Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INCORPORATION OF REDUCED 09, 0B, 0D AND 0E STRUCTURES INTO INVERSE MIX COLUMNS FOR AES-128 TECHNIQUE

[1]M.SENTHIL KUMAR, [2]Dr.S.RAJALAKSHMI

[1]Research Scholar, SCSVMV University, Kanchipuram, Tamilnadu, INDIA.

[2]Professor, Dept of CSE, SCSVMV University, Kanchipuram, Tamilnadu, INDIA.

Email: [1]msklecturer@gmail.com , [2]raji.scsvmv@gmail.com

ABSTRACT

Cryptography technique plays a vital role in Signal Processing, Wireless Communication, Satellite Communication, Cellular Mobile Communication and Wi-Max for high security features. AES Encryption is performed to convert plain text into cipher text, and AES Decryption is used to retrieve the original information through some secure Key. Encryption process is divided into Sub-Bytes, Shift-Rows, Mix-Column and Add Round key. Decryption process is split into Inverse Sub-Bytes, Inverse Shift-Rows, Add Round Key and Inverse Mix-Columns. Conventional AES Mix-Columns and Inverse Mix-columns are designed using X-Time unit. X-time unit is used to perform shift and XOR operation more than one time. Hence it consumes more area, delay and power. To overcome this problem, Inverse Mix-Columns unit is designed using reduced 09, 0B, 0D and 0E structures which perform 3 shift operations directly than XOR with fixed coefficient 1B. Number of Shift and XOR operation is reduced in proposed Inverse Mix-Columns structure. Hence reduced Inverse Mix-Columns based AES decryption provides less area, delay and power than conventional X-Time based AES decryption process. Simulation is performed by ModelSim6.3c and Synthesis is carried out Xilinx10.1. Implementation is performed on FPGA Spartan3 device.

Keywords: *Cryptography, X-Time unit, Reduced Inverse Mix-Columns, Modified 09, 0B, 0D and 0E structures FPGA.*

1. INTRODUCTION

Cryptography techniques are studied and practiced for high secure communication in the presence of unknown people. In general, it is about creating and examining procedures that conquer the authority of challenger and which are associated to different features in data security for example authentication data, data integrity, and confidentiality. Cryptology-related knowledge has improved a number of authorized problems [1]. At present cryptography refers encryption, which is the method of converting normal information (called as plaintext), into meaningless information (called as cipher text). Decryption is the reverse process, in other words, moving from the meaningless cipher text return to plaintext [2].

A secret message or cipher is a couple of algorithms that make the encryption process and the reversing decryption process. The exhaustive procedure of a cipher is restricted both by the algorithm and in each and every occasion by a key. This top secret key constraint is perfectly known just by the communicants for a particular message swap situation [13]. A "cryptosystem" is a structured list of building blocks of the encryption and decryption algorithms, finite possible cipher texts, finite possible plaintexts and finite possible keys, which correspond to each and every key [10]. Keys are significant, as secret messages without variable keys can be slightly broken with only the knowledge of the secret message used and are consequently useless.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Secret messages were frequently used straightforwardly for encryption or decryption without extra procedures for example integrity checks or authentication [9]. The major traditional cipher types are transposition ciphers, which reorganize the order of letters in a substitution ciphers and message which systematically modify letters or clusters of letters with additional letters or groups of letters. Easy versions of cipher have not at all offered much privacy from innovative enemies. An early replacement cipher was the Caesar cipher, in which every letter in the plaintext was restored by a letter to a few fixed numbers of locations further down the alphabet.

AES algorithm can be designed effectively by introducing efficient Key generation algorithm, S-box, MixColumns/Inverse MixColumns and better Error detection and correction (EDC) code for fault detection and correction. Hamming code and extended hamming code are used to find fault detection in AES techniques [11]. Key generation is important in AES algorithm, which can be generated using different methods. We can perform the AES operation without Key to obtain high security [14].

Conventional S-box are designed using Linearity S-box and Non Linearity S-box, which consist of multiplicative inverse operation, shift operation and XOR operation or affine Matrix based S-box generation [12]. This S-box provides less security and occupies more chip size. To improve the security higher and reduce area and power, Composite S-box is used in current AES operation, which consist of Galois field GF($(2^4)^2$) for 8 bit to provide high security and high speed operation [8]. MixColumns are designed using standard matrix operation such as 0, 1, 2, 3 operations. Efficient MixColumns operation are performed by introducing shrunk 0, 1, 2, 3 structures. Similarly Inverse MixColumns is performed by incorporation of reduced 09, 0b, 0d, 0e state matrix structures. Multiplier based MixColumns/Inverse MixColumns consumes more area and power [15]. To overcome this problem, Xtime unit is introduced in AES techniques [3] and [4]. It offers less area and power, when compared to multiplier based MixColumns/ Inverse MixColumns structures. Further to reduce the area, delay and power, the reduced Xtime unit is proposed in this paper.

In this paper, a novel reduced Xtime unit is presented to generate shrunk 09, 0b, 0d, 0e structures from regular Xtime unit in the decryption MixColumns structures. Then this reduced MixColumns is incorporated into AES 128 bit standard for smaller chip size, less delay and low power utilization than the all other methods. The main objective of this research work is to reduce the MixColumns/ Inverse MixColumns architecture to obtain low area, delay and power utilization than the conventional all other MixColumns. Also an efficient Composite S-Box technique is incorporated into AES to further improve the security than the Linear and Non-Linear S-Box.

Rest of the manuscript is structured as follows: Section1 briefly establishes the Advanced Encryption Standard (AES) algorithm and its importance in various applications; Section 2 describes about the conventional composite S-box and MixColumns based AES algorithm; Section 3 illustrates the construction of proposed Inverse MixColumns with reduced 09,0b,0d and 0e structures for low power, area efficient and high speed AES standard; Section 4 expresses the VLSI implementation of the proposed AES design and section 5 presents conclusions on our work.

2. CONVENTIONAL AES METHOD USING COMPOSITE S-BOX, XTIME BASED MIXCOLUMNS and INVERSE MIXCOLUMNS

Existing AES method is designed using Composite S-box and Xtime based MixColumns/Inverse MixColumns structures. The complex signal paths of the composite field S-Boxes, which is the major reason for their larger power utilization, can be spitted by converting few parts of the S-Box logic into two-level logic [7]. Even if converting the whole circuit into a single two-level logic configuration would enlarge the circuit size and lose an significant benefit of the composite field S-Box, exchanging carefully chosen sub-elements into two-level logic can make a much better S-Box for AES, if an appropriate partitioning of the S-Box into sub-elements is done [5]. The conventional composite S-box is shown in Figure 1 [17]. This S-box is incorporated into AES 128 bit operation to obtain high security than the linear and nonlinear S-box based AES techniques.

The conventional AES MixColumns is altered to get less area and delay than the previous MixColumns. This MixColumns architecture is reduced using X-time circuit as shown in Figure 2. In Masked AES architecture use complex

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MixColumns [15]. It contains eight multipliers and eleven adders. Hence it consumes larger area and power. In this conventional method, Xtime based MixColumns/Inverse MixColumns are used to reduce the area and power than the masked AES architecture. Because it contains only 12 adders and 4 Xtime in MixColumns and 21 adders and 7 Xtime units in Inverse MixColumns structures.

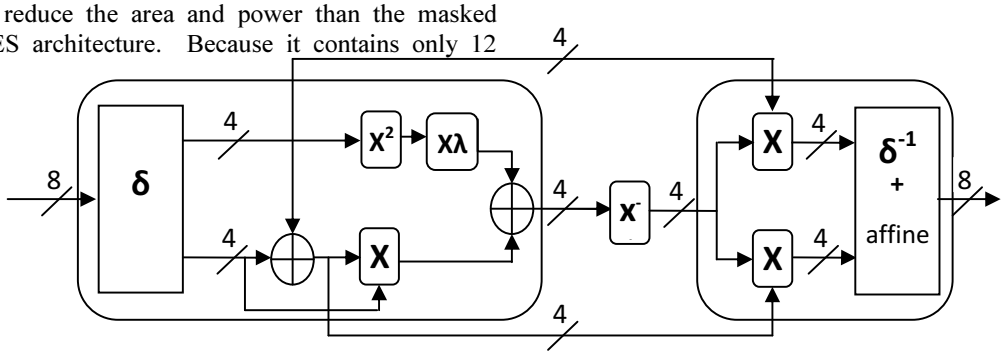

Figure 1 Block diagram of composite S-box for AES 128-bit.

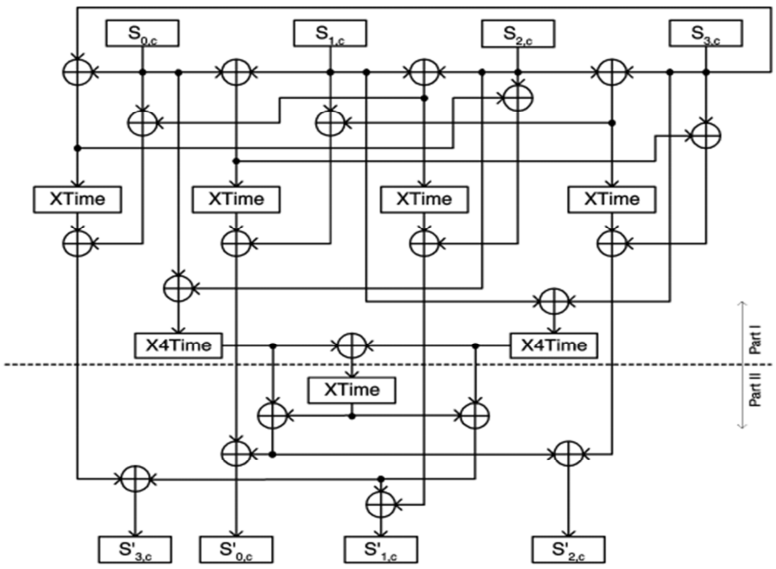

Figure 2 Block diagram of Inverse MixColumns structure using Xtime unit for AES.

Composite S-box and Xtime based MixColumns are included in conventional AES architecture to analyze the area, delay and power utilization [6]. This conventional AES offers more area, delay and power. Further to reduce the area, delay and power of AES architecture, this Xtime based Inverse MixColumns are modified and presented in next section of this paper.

3. REDUCED XTIME BASED INVERSE MIXCOLUMNS

In the proposed method, a novel Inverse MixColumns is introduced to reduce the area and power than the existing AES method. The proposed Inverse MixColumns consists of reduced structures for 09, 0b, 0d and 0e state matrixes. Reduced 09, 0b, 0d and 0e state matrix structure are designed to generate the coefficient by using some equations. Instead of normal Xtime in the Inverse MixColumns, we are using reduced

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

X-time unit to reduce the circuit complexity, area, delay and power.

In the reduced Xtime unit perform three shift operation directly and every steps it perform only 3-bit XOR operation for each 09, 0b, 0d and 0e structures, instead of 3 shift one by one and 8 bit XOR operation for every steps of inverse MixColumns as shown in Figure 3.

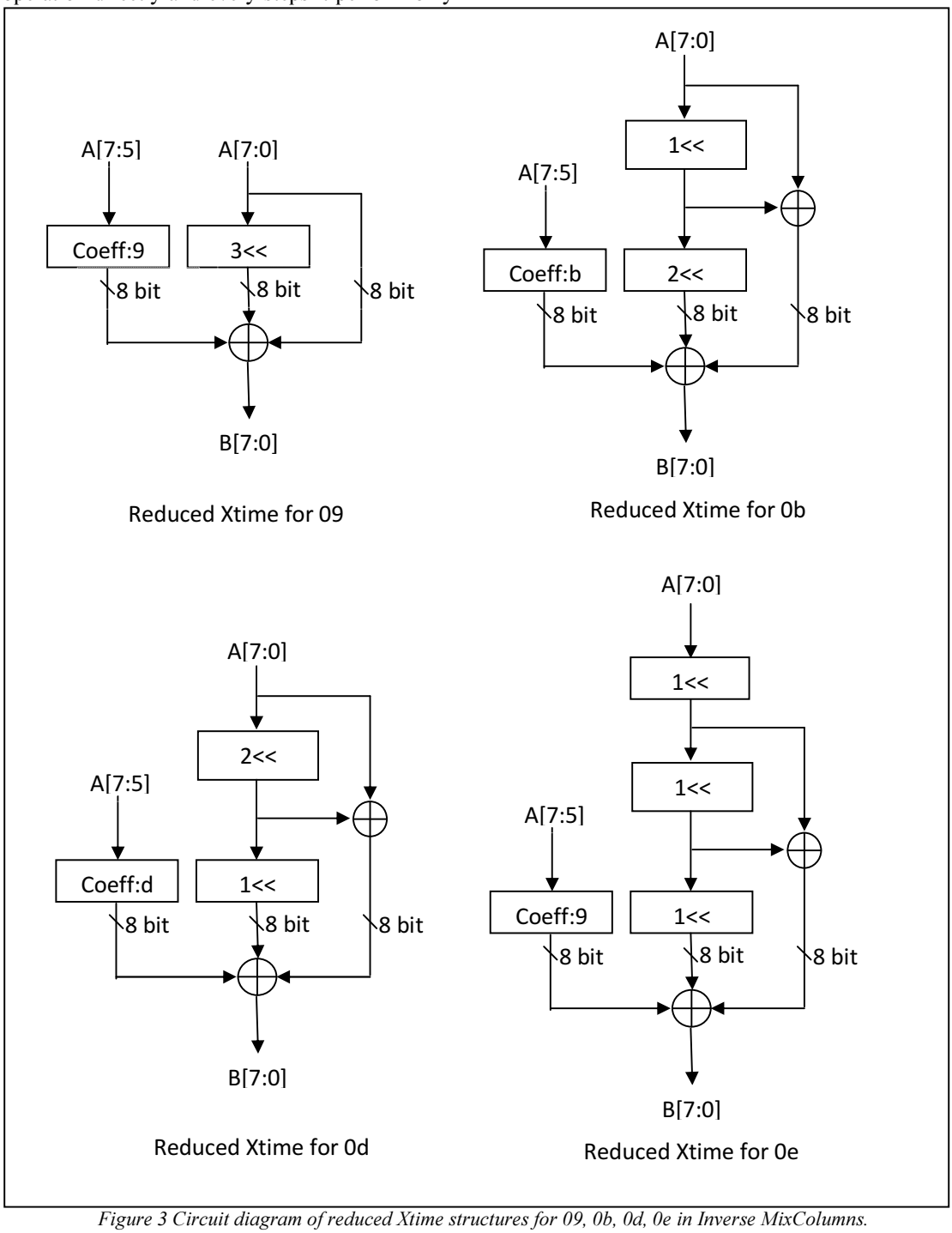

Figure 3 Circuit diagram of reduced Xtime structures for 09, 0b, 0d, 0e in Inverse MixColumns.

128-bits MixColumns are performed by four 32-bits and this 32-bit is split into four 8-bits. For Every 8-bits, 09 (01+08), 0b (01+02+08), 0d (01+04+08) and 0e (02+04+08) operation are

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

performed in inverse MixColumns. From the 8-bit of input last 3bits are shifted and then perform 01, 02, 04 and 08 operation for every steps of 09, 0b, 0d and 0e structures.
Last three bits (i.e b7:b5) coefficient are generated by using equations for every structures.

For 09, the coefficient of 3 bits are generated by using this equations

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

Similarly for 0b, the coefficient of 3 bits are generated by using this below equations

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

For 0d, the below equation are used to generate the 3-bits coefficients.

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

For 0e, the below equation are applied to make the 3-bits coefficients.

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

From the above equations, only 3XOR operations are required for every step of 09, 0b, 0d and 0e structures. Hence it is called as reduced Xtime unit. In this paper, a novel Inverse MixColumns of 09, 0b, 0d and 0e are performed using reduced Inverse MixColumns. Then this Inverse MixColumns based on reduced Xtime is incorporated into AES 128-bits cryptography process for high security, smaller chip size, high speed and low power utilizations than the conventional Xtime based AES 128-bits operations.

Limitation of Current S-Box and Inverse MixColumns:

Composite S-Box consists of Isomorphic mapping, Inverse affine, Multiplexer, Multiplicative Inverse, Inverse isomorphic mapping and affine. Isomorphic mapping is used to split GF (2^8) into three GF (2^2).Similarly Inverse isomorphic mapping is used to reconstruct three GF(2^2) into GF(2^8). Affine transformation and inverse affine transformation are performed for the fixed matrix. Multiplexer is used to select the encryption option, when the selection line is zero. Consequently, decryption process is performed by this composite S-Box, when the selection line of multiplexer is one. Multiplicative inverse operation is the important operation in composite S-Box. It is very difficult to design. In future, the complexity of multiplicative inverse operation will be reduced to improve the high security and to reduce the area and power utilization of composite S-Box. Also

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

we cannot simplify fixed affine matrix. This is the limitation of this S-Box. In future, this composite S-Box will be designed by reducing the multiplicative inverse operation and affine matrix.

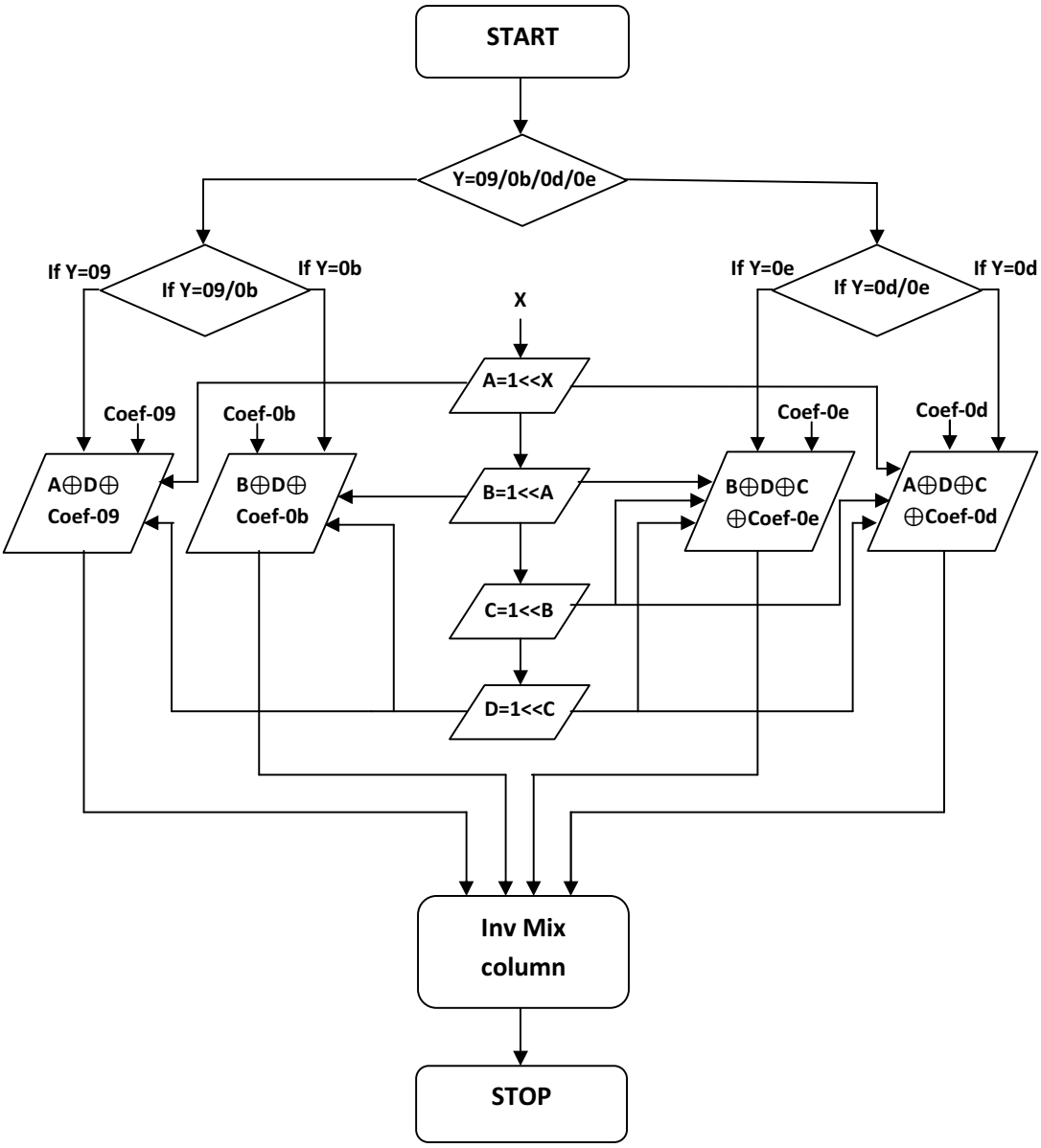

Figure 4 Flow diagram of reduced Inverse MixColumns for AES.

The Fig.4 Shows the flow chart of reduced inverse MixColumns. Initially, from 09, 0b, 0d and 0e structures, any one process is started depends upon the inputs. Every structures corresponding coefficient are generated using the above equation. After that, the inputs and coefficients are processed to perform the inverse MixColumns operation. Here shift and XOR operation are performed to secure the data through substituted value.

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. RESULTS AND DISCUSSION

In this paper, the design of reduced inverse MixColumns with Shrunk Xtime unit is proposed for AES 128-bits process. The proposed AES process offers 5% area reduction, 5 % delay reduction and 4.9% power reduction, when compared to the conventional AES process. Simulation is carried out by ModelSim6.3c and synthesis is carried out by Xilinx10.1. The proposed AES scheme is implemented in FPGA

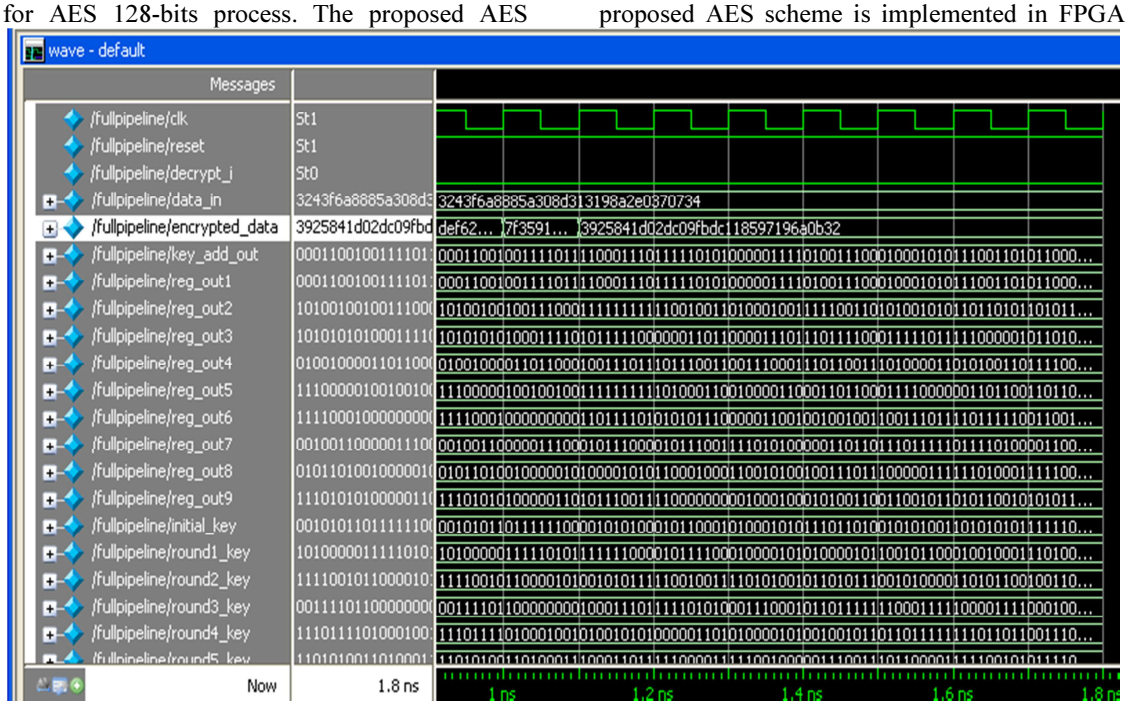

Figure 5 Simulation result of proposed AES encryption process.

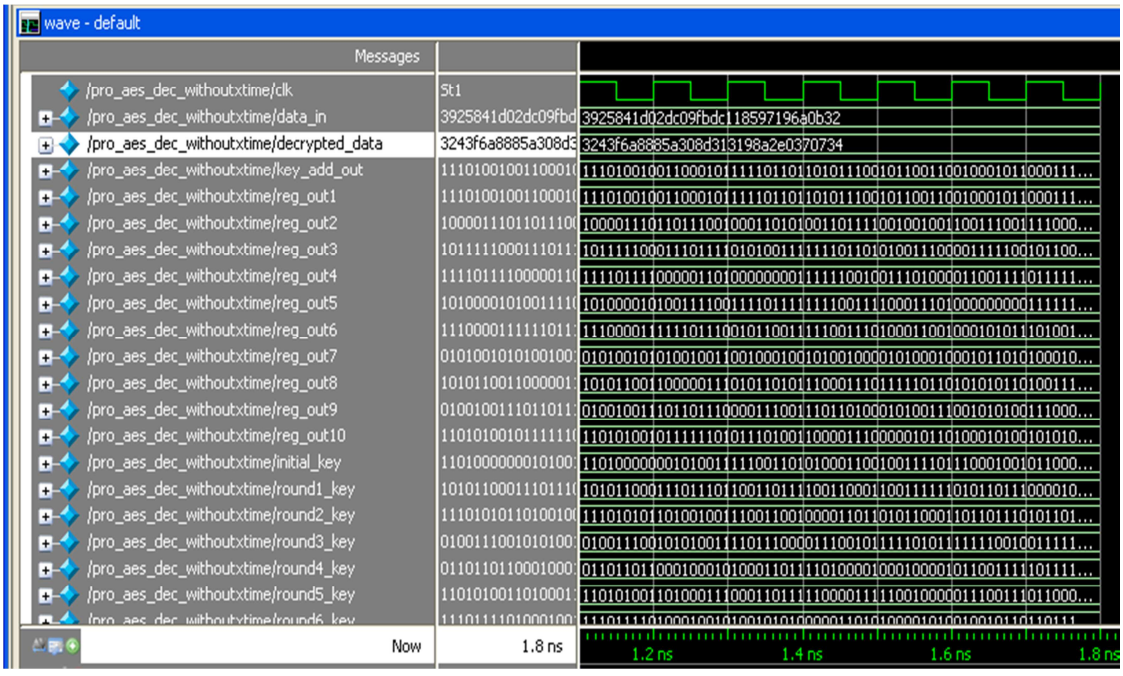

Figure 6 Simulation result of proposed AES decryption process.

Journal of Theoretical and Applied Information Technology
10th December 2014. Vol.70 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Spartan3 to verify this functionality. Figure 5 shows the simulation result of AES encryption process. Active low reset is used in this process. So whenever the reset is high, 128 bit input are encrypted and it is given as iinput for decryption process. Decrypted output is obtained as shown in Figure 6. Original information or data is retrieved in decryption output. The results are tabulated as shown in Table 1.

Table 1 Comparison between existing AES and proposed AES with reduced inverse MixColumns.

AES Decryption	***Slices***	***Frequency (MHz)***	***Power (W)***
Existing AES decryption with X-time based Inverse Mix-Columns	*8685*	*210.194*	*16.819*
Proposed AES decryption with reduced X-time based Inverse Mix-Columns	*8214*	*221.312*	*15.979*

The performances of proposed AES with reduced Xtime over existing AES with regular Xtime are analyzed as shown in Figure 7.

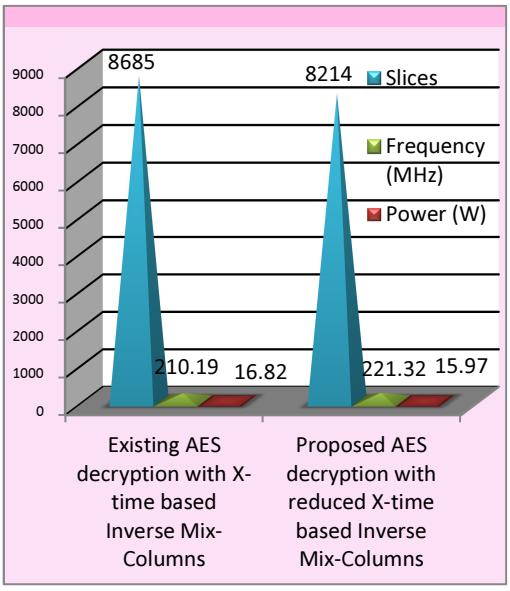

Figure 7 performances of proposed AES over conventional AES process.

The power consumption in case of existing AES with Xtime 16.819W, which is improved to 15.979W using reduced inverse MixColumns with shrunk Xtime, based proposed AES process. The number of occupied slices used in existing AES with Xtime is also reduced. In case of existing AES with Xtime it is 8685 and in reduced inverse MixColumns with shrunk Xtime based proposed AES it is 8214. The frequency utilization incase of existing AES with Xtime 210.194MHz, which is improved to 221.312MHz in proposed AES with reduced inverse MixColumns based on Shrunk Xtime unit.

5. CONCLUSION

In this paper, high speed and area efficient and low power Reduced 09, 0b, 0d and 0e structures is presented. Reduced 09, 0b, 0d and 0e are designed using shrunk Xtime compared to conventional Xtime. These shrunk Xtime is applied in the inverse MixColumns process to analyze the performance. After applying the shrunk Xtime in Inverse MixColumns, Improved Inverse MixColumns is applied to AES process further reduce the area, power and delay. The proposed AES with reduced Inverse MixColumns offers optimized 15% APD (Area=5%, Power = 4.9%, Delay=5%) product than the conventional AES process. This AES can be used in high security applications such as satellite communication techniques, Net Banking and ATM. The proposed Inverse MixColumns with reduced Xtime unit is best for optimum APT product. Further, we cannot reduce this inverse MixColumns. In future, we will try to minimize this Inverse MixColumns to further reduce the area, delay and power of Inverse MixColumns of AES. Also compact composite S-Box technique will be introduced in the AES by reducing the Multiplicative inverse structure or Isomorphic mapping. This will leads to further improve the security.

REFERENCES

[1] Abdelhalim, M.B., Aslan, H. K., Mahmoud, A. and Farouk, H., "A Design for an FPGA Implementation of Rijndael Cipher". ICGST-PDCS Journal, Volume 9, Issue 1, October 2009.

[2] Advanced Encryption Standard (AES), FIPS-197, Nat. Inst. of Standards and Technol., 2001.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[3] Balamurugan, J. and Dr. Logashanmugam, E., "Design of Efficient AES using modified mix-column architecture". International Journal Of Technology And Engineering Science (IJTES), Vol 1(7), pp1054-1059,Oct 2013.

[4] Balamurugan, J. and Dr. Logashanmugam, E., "Design of High Speed and Low Area Masked AES Using Complexity Reduced Mix-Column Architecture". IJCSEC-International Journal of Computer Science and Engineering Communications, Vol.2 Issue.3, May 2014.

[5] Chetna Sangwan, Chetna Bhardwaj, Nisha and Taruna Sikka, "VLSI Implementation of Advanced Encryption Standard". Second International Conference on Advanced Computing & Communication Technologies, IEEE, 2012.

[6] Hodjat, A., Verbauwhede, I., "Area-Throughput Trade-Offs for Fully Pipelined 30 to 70 Gbits/s AES Processors". IEEE Transactions on Computers, vol. 55, 2006, pp.366-372.

[7] Juanli Zeng, Yi Wang, Cheng Xu and Renfa Li, "Improvement on Masked S-box Hardware Implementation", International Conference on Innovations in Information Technology (IIT), IEEE, 2012.

[8] Mathew, S. K., Sheikh, F., Kounavis, M., Gueron, S., Agarwal, A., Hsu, S. K., Kaul, H., Anders, M. A. and R. K. Krishnamurthy, "53 Gbps native GF(24)2 composite-field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors," IEEE J. Solid-State Circuits, vol. 46, no. 4, pp. 767–776, Feb. 2011.

[9] Raneesha K, Rema Vellody and Nandakumar, R., "Hardware Efficiency Comparison of AES Implementations". International Conference on Communication Systems and Network Technologies, IEEE, 2012.

[10] Richa Kumari Sharma, Biradar, S.R. and Singh, B.P., "Shared Architecture for Encryption/Decryption of AES". International Journal of Computer Applications (0975 – 8887), Volume 69–No.18, May 2013.

[11] Senthilkumar, B. and Rajamani, V., "VLSI Implementation of Key Dependent Substitution Box using Error Control Algorithm for Substitution-Permutation Supported Cryptography". Journal of Theoretical and Applied Information Technology (JATIT), Vol. 64 No.1, 10th June 2014.

[12] Siva Ganesh, E., Prof. Velayutham, R. and Dr.D.Manimegalai, "A Secure Software Implementation of Nonlinear AES S-Box with the Enhancement of Biometrics". International Conference on Computing, Electronics and Electrical Technologies [ICCEET], IEEE, 2012.

[13] Sklavos, N., and Koufopavlou, O., "Architectures and VLSI Implementations of the AES-proposal Rijndael," IEEE Transactions on Computers, vol. 51, Issue 12, pp. 1454-1459, 2002.

[14] Xiaona Lv and Liping Xu, "AES encryption algorithm keyless entry system" IEEE, 2012.

[15] Yi Wang and Yajun Ha, "FPGA-Based 40.9-Gbits/s Masked AES with Area Optimization for Storage Area Network". IEEE Transactions on Circuits and Systems—Ii: Express Briefs, Vol. 60, No. 1, January 2013.

[16] Yuan,Z., Wang, Y. , Li, J. , Li, R. , and Zhao, W. , "FPGA based optimization for masked AES implementation," in Proc. IEEE 54th Int. MWSCAS, Seoul, Korea, 2011, pp. 1–4.

[17] Sumio Morioka and Akashi Satoh, "An Optimized S-Box Circuit Architecture for Low Power AES Design". CHES 2002, LNCS 2523, pp. 172–186, 2003.