Research Journal of Applied Sciences, Engineering and Technology 8(15): 1719-1723, 2014
DOI:10.19026/rjaset.8.1155
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: July 18, 2014 Accepted: September 13, 2014 Published: October 15, 2014

Research Article

Incorporation of Wave Pipelined Techniques into Composite S-Box and AES Architectures

[1]M. Senthil Kumar and [2]S. Rajalakshmi
[1]Department of ECE,
[2]Department of CSE, SCSVMV University, Kanchipuram, Tamil Nadu, India

Abstract: Advanced Encryption Standard is one of the most successful techniques used in various security applications. The AES technique is known to provide reliable security standards, which is why it is preferred over many other methods. The AES architecture consists of S-Box, Shift-Rows, Mix-Columns and Add Round key. Improving the S-Box structure using pipelining improves the speed of operations along with the security. The main aim of this research study is to design a modified composite S-Box for low area, power and high Speed with high security for application in AES process. In this study, we propose a WPT in S-Box also controlling the registers with a clock-gate structure, to further reduce the operational delay and obtain high security. The modified S-Box is then included in the AES architecture with an additional modification on the overall AES architecture by introducing the WPT in every round of AES operation. This is not only improves the speed of operation and also it provides high security compared to many existing techniques along with the area and power reduction. Simulations have been performed in the ModelSim6.3c and Synthesis is carried out using Xilinx10.1.

Keywords: AES, modified S-box, Wave Pipelined Technique (WPT), xilinx

INTRODUCTION

Cryptography is used to transfer the information in the secure way. Besides its uses in Government's secret communication and Military, cryptography is in addition used for shielding several types of civilian systems like Mobile networks, ATM machine transactions, internet e-commerce, copy protection and many of Encryption is attained by following a scientific principle called as cryptography formula (Wang and Ha, 2013). An encryption formula offers privacy, Integrity, Non-repudiation and Authentication. privacy is that the demand that data is unbroken secret from those who do not appear to be authorized to access it. Authentication is that the knowing that the message thus initiates from the reputed sender. Integrity is that the demand that information is unchanged and complete. Non repudiation means that the sender or receiver of a message cannot reject or received the message (Gurpreet and Nishi, 2014).

Cryptography take part in a very important role within the security of awareness transmission. The event of computing technology imposes stronger needs on the cryptography methods. The Data Encryption Standard (DES) has been the U.S. government customary since 1977. However, at the present, it may be cracked rapidly and inexpensively. In 2000, the Advanced Encryption Standard (AES) changed the DES to complete the ever-increasing requires for security. This normal specifies the Rijndael formula, a symmetrical block cipher that the information blocks of 128 bits, using cipher keys with lengths of 128, 192 and 256 bits, respectively. Rijndael was designed to handle additional block sizes and key lengths; however they're not adopted throughout this normal (Gnanambika *et al*., 2013). The main objective of this paper is to design of optimum ADP (Area, Delay and Power) product based composite S-Box using Wave Pipelined Technique (WPT). This Composite S-Box with WPT is incorporated into AES encryption/ Decryption process to further improve the security.

Existing AES with regular S-box architecture: AES 128 bit encryption and decryption is performed based on Rijndael algorithm. For encryption S-Box, Shift-Rows, Mix-Columns and Add Round key is performed to convert the cipher text.

To perform the decryption process, Inv-S-Box, Inv Shift-Rows, Add Round Key and Inv-Mix-Columns is applied to convert the plain text (Menakadevi and Madheswaran, 2011). Encryption is the process of converting the plain text into a format which is not easily readable and is called as cipher. The cipheris got by doing a series of mathematical operations iteratively (Anumol and Sathyanarayana, 2013).

As shown in the block level diagram in Fig. 1, the AES decryption initially performs key-expansion on the 128-bit key block. Then the round key signal starts the actual decryption process once the data process is ready. It starts by executing an inverse add round key

Corresponding Author: M. Senthil Kumar, Department of ECE, SCSVMV University, Kanchipuram, Tamil Nadu, India

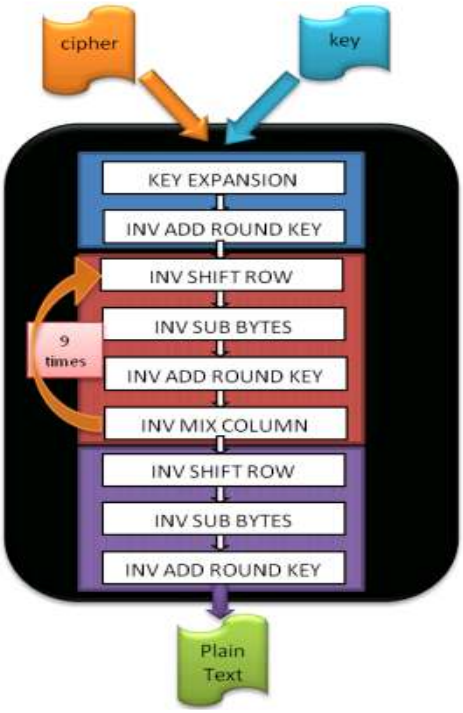

Fig. 1: Block diagram of regular AES architecture

between cipher texts with the modified key (generated in the last iteration of the encryption process) from key expansion. After this step, the AES decryption repeats the inverse shift row, inverse sub, inverse add round key and inverse mix column steps nine times. At the last iteration, it does an inverse shift row, inverse sub bytes and inverse add round key to generate the original data (Raneesha *et al*., 2012).

PROPOSED MODIFIED AES AND S-BOX STRUCTURE BASED ON WPT

In this study, Wave Pipelined Techniques (WPT) is considered. Proposed AES is implemented using WPT. And also the composite S-Box is constructed using Wave Pipelined Techniques (Anbuselvi *et al*., 2011). Modified Composite S-Box with WPT consists of 5 clock gating structures to reduce the delay and security. The design optimization is done in the composite S-Box and overall AES architecture (Ganesh *et al*., 2012). Clock gating structure is designed using one register and any one basic gate (Hauckand and Huss, 1998). Here we are using and gate to control the register. Whenever the en = 0 and global clk = 1, during that time only clock for register is generated.

So switching activity is reduced to increase the speed of the S-Box and overall AES architectures. Proposed AES with modified composite S-Box consumes less area, delay and power than the regular AES architectures. The overall AES structure with wave pipelined techniques is shown in the Fig. 2. Also modified composite S-Box structure is constructed by clock gating structure as shown in the Fig. 3.

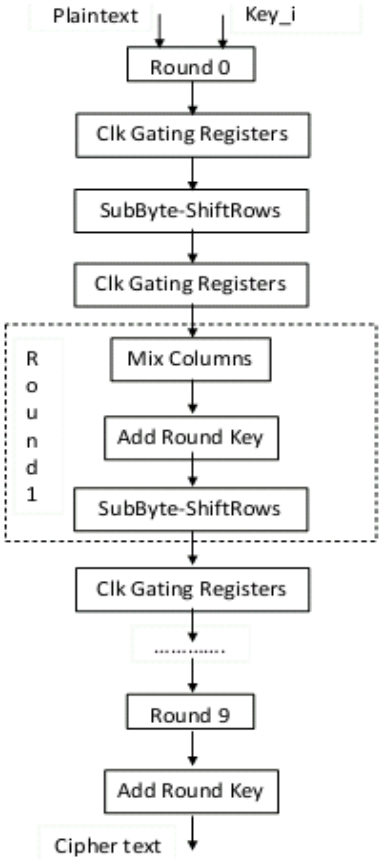

Fig. 2: Structure of proposed AES using Wave Pipelined Techniques (WPT)

Table 1: Comparison of proposed AES with modified composite S-box over regular AES

Performance	Slices	LUT
Existing AES with regular S-box	584	881
Proposed AES with modified composite S-box	269	470

RESULTS AND DISCUSSION

The design of a novel AES with modified composite S-box using Wave Pipelined Techniques are done using Verilog and implemented in a Xilinx Virtex 4 (package: FF668, speed grade: -12) FPGA using the Xilinx ISE 10.1i design tool. Total equivalent LUT in case of conventional AES with regular S-box is 128 and that is improved to 89 using composite S-Box. The power consumption in case of existing AES is 552 mW and that is also improved to 501 mW using modified S-Box. The number of occupied slices used in proposed AES is also improved. In case of existing AES it is 64 and in proposed modified AES structure it is 47. The result is illustrated in the Table 1 and 2.

Figure 4 shows the performance investigation between conventional regular S-Box and modified composite S-Box with Wave Pipelined technique. From the above analysis, the proposed composite S-Box with Wave Pipelined technique offers 26.5% Slices

Table 2: Comparison of proposed AES with WPT over conventional AES

Performance	Slices	LUT	Delay (nsec)	Power (w)
Existing regular S-box	64	128	6.864	0.552
Modified composite S-box using WPT	47	89	5.138	0.501

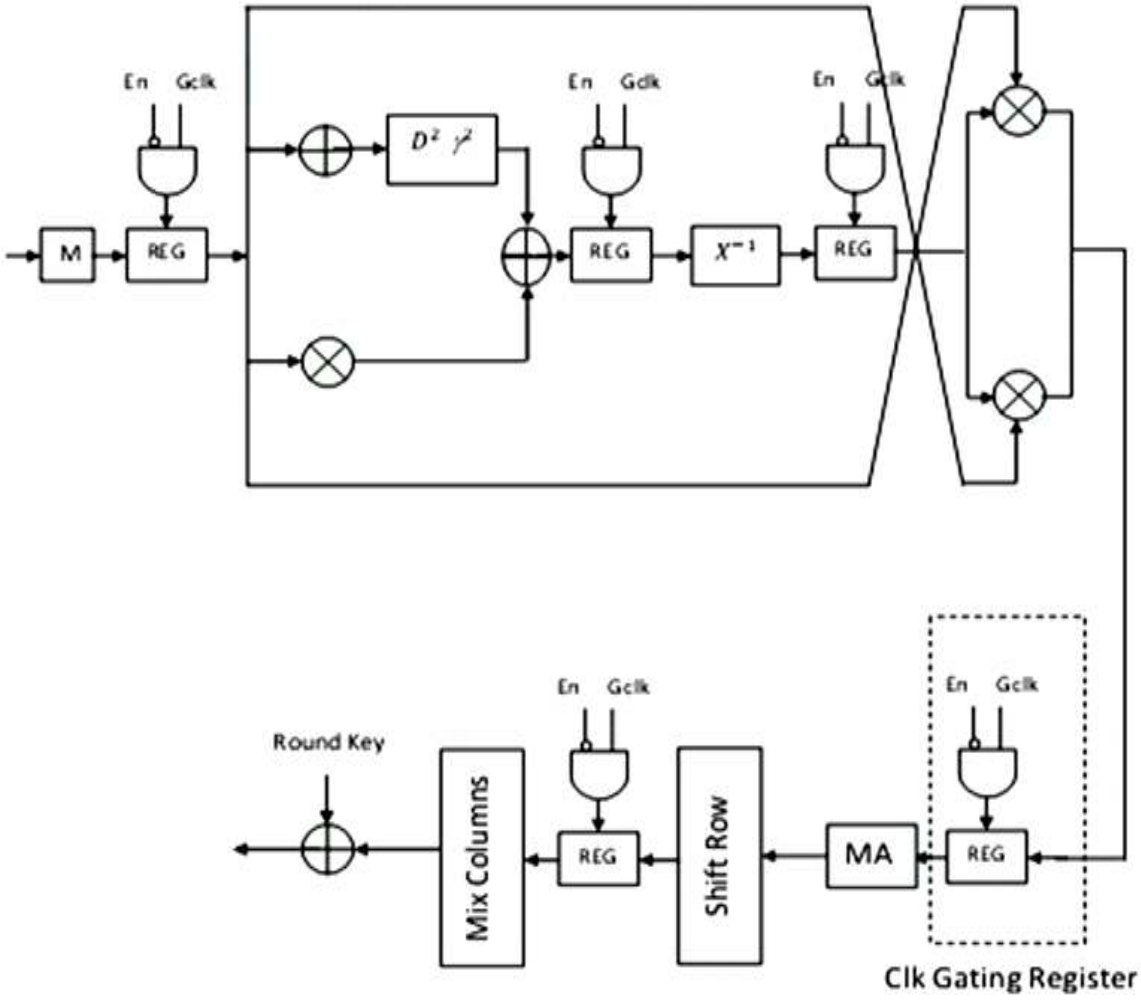

Fig. 3: Block diagram of modified S-box with wave pipelined techniques

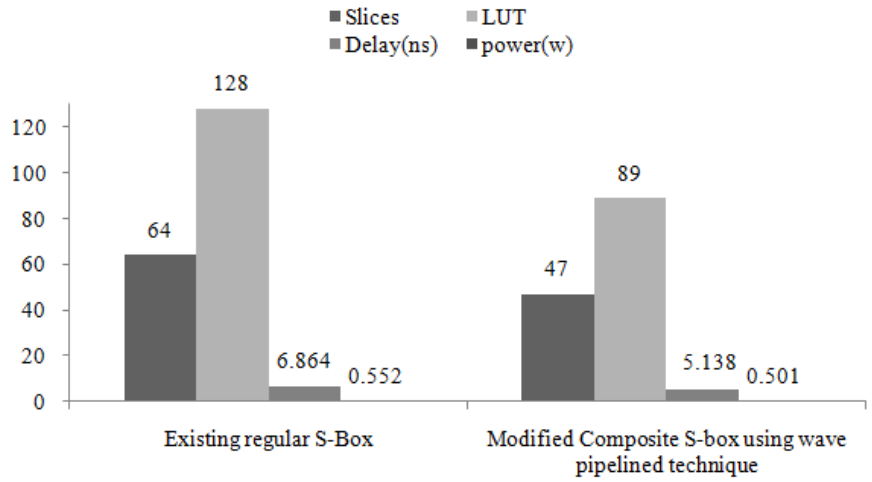

Fig. 4: Performance of proposed AES over existing AES

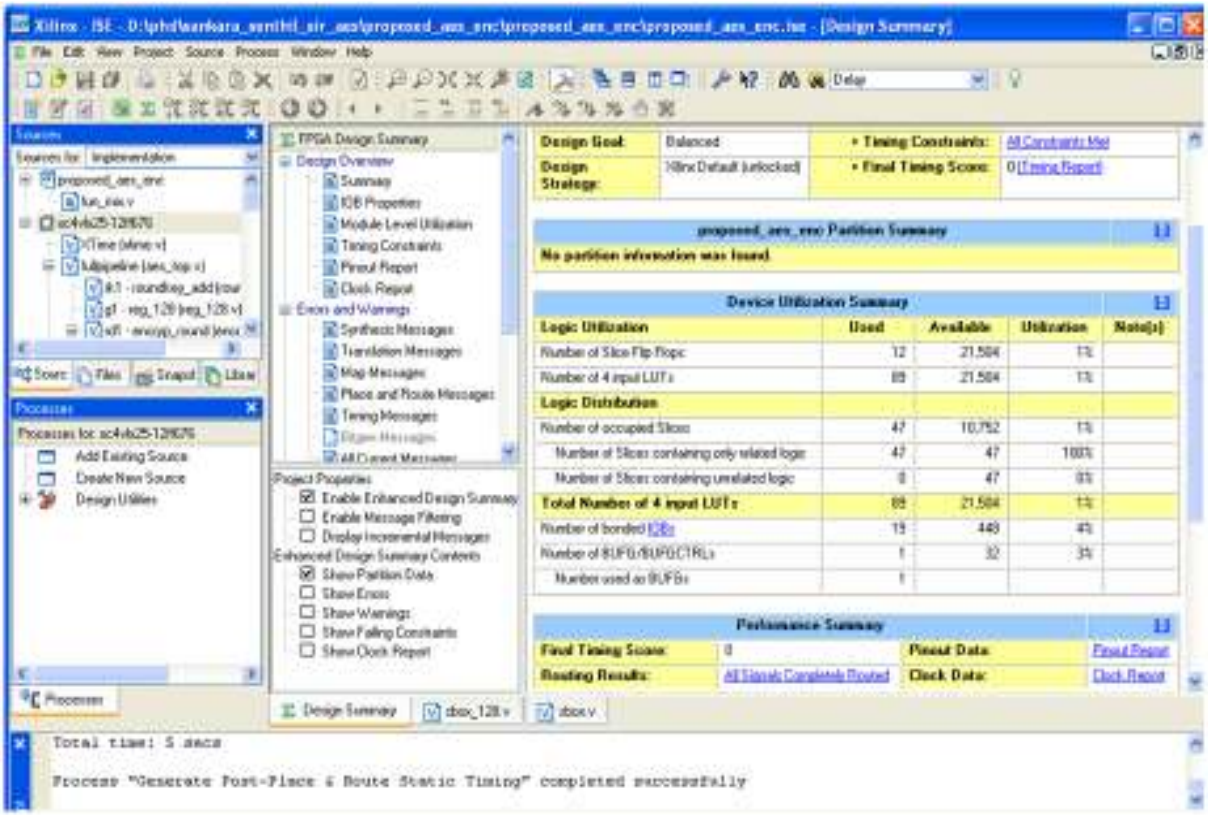

Fig. 5: Synthesis result of proposed composite S-box with WPT for area utilization

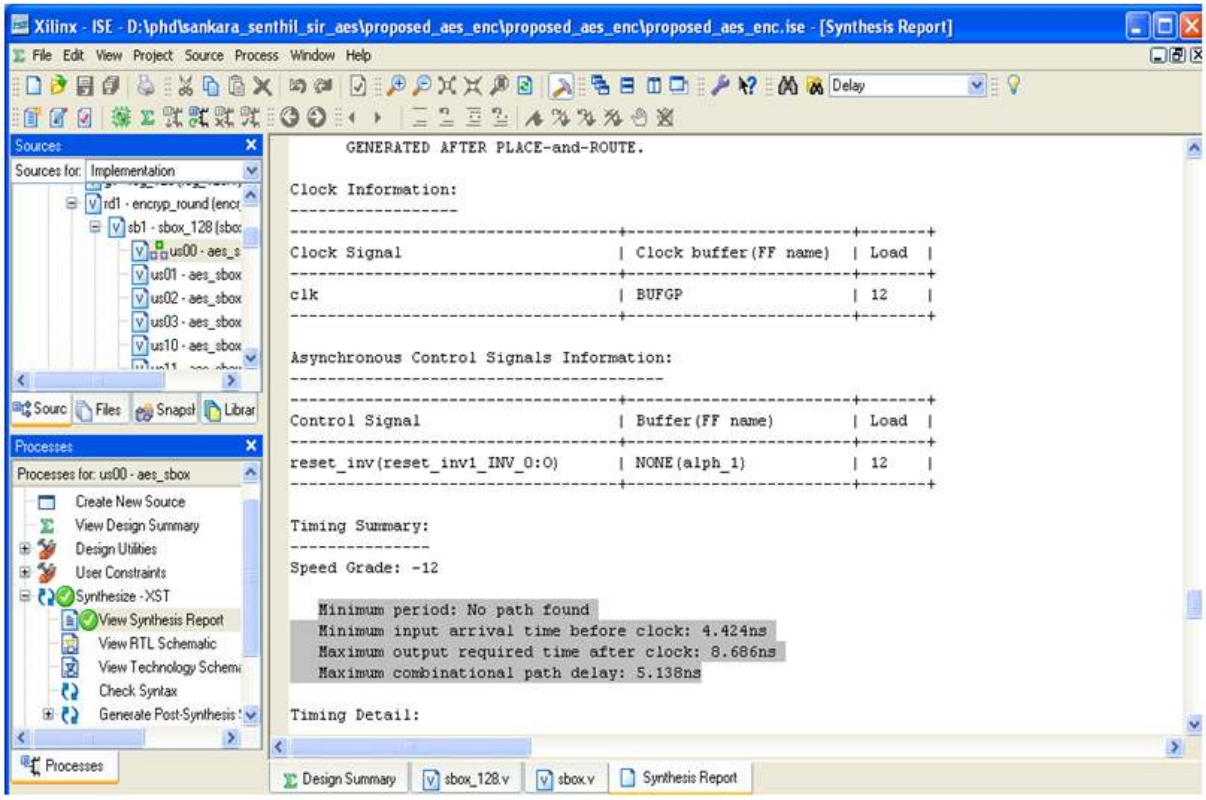

Fig. 6: Synthesis result of proposed composite S-box with WPT for area utilization

reduction, 30% LUT reduction, 25% delay reduction and 9% power reduction when compared to the conventional regular S-Box structures.

Synthesis results of proposed composite S-Box with Wave Pipelined Technique are processed for area and delay utilization. The area or slices (Slices = 2 LUT+Flip Flops) utilization of proposed composite S-Box with WPT is measured using Xilinx10.1 EDA tool as shown in Fig. 5. Similarly the delay utilization of proposed composite S-Box is measured through synthesis process of Xilinx as shown in Fig. 6.

CONCLUSION

In this study we have designed an improved S-Box structure with the introduction of WPT. This improved S-Box is applied in the AES architecture. Also, the WPT technique is introduced in every round of the AES architecture along with the improved S-Box. This changed the overall AES architecture improving the speed of operation and security. The area is reduced by 30% and power is reduced by 10%. This proves the efficiency of the improved AES architecture. In future, AES Mix Columns will be designed using various pipelined techniques to improve the speed and security.

REFERENCES

Anbuselvi, M., S. Salivahanan and P. Saravanan, 2011. Analysis of wave-pipelined architecture of ara-LDPC codes. Int. J. Comput. Appl., 24(3): 43-47.

Anumol, M. and M. Sathyanarayana, 2013. Design of area optimized AES 128 algorithm using mix column transformation. Int. J. Innov. Res. Dev., 2(7).

Ganesh, E.S., R. Velayutham and D. Manimegalai, 2012. A secure software implementation of nonlinear AES S-Box with the enhancement of biometrics. Proceeding of International Conference on Computing, Electronics and Electrical Technologies (ICCEET, 2012), pp: 927-932.

Gnanambika, M., S. Adilakshmi and F. Noorbasha, 2013. AES-128 bit algorithm using fully pipelined architecture for secret communication. Int. J. Eng. Res. Appl. (IJERA), 3(2): 166-169.

Gurpreet, K. and M. Nishi, 2014. A comparative study of AES encryption decryption. Int. J. Sci. Res. (IJSR), 3(4), ISSN (Online): 2319-7064.

Hauckand, O. and S.A. Huss, 1998. Asynchronous wave pipelines for high throughput datapaths. Proceeding of IEEE International Conference on Electronics, Circuits and Systems. Lisboa, pp: 283-286.

Menakadevi, T. and M. Madheswaran, 2011. Design and analysis of hybrid wave pipelined phase accumulator for direct digital synthesizer. ARPN J. Eng. Appl. Sci., 6(11), ISSN: 1819-6608.

Raneesha, K., R. Vellody and R. Nandakumar, 2012. Hardware efficiency comparison of AES implementations. Proceeding of International Conference on Communication Systems and Network Technologies, pp: 869-873.

Wang, Y. and Y. Ha, 2013. FPGA-based 40.9-gbits/s masked AES with area optimization for storage area network. IEEE T. Circuits-II, 60(1): 36-40.