SoC Implementation of AES 128 bit Algorithm for IEEE 802.16e Mobile WiMax Standards

T. Subha Sri Lakshmi
Asst. Professor, CVR College of Engineering/ECE Department, Hyderabad, India
Email: rupashubha@gmail.com

Abstract: **Wireless Technology plays a very vital role in data transmission process. The most widely used wireless technology standard is IEEE 802.16. Especially the basic standards like Zig-be, Li-Fi, Bluetooth and Wi-Max be the most widely used for connecting point to multipoint networks wirelessly in a secured environment. Security is the main issue of any transmission system in today's world. Many security algorithms were proposed for the MAC layer in Wi-Max but most commonly used is AES (Advanced Encryption Standard) algorithm. In this paper 128-bit AES algorithm is implemented in CTR mode. CTR mode is preferred compared to other modes because it avoids data dependency both in encryption and decryption process. All the Blocks were designed using Verilog HDL, simulated using ncvlog simulator, synthesized in cadence- RTL Complier and finally implemented in Soc Encounter using GPDK 45nm technology libraries.**

Index Terms**: AES Encryption/Decryption, Galois field, CTR mode, RTL Compiler, SoC Encounter.**

I. Introduction

Security is the main issue both in wireless and wired communication. Nowadays wireless communication is growing vast. Broadband Wireless Access (BWA) has been serving enterprises and operators for years, to the great satisfaction of its users. However, the new IP-based standard developed by the IEEE 802.16 is likely to accelerate adoption of the technology. It will expand the scope of usage i.e., the possibility of operating in licensed and unlicensed frequency bands and unique performance under Non-Line-of-Sight (NLOS) conditions. The most important features of Wi-MAX are Quality of Service (QoS) for real time video conferencing and orthogonal frequency division multiplexing in physical layer of Wi-MAX. Design similar to OSI model, Wi-MAX [2] uses two layers namely, physical layer and data link layer. MAC layer in Wi-MAX is nothing but data link layer in OSI model and is connection-oriented [2]. MAC layer mainly consists of three sub layer MAC CS, MAC SAP and MAC Common Part Sub Layer (MAC CPS) [3]. The main requirement of end user being the security of data and that service provider to view unauthorized network access. To solve many security issues, many protocols like wired equipment protocol (WEP), Li-Fi, Zig-be, Bluetooth and finally AES. WEP was widely used till 2009 but was broken by brute force attacks. Finally, Rijndael AES which assures more reliable and data authentication remains to be the main security issues which were offered by Rijndael AES in counter mode with Cipher Block Chaining (CBC- MAC) mode.

II. Wi-Max Layer Security

The link between upper layers and MAC layers used in Wi-MAX [1, 8] standard is shown in Figure 1**.** The security issues are handled in these layers. Being the core part of IEEE 802.16e, MAC-CPS defines all the processes required for the proper transmission such as bandwidth requirements, connection establishment and management. The connection between the MAC CPS and convergence sub layer (CS) is established by MAC service access point (MAC SAP). SAP also does other functions like carrying out the communication process, connection and transportation of data over the channel. Encryption and Decryption process are performed by privacy sub layer by receiving the data from higher layers. Processes like authentication and secure key exchange between base station and subscriber station are also performed by security sub layer [3, 5]. Encapsulation and privacy key management are two set of protocols required for the smooth condition of the processes performed by security sub layer.

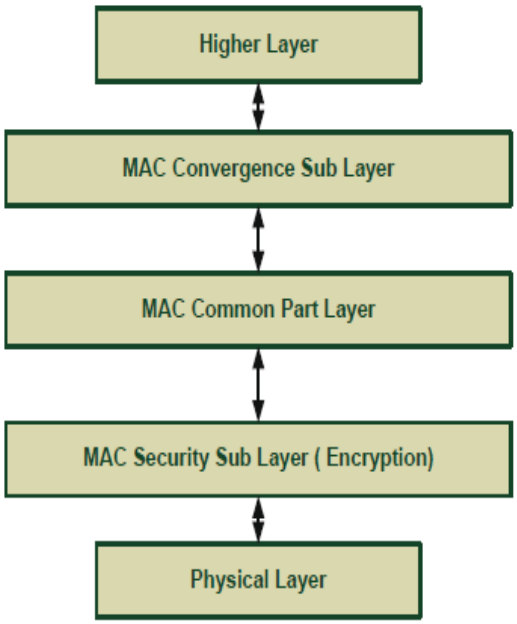

Figure.1. Overview of MAC layer

The process of sending the data packets across the fixed Broadband Wireless Access (BWA) is done by encapsulation protocol which also gives conditional access by the main station. The privacy key management mainly has two versions: PKM1 and PKM2 used in mutual

authentications. To refresh the key between main station and subscriber station is provided by PKM protocol. Traffic encryption keys (TEKs) are exchanged to secure subsequent PKM which is shared secretly. [8]

III. Advanced Encryption Standard

AES encryption and decryption [4] use same private key so it is called as symmetric key block cipher algorithm. For instance, if the block size is 128-bit i.e., it contains 128-bit information. Here, the input for encryption is the plaintext and output is cipher text which is generated by using ciphers and for decryption it is vice-versa. In this different sizes of keys are used depending upon the number of rounds for data abstractions which are required. The different sizes of keys used in AES are 128, 192 and 256 keys for 10, 12 and 14 rounds respectively [4]. Unlike DES, the entire block is used for each round of operations.

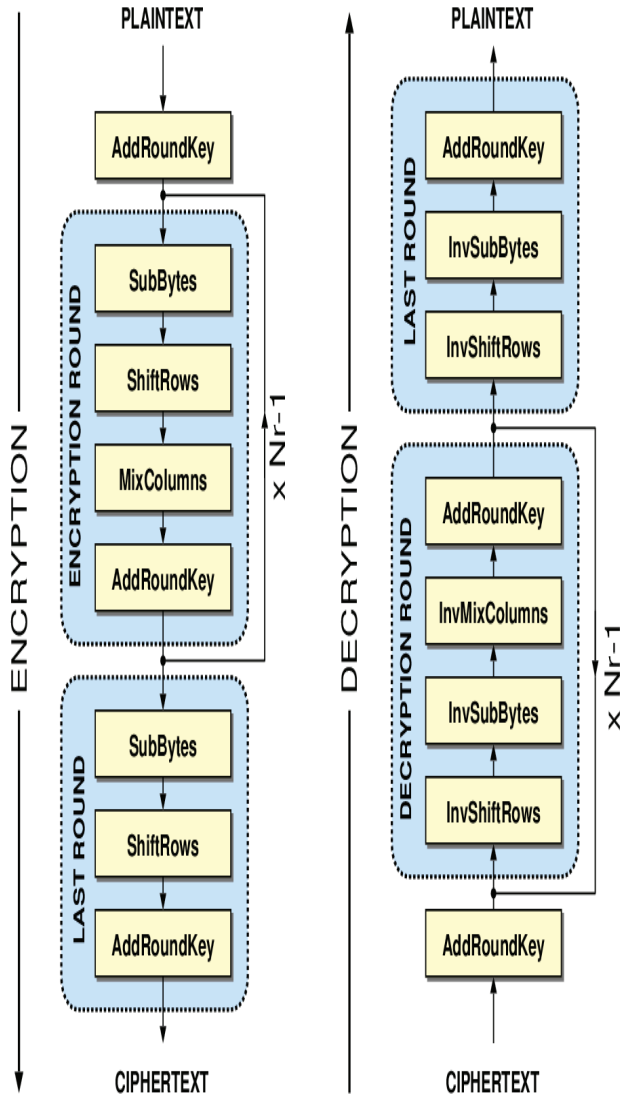

Figure.2. AES Encryption & Decryption Process

Rijndael AES algorithm [9] consists of four operations namely Sub Byte Transformation, Shift Row Transformation, Mix Column Transformation and Add Round Key in encryption. In decryption, the same operations are but each of the above operation takes its inverse form. For both encryption and decryption, key expansion units are used to generate ten different keys for ten rounds in the case of 128 bit. In every round a new key is generated from the previous key with the help of a key matrix and the primary key is referred as cipher. In this paper, AES is designed for 128 and 256 bit keys with 10 and 14 rounds of operations respectively [6]. In the first round, Add Round Key operation is solely performed and in the last round, all the operations except Mix column Transformation are performed in both encryption and decryption. The complete process AES encryption and decryption is explained briefly in the form of a flow chart as shown in Figure.2.

A. Sub Byte Transformation

The most important in Sub Byte Transformation is the S-Box. In this operation, the input byte is considered to be one of the elements of Galios field. The S-Box is implemented by passing the given input through multiplicative inverse and then affine transform. For performing this transformation all the S-Box values will be available well before hand and store in the memory. The 128 bit data is presented in 4*4 matrixes in byte format where in the mappings to S-Box replaces the original data byte [6, 7]. The mappings to S-Box are as shown in Figure 3(a).

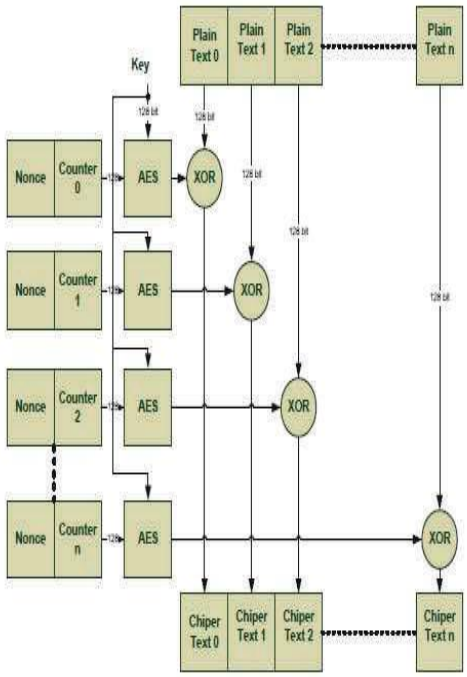

Figure.3 (a). Mapping to S Box

B. Shift Row Transformation

As its name suggests, the shift row transformation is done on 4*4 matrix row by row. In encryption the shift is towards left and the change in position of bytes depends on the row number. Elements in 0^{th} row will not be shifted but in 1^{st}, 2^{nd}, 3^{rd} rows, the elements are shifted by 1,2 and 3 times respectively. The shift row operation in encryption

performed as shown in Figure. 3(b).For decryption the shift takes place towards right [6].

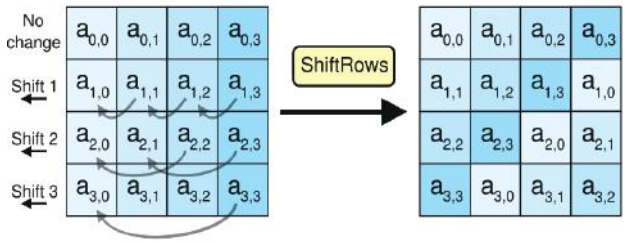

Figure.3 (b). Shift Row Transformation Process

C. Mix Column Transformation

Mix Column Transformation operation is one of the most power consuming operation in which the multiplication is carried out by galios field by inter byte mixing. Here, a constant 4*4 matrix is used for forward operation and another for reverse operation as shown in Figure.3(c). [6,7]

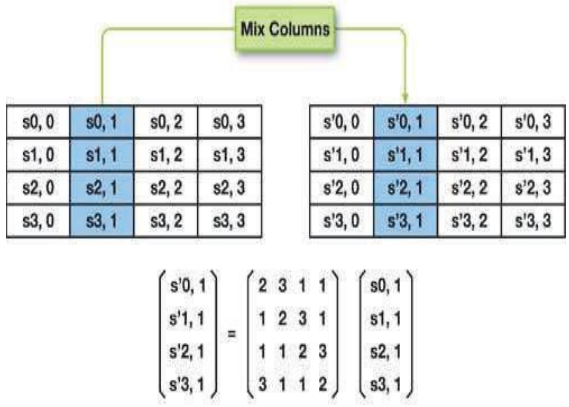

Figure.3(b). Mix Column Transformation Process

D. Add Round Key

In this operation, the Mix Column is XORed with the cipher key that is updated in each round using key expansion procedure to produce another 4*4 matrix and the output is given to next round [6] as shown in Figure. 3(d).

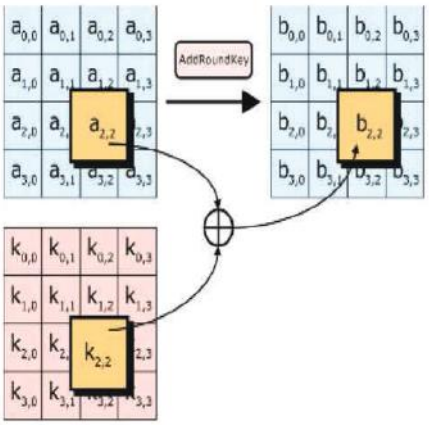

Figure.3 (d). XORed Operation Process Structure

E. Key Expansion

This unit takes a 128 bit cipher key, and perform a key expansion routine and generates a key schedule for every round. This unit contains Subword, Rotword and Rcon (i) where i represents round number. In every round Rcon (i) value is assigned and processed. In Subword operation, SubByte Transformation is applied to the word in that column. The function Rotword rotates the elements in the column by one shift from bottom to top. Then the byte is XORed with Rcon (i) to produce the corresponding column for the next round.

IV. AES Modes Of Operation

AES block cipher can be implemented in different modes of operation based on several implementation issues. Electronic Code Book (ECB), Cipher Feedback (CFB), Output Feedback (OFB), and counter (CTR) are the different types of modes in which AES operates for security purposes. In this paper, especially AES algorithm is implemented in CTR mode [9]. Data dependency of Cipher Block Chaining mode is avoided in the counter mode with the value of counter increasing by one in encryption and the same counter sequences are maintained in decryption process on the receiver side.

A. AES in CTR Mode

Prior to the encryption of plaintext, an arbitrary block called nonce and counter is encrypted, and then the result is XORed with plaintext to create cipher text. Due to the involvement of counter in encryption, the cipher block is not the same even if we have same plaintext. Due to non-linear concept of S-Box this mode avoids the attackers from predicting the patterns of repetition in cipher text. Further, this mode is more suitable for parallel encryption of various blocks. All these advantages make AES [4, 9] CTR mode be the best choice for AES implementation. The AES CTR model is same as shown in Figure.3 (a).

V. Implementation & Results

All the blocks are implemented using ASIC Cadence SoC Encounter [10] Tool with 45nm technology libraries. Figure.4 shows RTL Schematic of AES top module (which includes both encryption and decryption). Figure.5 shows RTL schematic of core structure of AES. Figure.6 shows RTL schematic of Encipher block, Figure.7 shows RTL schematic Decipher block. The timing of AES module with positive slack is 650ns. Figure. 8 shows the net power usage of AES. Table I and Table II, give the pre & post clock tree synthesis report in terms of nano seconds when routing is performed before special route and after nano route process. Finally, Figure.9 shows the IC chip Fabrication Layout structure which is named as GDS II file of AES top module.

Language Used - Verilog HDL
Simulator Tool - Ncvlog
Synthesis Tool - RTL Compiler
Implementation (Back-End Process) - SoC Encounter
Power Analysis n terms of nano watts

a) Internal Power - 0.650 (50%)
b) Switching Power - 0.62 (48%)
c) Leakage Power - 0.0006 (0.5%)

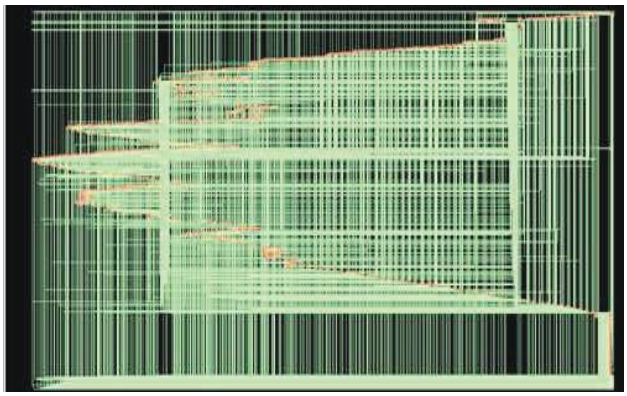

Figure. 4 RTL Schematic of AES Top Module

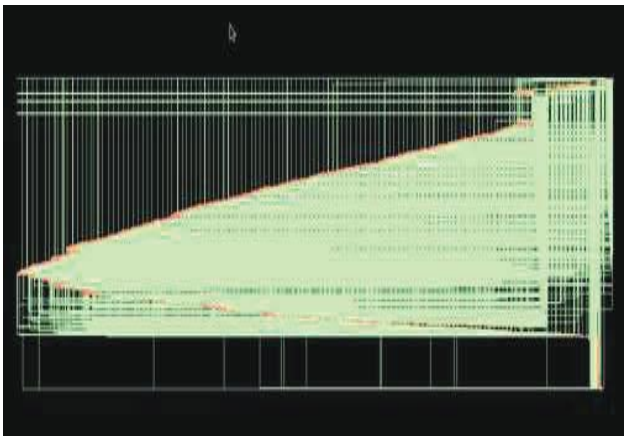

Figure. 5 RTL Schematic of AES Core Structure

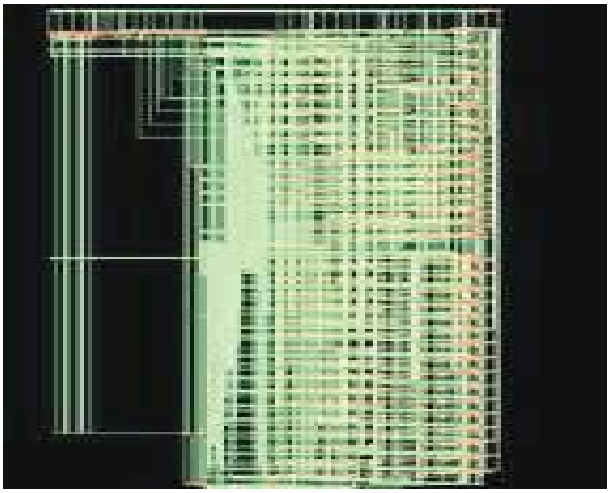

Figure. 6 RTL Schematic of AES Encipher Block

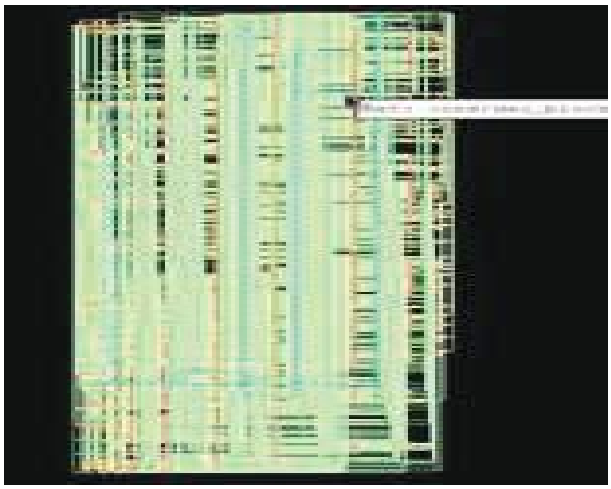

Figure.7 RTL Schematic of AES Decipher Block

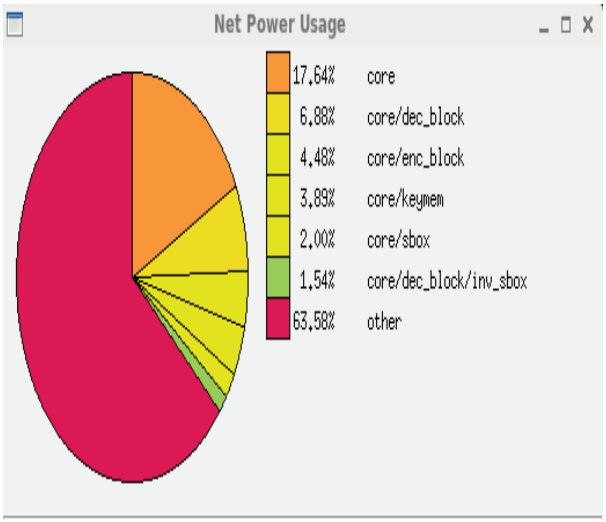

Figure. 8. Net Power Usage

TABLE I
PRE CLOCK TREE SYSTHESIS REPORT

Setup mode	all	reg2reg	default
WNS (ns):	0.464	0.464	5.894
TNS (ns):	0.000	0.000	0.000
Violating Paths:	0	0	0
All Paths:	2942	1071	1872

TABLE II
POST CLOCK TREE SYNTHESIS REPORT

Setup mode	all	reg2reg	default
WNS (ns):	0.390	0.390	5.713
TNS (ns):	0.000	0.000	0.000
Violating Paths:	0	0	0
All Paths:	2942	1071	1872

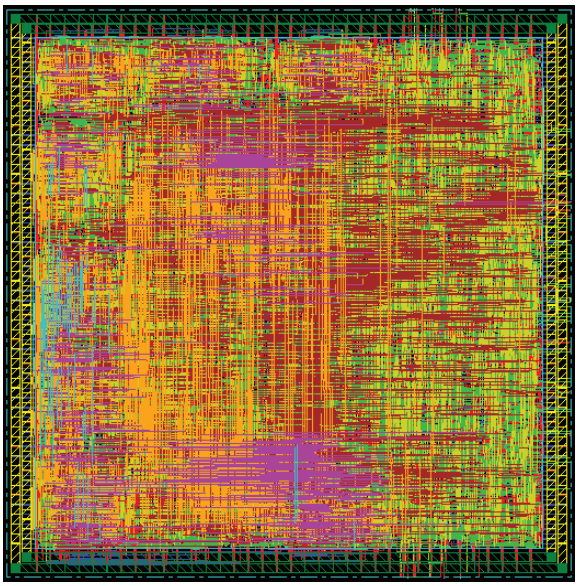

Figure. 9. GDS II of AES Top Module

VI. CONCLUSIONS

All the blocks are verified by ncvlog simulator and synthesis by using RTL complier and finally implemented in SoC Encounter and IC chip layout is obtained i.e., GDS II file. The top module consist of encipher and decipher blocks which is further designed by using inverse S-Box. The main advantage of AES algorithm in counter modes is, it consumes very less power as shown in figure 8 and as well as area occupancy on IC is also very less. These features play a prominent role for portable devices and have advanced improvements for Mobile Wi-MAX devices.

REFERENCES

[1] Dadhich,R.,Narang,G. and Yadav, D.M (2012) Analysis and Literature Review of IEEE 802.16e (Mobile Wi-MAX) security. International Journal of Engineering and Advanced Technology, 1,167-173.

[2] Khan, A.S., Fisal, N., Maqbool, W., Ullah, R. and Sardar, H. (2014) Secure Authentication and key Management Protocols for Mobile Multichip WiMAX Networks. Indian Journal of Science and Techology,7,282-295.

[3] Hasan, J. (2006) Security issues of IEEE 802.16 (WiMAX).4th Australian Information Security Management Confernece, Perth, 5 December 2006.

[4] FIPPUB197 (2001) Advanced Encryption Standard (AES). November 2001.

[5] Rajeeth, K.D., Alukaidey, T., Salman. K.and Alzaabi, M.(2013) Security Algorithm for WiMAX. International Journal of Network Security and its applications.

[6] Willam Stallings (2008) Cryptography and Network Security. 5th addition Prelitce Hall, Pearson Education, USA.

[7] Tshering, F. and Sardana, A. (2011) A review of privacy and Key Management Protocol in IEEE 802.16e. International Journal of Computer Applications,20,25-31.

[8] Mohamed, M.A., Zaki, F.W and El-Mohandes,A.M (2012) Novel fast Encryption Algorithm for Multimedia Transmission over Mobile WiMax Networks. International Journal of Computer Science,9,60

[9] Litochevski, M. and Dongjum, L. (2012) High Throughout and Low Area AES: Core Specifications, Opencores,1-9.

[10] Prof.Micea Stan, Cadence SoC Encounter, University of Virginia.