International Journal of MC Square Scientific Research Vol.9, No.3,2017

VLSI Architecture Based Advanced Encryption Standard (AES) With Optimized Inverse Mix-Column and X-Time Multiplication Process

Azath mubarakali
Assistant professor, department of computer Networks and communication Engineering, college of computer Science, king Khalid university, Saudi Arabia
aabdurrahman @kku.edu.sa

Abstract

Rijndael is the security based methodology used to protect the information from the attackers. Rijndael algorithms perform with the data encryptions and data decryptions. Data Encryption is transform the plain text into the cipher text and the data decryption is recovering the original data. Mix-column and Inverse Mix-column is one of the difficult operations in the Rijndael algorithm. In this paper, Optimized Inverse Mix-Column transformation has been designed with the help of Xtime multiplication process. Xtime multiplication performs the multiplication function for ‘m X m’ data; results will be m-bit data. Further the complexity of Xtime multiplication process has been identified and re-designed with the help of effective CSE techniques. Developed Reduced Xtime based optimized Inverse Mix-Column transformation provide better performances than traditional Xtime based Inverse Mix-Column multiplication. The proposed mix column and X-time multiplication design is implemented in terms of the VLSI Design Environment.

Keywords: Advanced Encryption Standard, Mix-column, Xtime Multiplication, Very Large Scale Integration.

Issn No:0975-0932

1. Introduction

Data security is one of the key features in any communication system. The security providing to the system is done by using some software. It was developed by using algorithm. In previous days Data Encryption Standard (DES) is the algorithm to provide security. DES algorithm provides security but it has some drawback to give full security to the system. DES process only 64-bit at a time. It cannot process large number of within a single time. To overcome the drawback by introduce a new algorithm named as Rijndael algorithm. It overcomes the drawback of DES algorithm. Because it has large number of steps to provide the security to the system. Finally, try to eliminate correlation between the secret keys and the power consumption. The multiplicative masking method is realized by using either standard CMOS cell (which has to be verified as glitch free and DPA resistant but it requires a partial automatic design low) or the RTL level (which has to be proved as insecure in terms of glitch attacks). Boolean masking is characterized at the algorithmic level and is immune to DPA and glitch attacks. Boolean masking had an benefit, it is simple to implement. It does not require further resources. Boolean Masking is a fine applicant to apply AES in Storage Area Networks.

2. Related Works

[1] presented VLSI architecture based Rijndael Algorithm. In this paper Rijndael methodology for Advanced Encryption Standard is written using HDL language.. It shows that, encryption and decryption is done with more security and consumes less time to provide encrypted and decrypted codeword's. The AES presented in this paper, performs the plain text into cipher text and cipher text plain text conversion decryption very well across a variety platform, including 8-bit and 64-bit resulting in very food software performance.

Issn No:0975-0932

[2] presented a method for encryption and decryption. In this paper, the data authentication goals were enhanced well and which achieves the data security on the communication channels by assembly it intricate for attacker to predicate a pattern as well as rate of the encryption/decryption scheme. The proposed method has been verified against several predefined attacks and proved to be authenticating against them. Therefore, it can be consider as an efficient method to some applications because of the high authentication and less computation time to encrypt and decrypt a data using a proposed methodology is much smaller than AES algorithm.

[3] presented a symmetric key based encryption and decryption algorithm. It was used to estimate the requirement of Symmetric Key Cryptography for Security in Distributed Systems. There are two different methods used for the efficient encryption and decryption. These two different methodologies were performed on the parameters such as key size, block size, number of iterations.

[4] described the parallel AES Encryption engines for many-core processor arrays. By exploring different granularities of data-level and task-level parallelism, they mapped 16 implementations of an Advanced Encryption Standard (AES) cipher with both online and offline key expansion on a fine-grained many-core system. The smallest design utilizes only six cores for offline key expansion and eight cores for online key expansion, while the largest requires 107 and 137 cores, respectively. In comparison with AES cipher implementations on general purpose processors, their design has 3.5-15.6 times higher throughput per unit of chip area and 8.2-18.1 times higher energy efficiency.

[5] presented FPGA implementations of Advanced Encryption Standard. It based on the Rijndael Algorithm is an efficient cryptographic technique that involves generation of ciphers for encryption and inverse ciphers for decryption. Higher speed and security of encryption/decryption is ensured by operations like SubBytes, Inv SubBytes, MixColumns/Inv

Issn No:0975-0932

MixColumns and Key Scheduling. Extensive research has been conducted into the development of S-box /Inv. S-Box and MixColumns/Inv. MixColumns on dedicated FPGA and ASIC to speed up the AES algorithm and to reduce circuit area. This is an attempt, to survey in detail, the work conducted in the fields. The main focus is on the FPGA implementations of optimized novel hardware architectures and algorithms.

[6] presented Implementation of Rijndael Encryption in Reconfigurable Hardware. Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Design and Improvements Tradeoffs. It addressed various methods for efficient FPGA implementations of the Advanced Encryption Standard algorithm. The implementation of block ciphers, several categories can produce effective designs. Inherent constraints of FPGAs were taken into account in order to define an efficient methodology. Inside these architectures, the authors proposed algorithmic optimizations for the substitution box, and also efficient combinations between the diffusion layer and the key addition.

3. Proposed Methodology

Compared to Mix-Column transformation, Inv Mix-Column transformation has multiplication of long word length. Design of modified mix-column is represented in figure below. The circuit diagram for modified Mix-Column is illustrated in fig.1, in the proposed diagram uses less number of gates to perform the operations. The AES is a symmetric key cryptography, in which both the transmitter and the receiver use a single key for encryption and decryption. AES process the data with the bit length up to 128, 192, 256 bit elements per process. Each bit length has different rounds to process. 128-bit data length uses 10 rounds to complete the process. 192-bit data uses 12 rounds to process the complete action. Likewise 256-bits uses 14 rounds to complete the entire process. AES contain four steps to process the design, S-box, Shift row, mix-column, Add round key, these are the steps to process the complete

Issn No:0975-0932

security algorithm. It process the bit by using 4x4 matrix , each cell contain 8-bit to process the data. Likewise each cell 128-bit into 16 groups and process each group in each cell. In future the process can be improved by using 2x2 matrix, in each cell process 24-bit data to reduce the computational time during the time of operation.

When compared to Mix-Column transformation, Inv Mix-Column transformation has multiplication of long word length. Therefore, Matrix multiplication of Inv Mix-Column can be realized and re-designed. Design of Optimized Inv Mix-Column is represented in below. In Inv Mix-Column, {09, 0b, 0d, 0e} is multiplied with input bytes. Let input bytes are represented as b_0 to b_7 and output of Inv Mix-Column are represented as t_0 to t_7. The multiplication can be described as follows:

Multiplication of {09} with state-byte,

$$t_7 = 0\ ,\ \ t_6 = b_7\ ,\ t_5 = b_6\ , t_4 = b_5 \oplus b_7\ , t_3 = b_5 \oplus t_4\ , t_2 = b_6\ , t_1 = t_4\ , t_0 = b_5 \oplus b_6$$

Multiplication of {0b} with state-byte,

$$t_7 = 0\ ,\ \ t_6 = b_7\ ,\ \ t_5 = b_6 \oplus b_7, t_4 = b_5 \oplus t_5\ , t_3 = b_5, t_2 = t_5, t_1 = t_4, t_0 = b_5 \oplus b_7$$

Multiplication of {0d} with state-byte,

$$t_7 = 0\ ,\ \ t_6 = b_7\ ,\ \ t_5 = b_6\ , t_4 = b_5 \oplus b_7\ , t_3 = b_5 \oplus t_4\ , t_2 = b_6\ , t_1 = t_4\ , t_0 = b_5 \oplus b_6$$

Multiplication of {0e} with state-byte,

$$t_7 = 0\ ,\ \ t_6 = b_7\ ,\ \ t_5 = b_6\ , t_4 = b_5\ , t_3 = b_5 \oplus t_6\ , t_2 = b_6\ , t_1 = b_5\ , t_0 = t_3 \oplus b_7$$

4. Results and Discussions

Issn No:0975-0932

The modified Mix-Column was designed Verilog HDL. The simulation results are estimated using Modelsim 6.3C, and synthesis results are evaluated by using Xilinx 10.1i design tool. In modified Mix-Column design is reduced the gate counts with the Xtime multiplication. Further, modified Mix-Column Transformation is a technique used to progress the efficiency of the algorithm. The simulation results for AES encryption by using Optimized MixColumn design is illustrated in Fig.2 and the simulation results for AES decryption by using Optimized MixColumn design is illustrated in Fig.3.

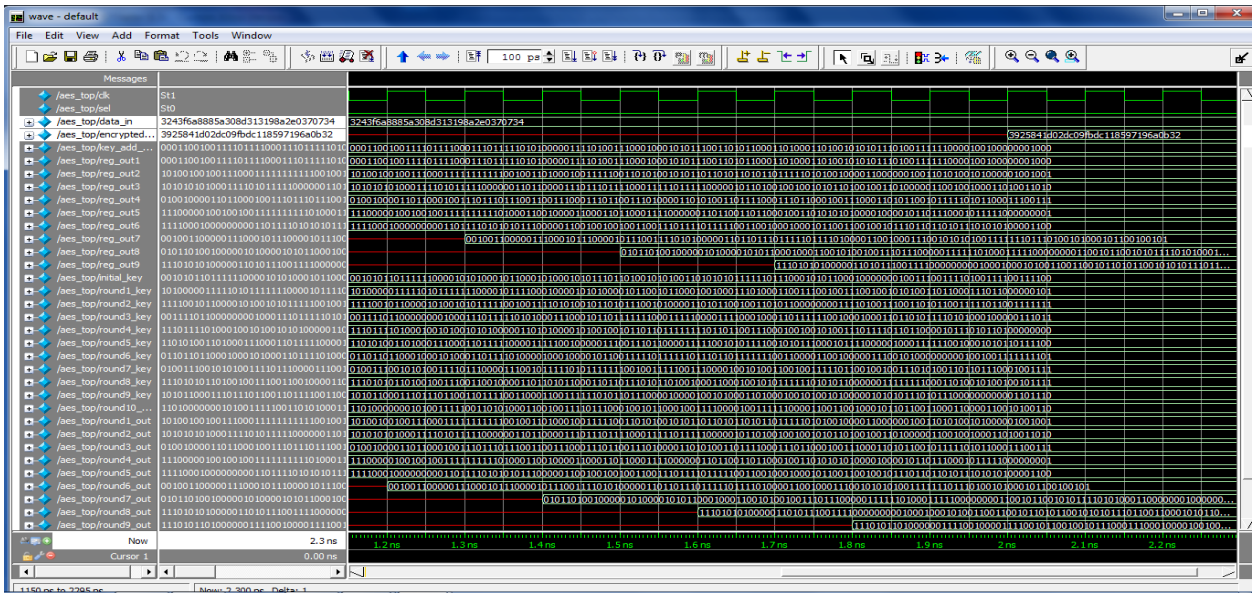


Fig. 2. Simulation Result for AES Encryption by using Optimized Mix-Column

Issn No:0975-0932

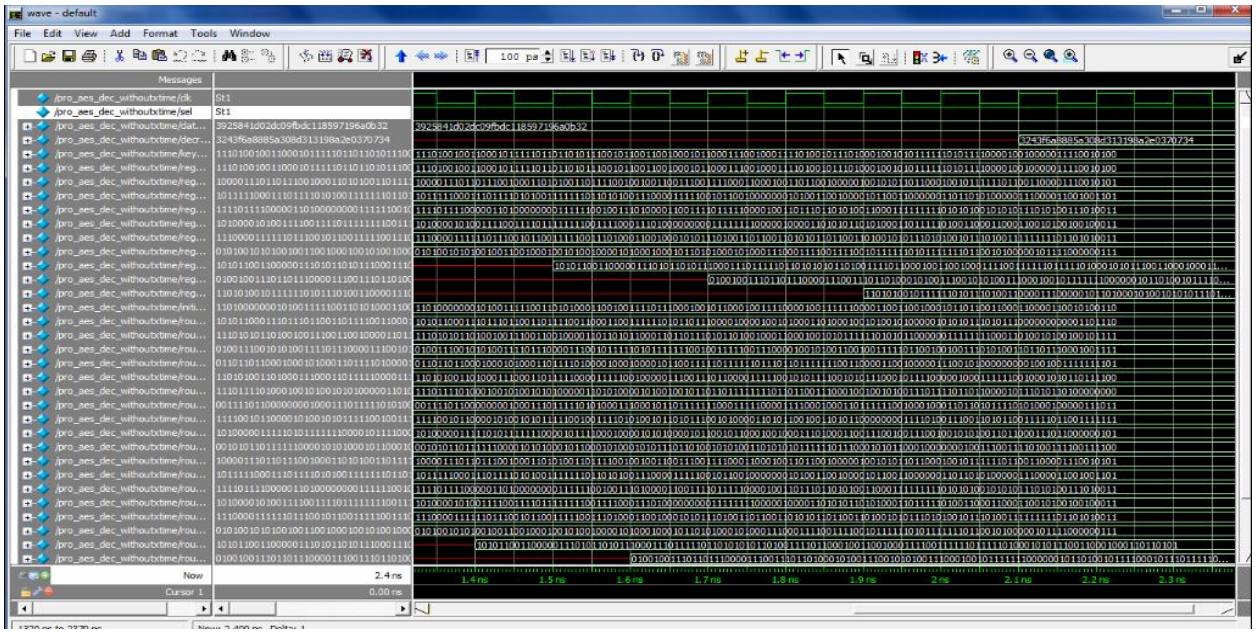
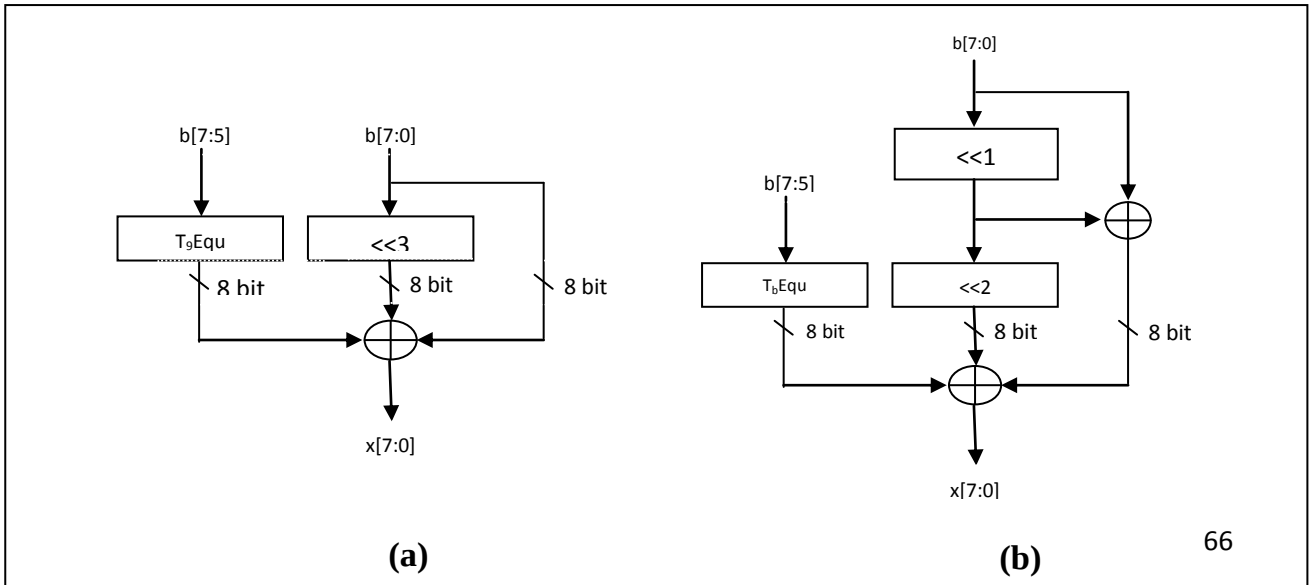


Fig. 3. Simulation Result for AES Decryption by using Optimized Mix-Column



Issn No:0975-0932

Fig. 1 Structure for Optimized Xtime Multiplication

Table. 1 Comparison of Existing and Proposed AES Mix column

Description	Slices	LUT	Delay(ns)	Power(mw)
Existing AES with Conventional	10746	20760	7.550	7.765

Issn No:0975-0932

Inverse Mix-column				
Proposed AES with Optimized Mix-column	10541	20064	7.531	6.722

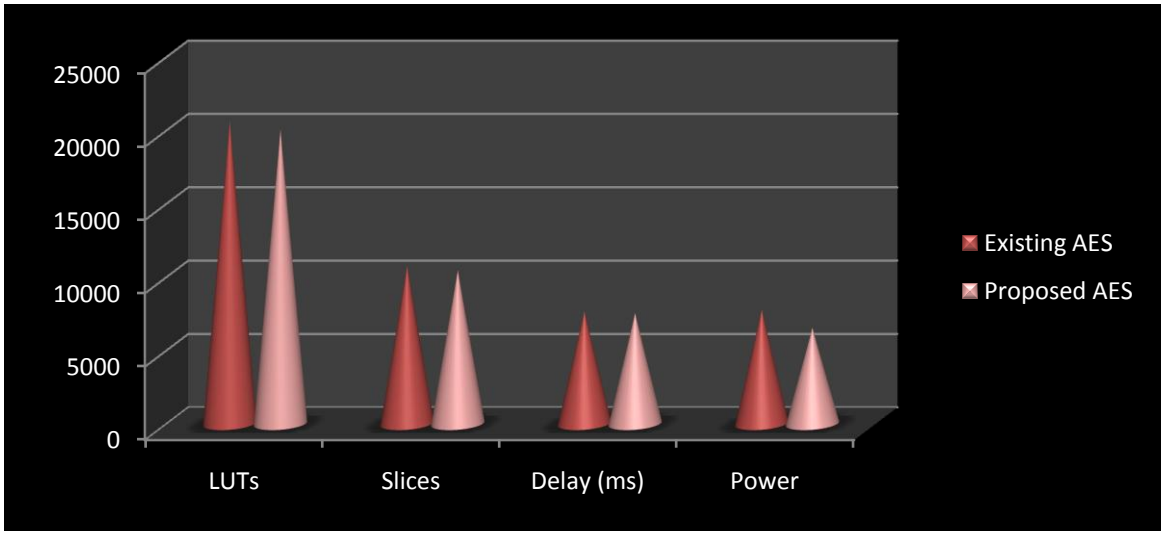


Fig. 4. Graphical Representation of Existing and Proposed AES

5. Conclusion

In this work, the proposed methodology was designed using in terms of the Very Large Scale Integration (VLSI) environment. The arrangement of Xtime multiplication is modified without any changes in operation for reducing the logic gate counts. In the proposed technique reduced the gate counts in the mix-column process. Proposed AES encryption provides 1.9%

Issn No:0975-0932

reduction in slices counts and 3.3% reduction in LUTs counts. Similarly computational delay is minimized than the existing AES encryption. When compared to existing AES encryption and Decryption using Xtime multiplication based mix-Column, the proposed AES decryption based Optimized mix-Column gives a better performance.

References

1. Agarwal, A, (2013) "VLSI Implementation of Advanced Encryption Standard using Rijndael Algorithm" International Journal of Application or Innovation in Engineering and Management (IJAIEM).
2. Al-Hazaime, O.M.A, (2013) "A New Approach for Complex Encrypting and Decrypting data" International Journal Computer Networks and Communications (IJCNC).
3. Babu, R. Abraham, G. and Borasia, K. (2012) "Securing Distributed Systems Using Symmetric Key Cryptography".
4. Liu, B. & Baas, B. M. (2013) "Parallel AES encryption engines for many-core processor arrays" IEEE Transactions on Computers pp. 536-547.
5. Shylashree, N. Bhat, N. & Shridhar, V.(2012) "FPGA implementations of advanced encryption standard: a survey" International Journal of Advances in Engineering & Technology, Vol.3, No.2, pp. 265-285.
6. Standaert, F.X. Rouvroy, G. Quisquater, J. J and Legat, J.D.(2004) "Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware".
7. Zhao, W. Ha, Y. & Alioto, M. " AES architectures for minimum-energy operation and silicon demonstration in 65nm with lowest energy per encryption" IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2349-2352, 2015.
8. Zhang, Q. Cao, J. Yu, D. Cao, X. & Zhang, X. " A Low-energy high-throughput asynchronous AES for secure smart cards" pp.487-490, 2015.

Issn No:0975-0932

Issn No:0975-0932