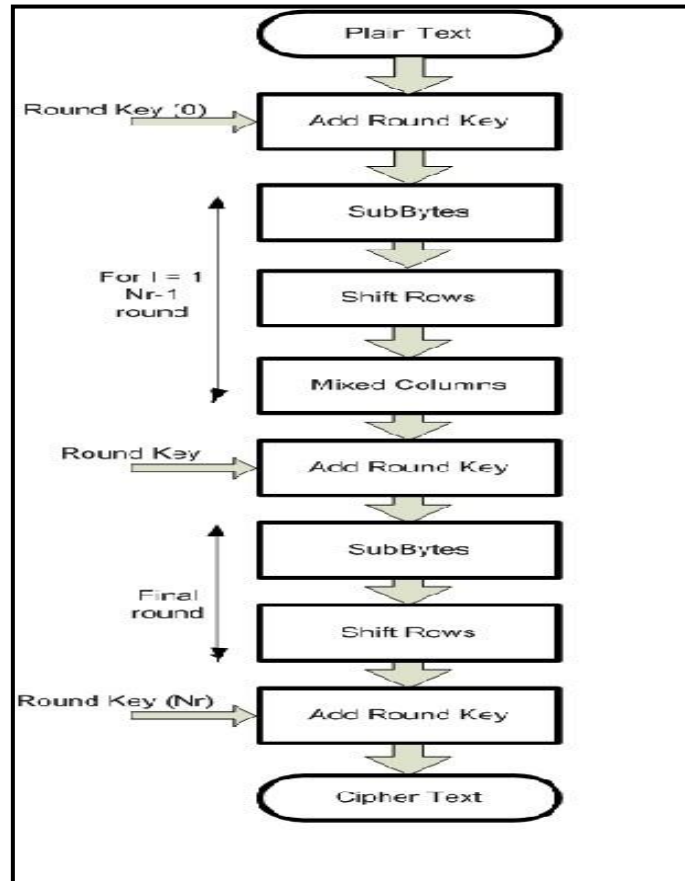


Fig. 1 AES implementation

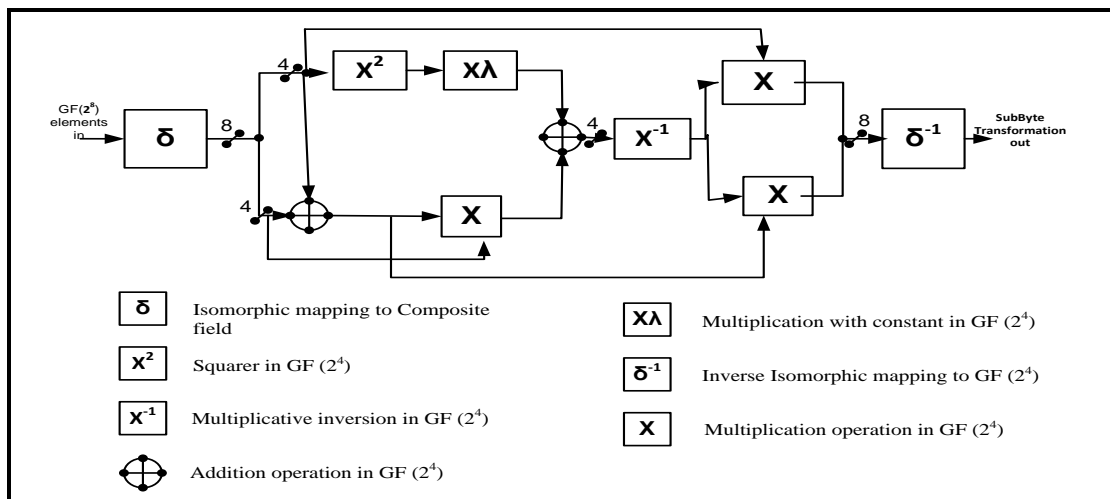


Fig. 2 Sub Byte transformation called S Box Implementation

3. S Box Implementation With Permutation

The proposed S Box is implemented and verified by writing Verilog Code using Xilinx tool as shown in Fig.3. The code of S Box Delta operation is shown in Fig.3 and the other S Box modules are seen. Fig. 4 gives the main Module of S Box implementation. The Screenshot shown in Fig.5 presents power summary in Xilinx Power Analyzer. The main purpose of implementing the proposed logic in Xilinx using Verilog code is to easily incorporate the Permutation and verify the impact of permutation on Power. In this paper the Power Analysis for different permutations applied is observed and is discussed in results.

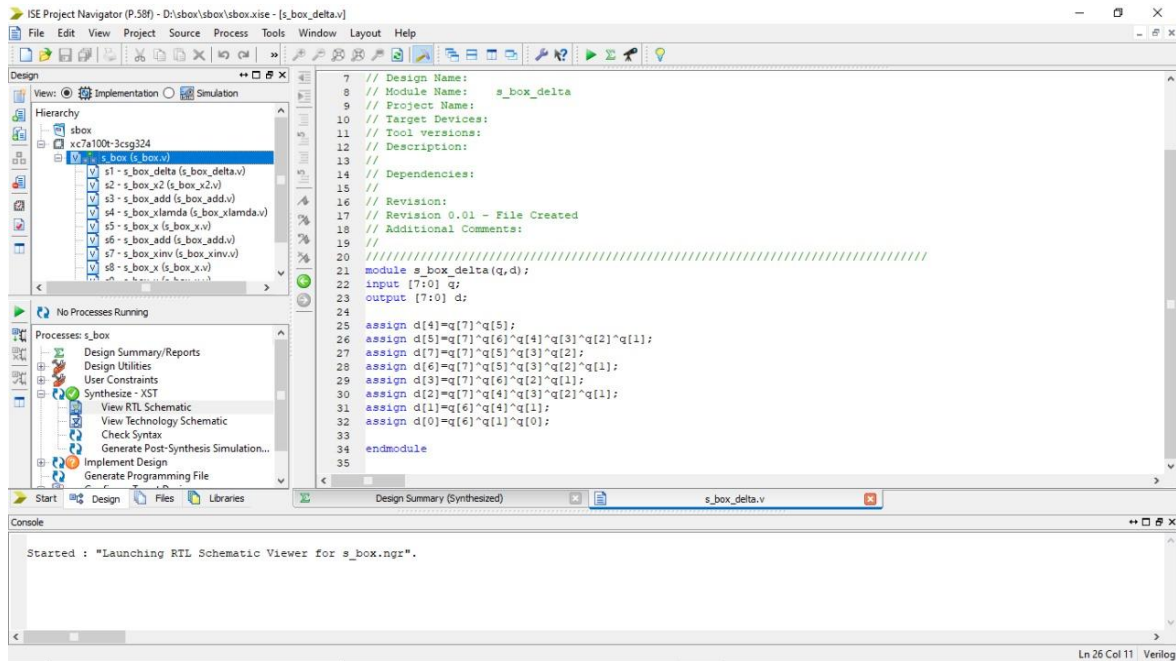


Fig. 3 S Box Delta implemented using Xilinx tool.

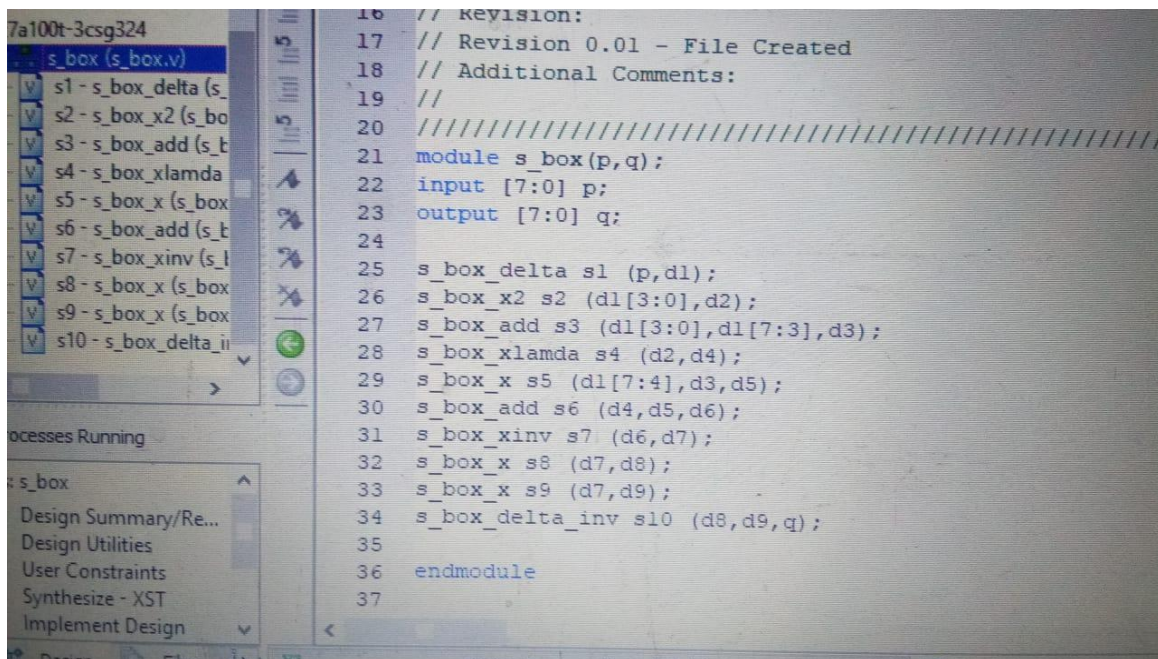


Fig. 4 S Box implemented by Verilog HDL using Xilinx tool

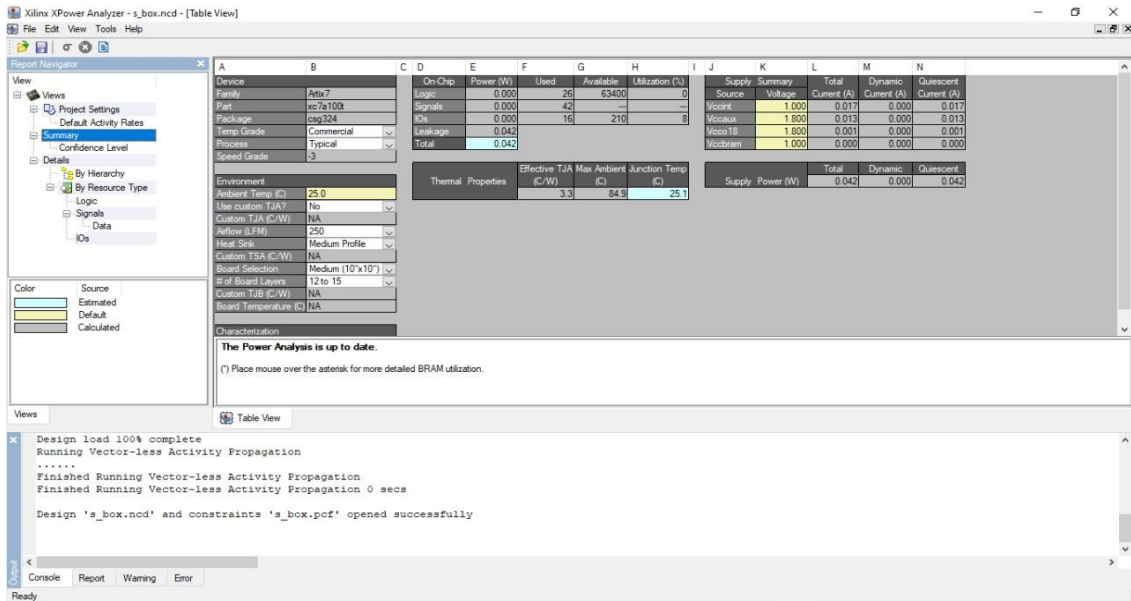


Fig. 5 Screenshot presenting power Summary using Xilinx Power Analyzer

The test sample of data is applied to the S Box is as shown in Fig.6 and the data just before the final transformation the Permutations is applied as shown in Fig.6 with a red color tick mark are as shown in Table .1 and the power results are given in results.

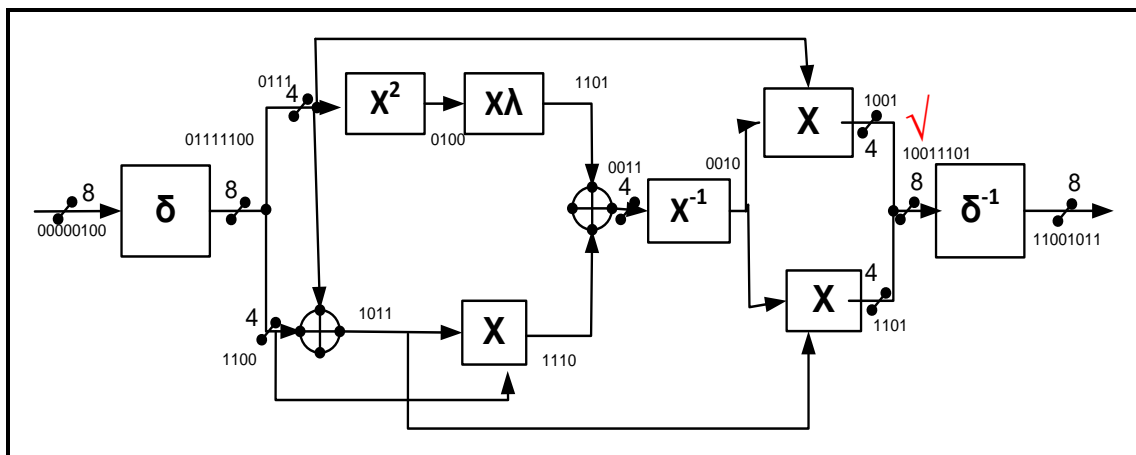


Fig.6 S Box applied with sample input combination

S. No.	Data bits positioned as below							
1.	D0	D1	D2	D3	D4	D5	D6	D7
2.	D1	D0	D3	D2	D5	D4	D7	D6
3.	D4	D5	D6	D7	D0	D1	D2	D3
4.	D7	D6	D5	D4	D0	D1	D2	D3
5.	D4	D5	D6	D7	D3	D2	D1	D0
6.	D5	D4	D6	D7	D3	D2	D1	D0
7.	D7	D6	D5	D4	D3	D2	D1	D0
8.	D4	D5	D7	D6	D3	D2	D1	D0

Table.1 Permutations applied in S Box

Table.1 Permutations applied in S Box	D0	D1	D2	D3	D4	D5	D6	D7	4.951
1.	D1	D0	D3	D2	D5	D4	D7	D6	4.550
2.	D4	D5	D6	D7	D0	D1	D2	D3	4.393
3.	D7	D6	D5	D4	D0	D1	D2	D3	4.482
4.	D4	D5	D6	D7	D3	D2	D1	D0	4.027
5.	D5	D4	D6	D7	D3	D2	D1	D0	4.035
6.	D7	D6	D5	D4	D3	D2	D1	D0	4.101
7.	D4	D5	D7	D6	D3	D2	D1	D0	4.030

Table.2 Power consumption by permuted data in (mW)

III. RESULTS

By applying Permutation in S Box the number of iterations needed for software hackers will get V double for every bit variation in the position of the hacker The respective permutations samples are also tabulated in Table.2 which states that the power consumption is almost a constant without much variation, so it implies that the proposed S Box is secured against the DPA attack as well..



IV. CONCLUSION

The proposed S Box implementation and the obtained results conclude that the S Box with Permutation is now only simple in construction as conventional S Box and also secured compared to conventional S Box implementation. The Proposed S Box need more number of iterations needed to crack by the hackers. For every one bit of permutation causes double the number of iterations needed. The Table.2 concludes that the deviation in power level for different permutation is almost same so the system can be made more secured by implementing with Ultra Low Power technique. The proposed technique is not only simple in construction and also most secured for practical implementation.

REFERENCES:

- [1]. Federal Information Processing Standards Publication 197, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", November 26, 2001.
- [2]. A. Joshi, P. K. Dakhole and A. Thatere, "Implementation of S-Box for Advanced Encryption Standard," 2015 IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, 2015, pp. 1-5.
- [3]. O. B. Sahoo, D. K. Kole and H. Rahaman, "An Optimized S-Box for Advanced Encryption Standard (AES) Design," 2012 International Conference on Advances in Computing and Communications, Cochin, Kerala, 2012, pp. 154-157.
- [4]. A. Levina, I. Kamnev and I. Zikratov, "Implementation White Box Cryptography in Substitution-Permutation network," 2020 9th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2020, pp. 1-3.
- [5]. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. "Power analysis attacks: revealing the secrets of smart cards" (2007). Google Scholar Digital Library, 2010.

AUTHORS PROFILE

	<p>Ms. Cheerla Padmini has done her Masters in Digital Systems at JNTUA, Ananthapur, Pursing Ph.D. at Jawaharlal Nehru Technological University, Hyderabad, working on a WOSA, DST project in Cryptanalysis at Vardhaman College of Engineering, Hyderabad. Other areas of interests are Cryptography, Ultra Low Power Adiabatic Circuits and Hardware Security.</p>
	<p>Dr. JVR Ravindra is Principal and Professor at Vardhaman College of Engineering, Hyderabad has done his PhD at IIIT-Hyderabad in 2007 and interested areas of research is Modeling of Ultra Low Power Interconnects, High Speed and Low Power Arithmetic Circuits, Low Power DSP architectures, Hardware Security and Wireless Sensor Networks</p>