IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 2, Ver. I (Mar.-Apr. 2017), PP 57-61
www.iosrjournals.org

FPGA Based Implementation of AES Encryption and Decryption with Low Power Multiplexer LUT Based S-Box

Ratheesh T[1], Seena Narayanan[2]
Assistant Professor, Dept. of ECE, College of Engineering Trikaripur, Kasaragod, Kerala,India [1]
PG scholar (M Tech in Power Systems and Power Electronics), LBS College of Engineering, Kasaragod, Kerala, India [2]

***Abstract**: Encryption is important to keep the confidentiality of data. There are many of encryption algorithms to ensure the data, but should be the select the algorithm depended on the fast, strong and implementation. For that choose the advance encryption standard (AES) algorithm for encryption data because speed and easy implementation on small devices and some the feature for it. In this paper, implementation of encryption and decryption of AES algorithm is presented with a High Secured Low Power Multiplexer Look-Up-Table (MLUT) based Substitution-Box (S-Box) . The main feature in the proposed MLUT based S-Box is that, it is implemented based on 256-byte to 1-byte multiplexer with a 256-byte memory instead of the conventional implementation of employing multiplication inversion in GF(2^8) and affine transformation. Thus, the proposed S-Box is simpler in circuit implementation and lower in power dissipation.*

***Index Terms:** AES, Multiplexer LUT, S-Box, FPGA.*

I. Introduction

Advanced Encryption Standard (AES) algorithms have been employed in a variety of security systems . It has been proven to be more effective to protect the secret information when compared to other reported encryption algorithms including the Data Encryption Standard (DES), Triple-DES (3DES) and Elliptic Curve Cryptography (ECC) [12]. The AES encryption process as depicted in Figure. 1 requires multiple rounds of iterations, each round consists of 4 arithmetic and logical operations namely Substitution Byte, Shift Row, Mix Column and Add Round Key except for the last round which does not have the Mix Column operation. Despite its highly secured features, AES is vulnerable against Side Channel Attack (SCA) which can reveal the secret information (secret key and plaintext) by correlating its intermediate data with the leakage physical parameters. The leakage physical parameters can be the power dissipation, electromagnetic radiation and timing information generated during the encryption process. There are three types of power analysis based SCAs, namely Simple Power Analysis (SPA), Differential Power Analysis (DPA), and Correlation Power Analysis (CPA). Among these 3 types of attacks, the CPA is the most effective attack to reveal the secret information [11],[12]. The CPA attack is the byte-based attack employing the statistical properties of power traces and the intermediate data to reveal the secrete key[1]. Substitution-Box (S-Box) is one of the main modules in the AES implementation. This module is a non-linear operation which makes AES highly secured in protecting the secret information. In another perspective, S-Box dissipates the most power and easily leak out the information of the processed intermediate data through CPA attack. The rest of the paper is described in four sections: Section II gives brief description of AES algorithm, Sections III describe the approach for implementing multiplexer LUT based S-box, Section VI summarizes the results of experiments and Finally, a conclusion is given in section V.

II. AES Algorithm

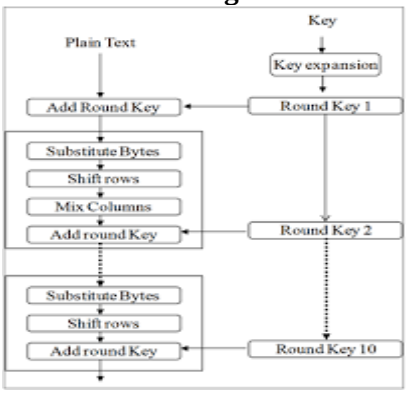

Fig.1 AES encryption process

The AES algorithm has a fixed block size of 128 bits and a key length of 128, 192 or 256 bits. It generates its key from an input key using the Key Expansion function. The AES operates on a 4x4 array of bytes which is called a state. The state undergoes 4 transformations which are namely the Add Round Key, SubByte, Shift Row and Mix Column transformation. SubByte transformation is a highly non-linear byte substitution where each byte in the state array is replaced with another from a lookup table called an S-Box. Shift Row transformation is done by cyclically shifting the rows in the array with different offsets. Finally, Mix Column transformation is a column mixing operation, where the bytes in the new column are a function of the 4 bytes of a column in the state array. Of all the transformation above, the SubByte transformation is the most computationally heavy.

The Encryption process of Advanced Encryption Standard algorithm is presented above, in Figure 1.This block diagram is generic for AES specifications. It consists of a number of different transformations applied consecutively over the data block bits, in a fixed number of iterations, called rounds. The number of rounds depends on the length of the key used for the encryption process.

A.SUB BYTE TRANSFORMATION

In this stage, each byte replace with another byte by using s-box. The s-box operation provides the non-linearity to encryption data. The figure.2 which illustrate substitution byte process .

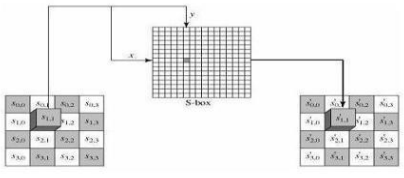

Fig.2. SubByte Transformation

B. SHIFT ROWS

In this stage, shift the row of data matrix to cyclically left shifts. The first row in data matrix is unchanged, the second row shift one byte to left, the third row shift two bytes to left and the fourth row shift three bytes to left as shown in figure.3.

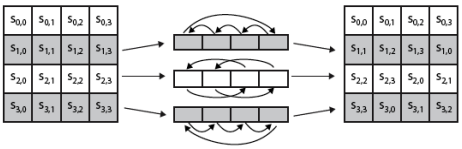

Fig.3. ShiftRows Operation

C. MIX COLUMNS

In this stage, transfers map of each column of input data matrix to a new column in output data matrix. Everyone input column considered as a polynomial vector above GF(2^8) and that multiplied with constant matrix. The multiplied operator used polynomial mathematical see the figure.4.

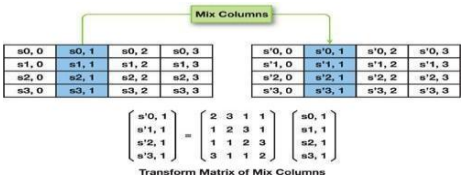

Fig. 4. Mix Column

D. ADD- ROUND KEY

Add Round Key step is applied one extra time comparing to the other encryption and decryption steps. This step is common among encryption and decryption. The first Add Round Key step is applied before starting the encryption and decryption iterations, where in the encryption process the first 128 bits of the input key the whole key in case of using key size of 128 bits are added to the original data block as shown in Fig 5. This round key is called the initial round key [4]. It is implemented in hardware as a simple exclusive-or operation of the 128 bit data and key as shown in fig.5.

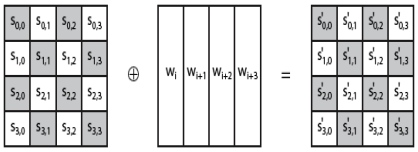

Fig.5. Add Round Key Operation

III. Ii. Implementation of Multiplexer LUT Based S-Box.

The input to the S-Box is an 8-bit data, *x*, which has 256 combinations of input values (28 =256). The output from the S-Box, *S*(*x*), for each possible input, *x*, can be pre-computed and stored in a Look-Up-Table (LUT). The corresponding output can then be retrieved directly from the LUT when a particular input arrives. In this context, a multiplexer can be used to select a corresponding output data from the LUT as depicted in Figure. 6(a). Hence, the *S*(*x*) can be generated faster (with only one multiplexer operation) and this operation dissipates lower power when compared to the conventional S-Box operation[1].

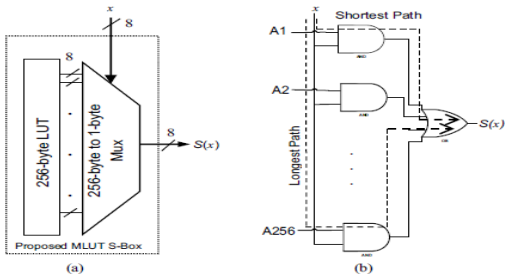

Fig.6. Multiplexer based S-Box (a) Proposed MLUT S-Box (b) Longest and Shortest Path delay

As depicted in Figure. 6(a), the proposed MLUT S-Box which consists of a 256-byte-to-1-byte multiplexer and a 256-byte LUT. The 256 stored values, *S*(*x*), in the LUT are based on the pre-computed values of S-Box operations for all possible 256 bytes of *x*. The longest and shortest path of the data of MLUT S-Box is depicted in Figure. 6(b). Although there is an interconnection delay difference in these paths, their power dissipation difference is small [1].

The dissipated power in MLUT S-Box is relatively low (when compared to the conventional S-Box) and highly uniform for different *x*, since only the selection of the corresponding *S*(*x*), from the LUT is performed. As depicted in Figure. 6(b), the data, *S*(*x*), selected from LUT passes through the AND gate and OR gate to the output, thus the power dissipation is low. However, the small differences of delay resulted from different paths of the data in multiplexer operation generates a marginal small power dissipation variation for different *x*. Hence, the power dissipation of our proposed MLUT S-Box has a smaller correlation with the processed data when compared to the conventional S-Box and thus it is highly secured against SCA[11].

IV. Result And Discussions

This section present the test environment and the experimental results of design modules. The design is done using Verilog code and simulated using ModelSim, Synthesizing & Implementing (i.e. Translate, Map & Place and Route) the code on Xilinx - Project Navigator, ISE 7i and finally implemented on Sparton-6 FPGA kit.

A. SIMULATION RESULT OF MULTIPLEXER-LUT BASED S-BOX

Simulation result of multiplexer-LUT based S-Box is shown in the below fig.7.

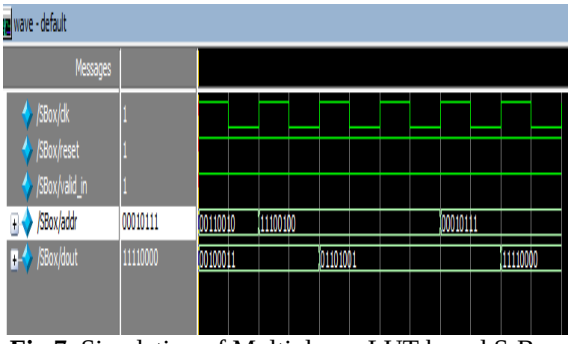

Fig.7. Simulation of Multiplexer-LUT based S-Box

B. SIMULATION OF ENCRYPTION

In AES Encryption 128 bit plain text and 128 bit encryption key are given as an inputs, and getting 128 bit cipher text as output (Table I.). The simulation waveform is shown in fig.8.

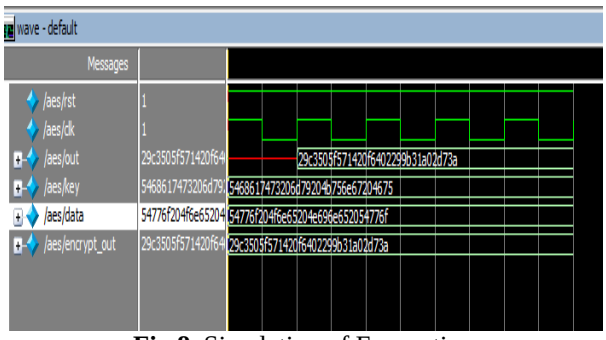

Fig.8. Simulation of Encryption

Plain Text	54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F
Secret Key	54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Cipher Text	29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D73A

Table. I. AES Encryption Plain text, Key and Cipher text

C. SIMULATION OF DECRYPTION

In AES Decryption 128 bit cipher text and 128 bitd secret key are given as inputs, and getting 128 bit plain text as an output. The simulation waveform is shown in fig.9.

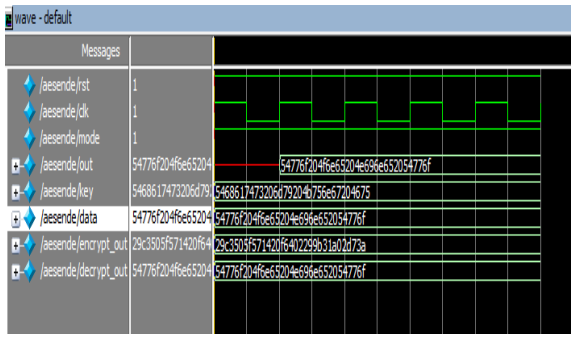

Fig.9. Simulation of Decryption

Cipher Text	29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D73A
Secret Key	54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
Plain Text	54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

Table.II. AES Decryption Cipher text, Key and Plain text

D. POWER ANALYSIS

Based on power analysis conducted using Xilink XPower Analyzer as shown in figure.10, the total power distribution of Multiplexer LUT based S-Box is only 0.55W and is nearly three times lower than Conventional S-Box. In addition, the power dissipation for different processed data is highly uniform for different input data, since only the selection of the corresponding output from the LUT is performed. The data selected from LUT passes through the AND gate and OR gate to the output, thus the power dissipation is low. However, the small differences of delay resulted from different paths of the data in multiplexer operation generates a marginal small power dissipation variation for different *x*. Hence, the power dissipation of the proposed MLUT S-Box has a smaller correlation with the processed data when compared to the conventional S-Box and thus it is highly secured against Side Channel Attack.

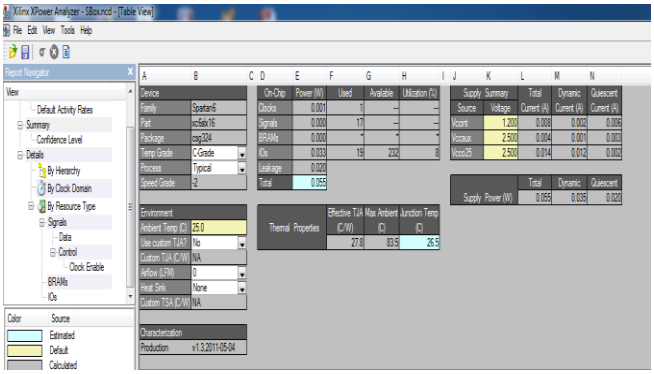

Fig.10. Power Distribution Analysis

V. Conclusion

The Advanced Encryption Standard algorithm is a symmetric block cipher that can process data blocks of 128 bits through the use of cipher keys with lengths of 128 bits. AES algorithm can resist any kinds of password attacks with a strong practicability in information security and reliability. AES provides better security and has less implementation complexity, it has emerged as one of the strongest and most efficient algorithms in existence today. Here we used a multiplexer LUT based S-Box for AES-128 implementation to reduce the power dissipation and to increase the resistance against side channel attacks. The MLUT S-Box design requires only one 256-byte-to-1-byte multiplexer and one 256-byte of LUT memory based on AES-128 implementation. The measurement results obtained from the experiment have shown that the power dissipation of the AES-128 based MLUT S-Box is significantly reduced. In addition, the power dissipation for different processed data is highly uniform which resulted in lower variance. So the proposed MLUT S-Box is more secured than the conventional methods.

Acknowledgment

The authors would like to express special thanks to teachers for providing an excellent guidance and motivation for the project work, parents and friends who helped a lot for finalizing the review work. Above all sincere thanks to god who is the power of strength in each step of progress towards its successful completion.

References

[1]. Ali Akbar Pammu, Kwen –Siong Chong, Kyaw Zwa Lwin Ne and Bah- Hwee Ghee, "High Secured Low Power Multiplexer-LUT Based AES S-Box Implementation",International Conference on Information Systems Engineering 2016.
[2]. Chandrasekhar Savalam1 & Prasanti Korapati, Assistant professor, ECE Dept., DIET College & Assistant professor, EIE Dept., VRSEC College "Implementation and Design of AES S-Box on FPGA" , IJRES, JAN-2015.
[3]. Gireesh Kumar .P and Mahesh Kumar, "Implementation of AES algorithm using Verilog", International Journal of VLSI and Embedded Systems-IJVES, Vol 04,June 2013.
[4]. Mahesh Walunjkar, Md. Manan Mujahid, Syed Anwar Ahmed, Ashish Jadhav ,"An AES-Core Development by Using Verilog" , IJIRCCE, Vol 04, June 2013.
[5]. Ahmed Tariq Sadiq, "Modification of AES algorithm based on Extended Key and Plain Text", Journal of Advanced Computer Science and Technology Research, Vol 5, 2015.
[6]. Saurabh Kumar,V.K. Sharma and K.K. Mahapatra, Department of Electronics and Communication Engineering, National Institute of Technology Rourkela, "An Improved VLSI Architecture of S-box for AES Encryption", International Conference of Communication Systems and Network Technologies, 2013.
[7]. Richa kumari sharma, S.R.Biradar,B.P.Singh**,** MITS University Lakshmangarh , "Shared Architecture for Encryption/Decryption of AES", International Journal of Computer Applications, Vol 69, May 2013.
[8]. Y.Aruna, Prof., Bharati Masram, JDCOE, RTM Nagpur University, "FPGA Based Implementation of AES Encryption and Decryption with Verilog HDL", IJERA, ICIAC-April-2014.
[9]. William Stallings, "Cryptography and Network Security", Chapter 5 , Fifth Edition.
[10]. Raj Jain, Washington University in Saint Louis, "Advanced Encryption Standard", CSE 571S, 2014.
[11]. Kevin Meritt , "Power Analysis Attacks on AES",Cryptography 2, VCSG 706, May 2016.
[12]. S. Mangard, E. Oswald, and T. Popp, , "Power Analysis Attacks", US : Springer 2010.