Improvement of Data Security Using Mixcolumn

Singh Poja Ramesh[1], Santhosh Kumar Singh[2]
[1] Research Scholar, AMET University, Chennai
[2] Assistant Professor, Tagore College of Science & Commerce, Mumbai

Article Info

Article history:

Received Oct 21, 2017
Revised Dec 27, 2017
Accepted Jan 12, 2018

Keywords:

AES
Mixcolumn
Xtime

ABSTRACT

Advanced Encryption Standard is the security based algorithm used to protect the data from the attackers.In this paper, Optimized Inverse MixColumn 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 MixColumn transformation provide better performances than traditional Xtime based Inverse MixColumn multiplication.

Corresponding Author:

Singh Poja Ramesh,
Research Scholar,
AMET University,
Chennai.

1. INTRODUCTION

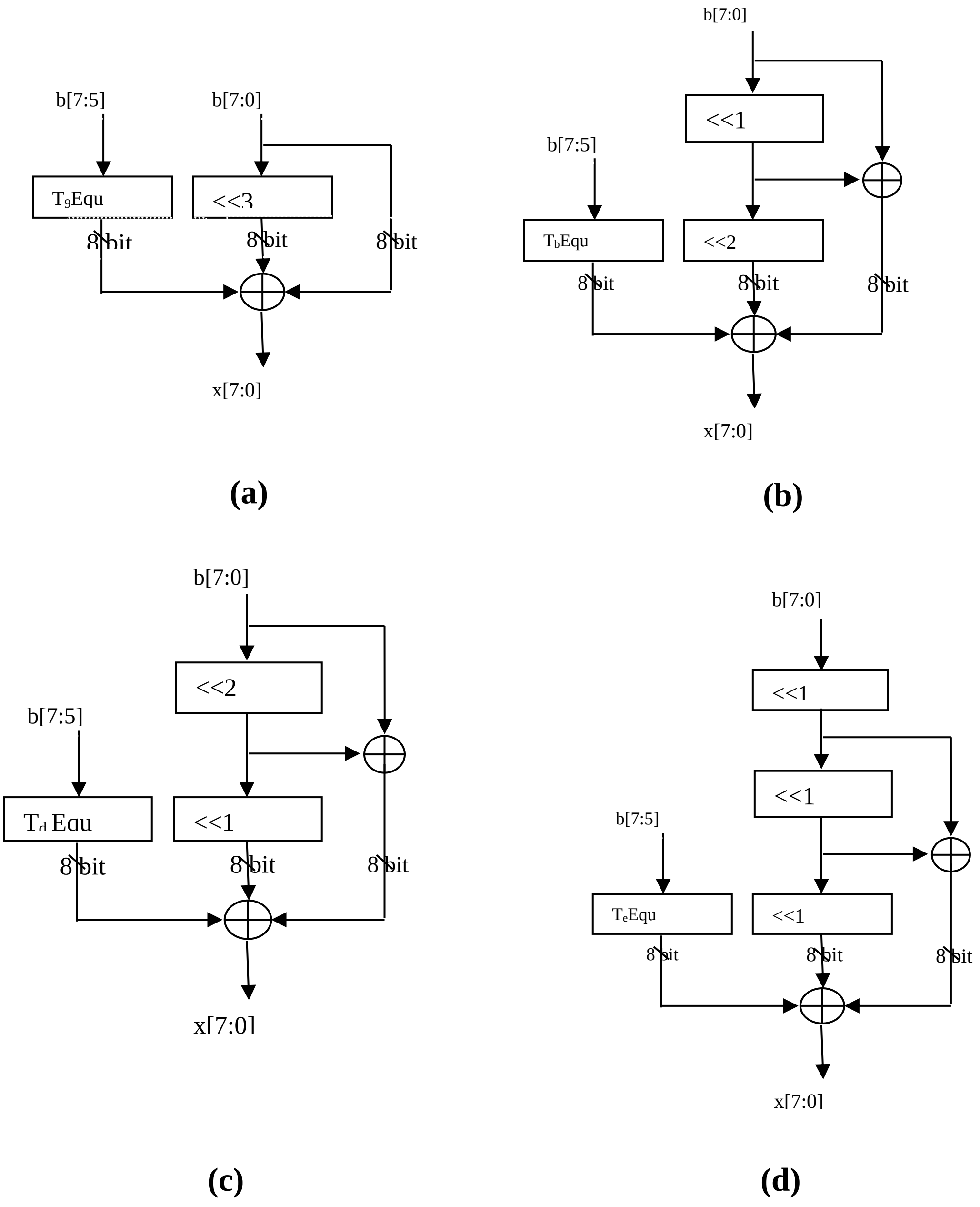
Data security is one of the key features in any communication system. The security providing to the system is done by using some software. It was developed by using algorithm [1]. In previous days Data Encry ption Standard (DES) is the algorithm to provide security. DES algorithm provides security but 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 [2]. To overcome the drawback by introduce a new algorithm named as Advanced Encryption standard (AES). It overcomes the drawback of DES algorithm. Because it has large number of steps to provide the security to the system [Mangard, S. et al., 2005]. Finally, try to remove correlation between the secret keys and the power consumption [3]. The multiplicative masking 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 gate level (which has to be proved as insecure in terms of glitch attacks). Divisive Hierarchical Bisecting Min–Max Clustering Algorithm is described in [4]. Boolean masking is realized to be at the algorithmic level and is immune to DPA and glitch attacks. Boolean masking had an advantage, it is easy to implement. It does not require any extra specific hardware. Boolean Masking is a fine candidate to apply AES in Storage Area Networks [Golic, J.D.et al, 2007].

2. 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 shown in Figure 1(a), Figure 1(b), Figure 1(c) and Figure 1(d) respectively, in the proposed diagram uses less number of gates to perform the operations. The AES is a symmetric key cryptography, in which both the sender and the receiver use a single key for encryption and decryption. AES process the data with the bit length up to 128, 192, 256 bits 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 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.



(a) **(b)**

(c) **(d)**

Figure 1. Diagrams for Optimized Xtime Multiplication

3. SIMULATION RESULTS AND DISCUSSION

The modified Mix-Column was designed Verilog HDL. The simulation results are validated using Model-sim 6.3C, and synthesis results are evaluated by using Xilinx 10.1i design tool. Inmodified Mix-Column design is reduced the gate counts with theXtime multiplication. Further, modified Mix-Column Transformation is a technique used to improve the performance of the algorithm.The simulation results for

AES encryption by using Optimized MixColumn design is illustrated in Figure 2 and the simulation results for AES decryption by using Optimized MixColumn design is illustrated in Figure 3.

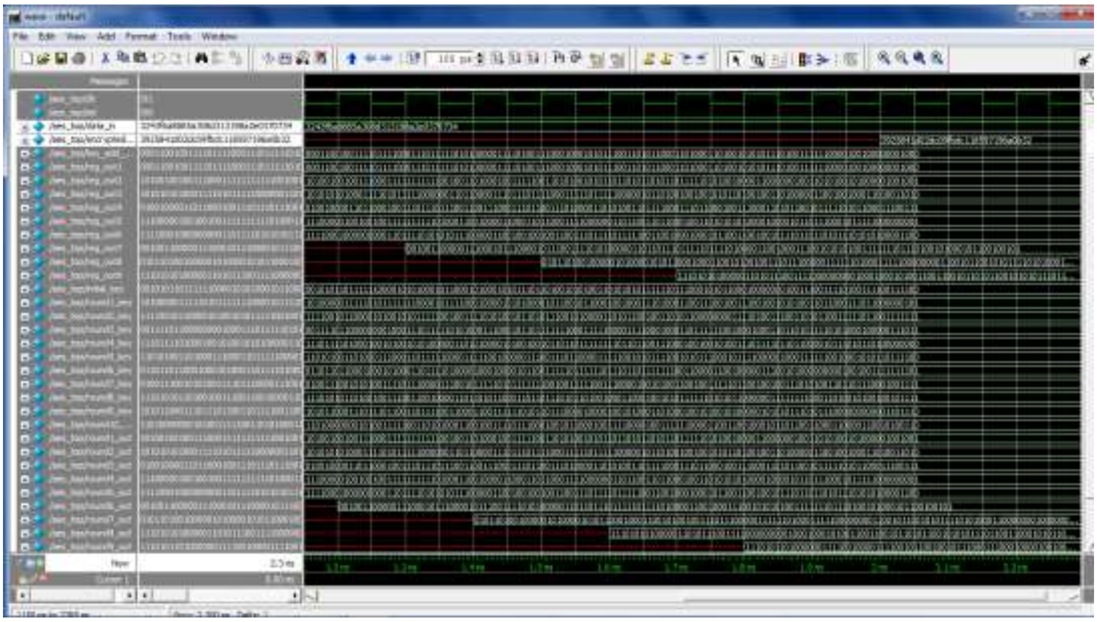


Figure 2. Simulation Result for AES Encryption by using Optimized Mix-Column

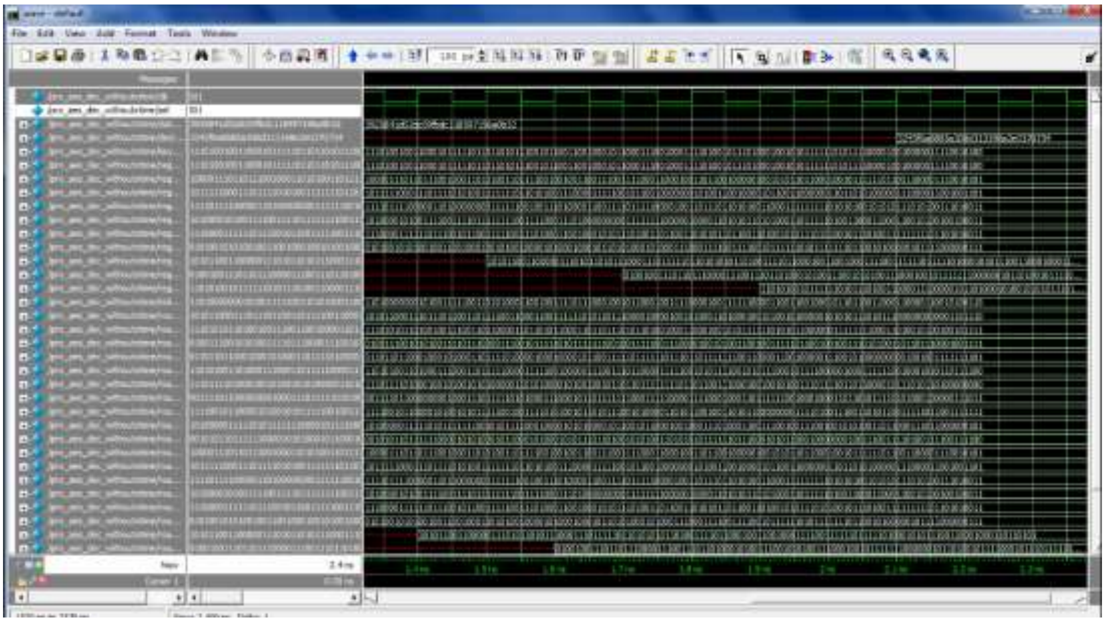


Figure 3. Simulation Result for AES Decryption by using Optimized Mix-Column

Table 1. Comparion of Existing and Proposed AES Mixcolumn

Type	Slices	LUT	Delay(ns)	Power(mw)
Existing AES	10746	20760	7.550	7.765
Proposed AES	10541	20064	7.531	6.722

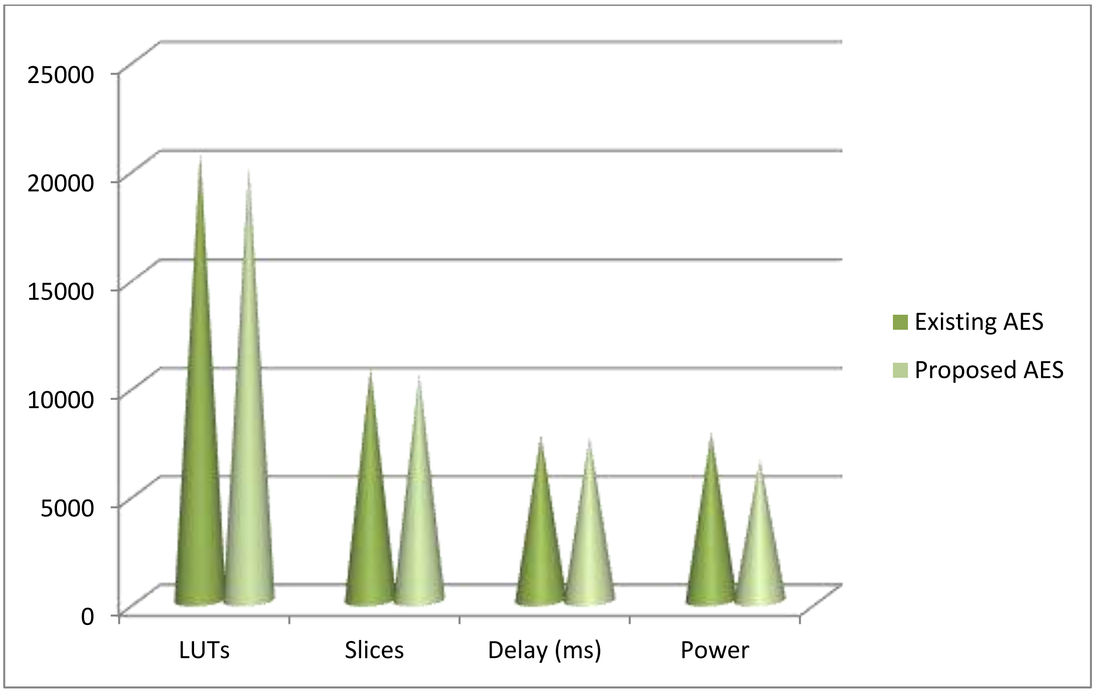


Figure 4. Performance Analysis of Existing and Proposed AES

4. CONCLUSION

In this paper, the proposed technique was designed using through Very Large Scale Integration (VLSI) System design. 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% reduction in slices counts and 3.3% reduction in LUTs counts.Similarlydelay is reduced when compared to the existing AES encyption. 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] A. Agarwal, “VLSI Implementation of Advanced Encryption Standard using Rijndael Algorithm,” *International Journal of Application or Innovation in Engineering and Management (IJAIEM),* vol/issue: 2(4), 2013.

[2] N. Ahmad, *et al.*, “Design of AES S-Box using combinational logic optimization,” *IEEE Symposium on Industrial Electronics & Applications (ISIEA)*, pp. 696-699, 2010.

[3] M. G. Alam, *et al.*, “Effect of glitches against Masked AES S-box implementation and countermeasure,” *IET Inf. Security*, vol/issue: 3(1), pp. 34–44, 2009.

[4] T. Johnson and S. K. Singh, “Divisive Hierarchical Bisecting Min–Max Clustering Algorithm,” in *Proceedings of the International Conference on Data Engineering and Communication Technology*, pp. 579-592, 2017.