Circuits and Systems, 2016, 7, 371-380
Published Online April 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.74032

Scientific Research Publishing

Efficient FPGA Implementation of AES 128 Bit for IEEE 802.16e Mobile WiMax Standards

P. Rajasekar[1], Dr. H. Mangalam[2]

[1]Department of Electronics and Communication Engineering, Kathir College of Engineering, Coimbatore, India
[2]Department of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India
Email: rajasekarkpr@gmail.com, hmangalam2@gmail.com

Received 14 March 2016; accepted 25 April 2016; published 28 April 2016

Abstract

In the present era of high speed communication, wireless technology plays a predominant role in data transmission. In the timeline of wireless domain, Wi-Fi, Bluetooth, ZigBee are some of the standards used in today's wireless medium. In addition, WiMax is introduced by IEEE as IEEE 802.16 standard for long distance communication, and mobile WiMax as 802.16e. WiMax is an acronym of worldwide interoperability for microwave access. It helps to provide wireless transmission with high quality of service in a secured environment. Privacy across the network and access control is the predominant goal in the wireless protocol. In the wireless environment one of the most widely used security algorithms in MAC layer is Advanced Encryption Standard (AES). Especially Medium Access Control (MAC) sub layer should be evaluated in the security architecture. AES is used in the MAC layer that consumes more power and involves high cost. So, in this paper an optimized architecture of AES 128 bit counter mode security algorithm for MAC layer of 802.16e standard is proposed. The SBOX and MixColumn transformation are modified in the architecture of AES to achieve optimized power and delay. The design has been implemented in Xilinx virtex5 device and power has been analyzed using XPower analyzer. It is compared with two standard existing architectures. The simulation results revealed a power reduction of 41% compared to existing one.

Keywords

AES Encryption/Decryption, Galois Field, Low Power Architecture, Electronic Code Book Mode, FPGA Implementation

How to cite this paper: Rajasekar, P. and Mangalam, Dr.H. (2016) Efficient FPGA Implementation of AES 128 Bit for IEEE 802.16e Mobile WiMax Standards. *Circuits and Systems*, **7**, 371-380. http://dx.doi.org/10.4236/cs.2016.74032

1. Introduction

It is evident that the wireless system uses the open type radio channel; it requires more security in order to protect the integrity and traffic confidentiality, and also to put off different network security attacks: denial of service and brute force attacks. In particularly, WiMax communication system needs more security because of open environment. It is generally called as last mile transmission for wireless systems as it is used for long distance communication around 50 Km. Initially IEEE 802.16 standard was planned to give up the access of data in the range of 30 Km to 50 Km with the line of sight communication. This wireless standard has various sub standards, depends upon the frequency range and modulation schemes used. It is designed to facilitate wireless internet service provider (WISP)'s backhaul, WIFI mesh networks, broadband internet connectivity to proprietary, but nowadays it is extended to end user model. It is also featured with quality of service (QoS) for real-time video conferencing, voice, and video services up to 280 Mbps per substation. In addition, an orthogonal frequency division multiplexing (OFDM) is used in WiMax. In the design perspective view of OSI model, it uses two layers: physical link layer and data link layer. The data link layer is named as MAC layer. This 802.16 MAC is connection-oriented, which is designed for point to multi-point wireless access applications in broadband. The 802.16 MAC layer is well defined protocol stock over the OSI model [1].

Meanwhile, this standard is made up of a properly defined protocol stack. Three sub layers are defined in MAC layer; the privacy sub layer/security sub layer (PS), MAC Common Part Sub layer (MAC CPS), and Service Specific Convergence Sub layer (MAC CS). The MAC CS sub layer is to converse with higher layers and transforms upper level data services to MAC layer flows and associations. In addition, the MAC CS is divided into two layers: packet convergence sub layer for packet data services and Asynchronous Transfer Mode (ATM) convergence sub layer for ATM networks. From the end users' perspective, privacy and data integrity are the primary security concerns, whereas in service provider's view unauthorized network access is to be prevented. In our design we concentrate on the security issues in MAC layer of WiMax protocol for both end users and service provider [2].

In wireless networks, there are so many network protocols which are used to protect the data confidentiality between the sender and the receiver. Till 2009, Wired Equivalent Privacy (WEP) protocol has been the widely used security tool for protecting the information in wireless media transmission. However, this WEP was broken in 2009. Based on this attack model, today there exist varieties of programs and tools that can be used to break the WEP protocol in few seconds. This leads to search for a new efficient algorithm or protocol that assures reliable and secured data transmission in wireless environment. Under these circumstances, Rijndael AES in Counter with Cipher Block Chaining (CBC)-MAC mode has become most assuring solution for achieving security in wireless networks. Especially we use this method in WiMax. This AES mode offers two services in security issues, namely, encryption and data authentication. In our paper, we analyzed the power and delayed efficient AES Counter Mode (AES CTR) architecture for MAC layer.

This paper is organized as follows: Section 2 describes the related works. Section 3 describes the Mathematical WiMax layer security. Section 5 describes Advanced Encryption standard. Section 5 discusses AES CTR mode and MAC protocol implementation. Section 6 gives the simulation results and Section 7 Discussion and Conclusion.

2. Related Works

M.H. Rais, S.M. Qasim (2009) discussed the efficient hardware design and FPGA implementation of 128 bit AES using residue prime number based design. In their paper, they analyzed the various hardware models of AES [3]. The high speed, high throughput AES 128 bit architecture has been discussed by C.P Fan, J.K. Hwang (2008). In this design the content addressable memory based SBox has been implemented with pipeline structure which takes the minimum delay compare with other design [4]. H. Samiee, R. E. Atani, H. Amindavar (2011) designed a novel area throughput optimized architecture for AES algorithm. They concentrated normal basis composite field arithmetic architecture model in their architecture [5]. A fully pipelined structure of high speed AES processor has been designed by Alireza Hodjat and Ingrid Verbauwhede (2004), which takes 21.5 Gbps throughput speed [6]. In application based implementation, J. Daemen V. Rijmen (1998) proposed the block cipher Rijndael for smart card application [7]. The literature survey of various wireless security design is done by GeetikaNarang, D. M. Yadav Reena Dadhich (2012) [8].

K.D. Ranjeeth, *et al*. (2012) elaborates WiMax structure and security issues in their paper. In their paper, they

mentioned the different security algorithms used in WiMax MAC layer [9]. N. Yu and H.M. Heys (2005) discussed the compact hardware implementation of AES. Here, the design has been discussed as efficient hardware structure for AES [10]. Claudia Feregrino-Uribe *et al*. addressed the privacy key management of WiMax MAC layer [11].

3. WiMax Layer Security

The brief model of MAC layer is shown in **Figure 1**, which shows the link between upper layers to physical layer used in WiMax standard. These layers are designed to handle the security issues in WiMax standards. The MAC Common Part sub layer (CPS) is the core part of the IEEE 802.16, which defines all methods for bandwidth distribution, request and grant, system access procedure, connection management, uplink scheduling, connection control, and automatic repeat request.

MAC Service Access Point (MAC SAP) is used to maintain the communication between the MAC CPS and Convergence Sub layer (CS). Further, this communication process, the creation, modification, deletion of connection, and transportation of data over the channel are carried out by SAP [11].

The data encryption and decryption process are done by the privacy (security) sub layer, where the data is taken to higher layer for encryption operation, and decryption process data is sent to higher layer. The privacy sub layer is also used for authentication and secure key exchange between the base stations and subscriber station [12].

To achieve this, two set of protocols; encapsulation, Privacy Key Management (PKM) protocols are used in the security sub layer for an encrypting a data and for handling secure key distribution from base station to subscriber station. The encapsulation protocol sends the encrypting data packet across the fixed Broadband Wireless Access (BWA). It also gives a enforcing conditional access by the base station. Two versions of PKM namely PKMv1 is used in unilateral, and PKMv2 in mutual authentications.

In addition periodic supports are given for re-authorization/re-authentication and key refresh between base stations to subscriber station. These PKM protocols establish a secret authorization between the base station and subscriber station. The shared secret is then used to secure subsequent PKM exchanges of Traffic Encryption Keys (TEKs). In general the implementation of PKM protocol, normally uses X.509 digital certificates, RSA algorithm, and strong encryption algorithm to carry out key exchanges between subscriber station and base station. Further for security enhancement, stronger unbreakable security methods such as AES are used IEEE 802.1 6 MAC [13].

This security sub layer also known as privacy sub layer provides access control and confidentiality of the data link. Furthermore the Security Association (SA) is identified by SAID which contains encryption algorithm/ decryption algorithm and Security Info such as key, Initialization Vector (IV) for AES.

The IEEE 802.16e-2005 standard has specified security mechanisms, using the AES-CCM algorithm to provide better security services. Although this method requires more number of operations, several iterations, and multiple processes for execution, it offers best security. In this work, proposed hardware architectures are based on the AES-CCM, incorporating parallelization and modular specialization, and reducing critical path without increasing the execution latency.

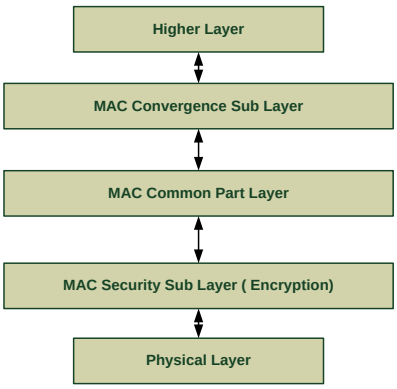

Figure 1. Overview of MAC layer.

For the privacy and authentication process, two different security algorithms are used in IEEE 802.16e. But, if we use the AES, these two security mechanisms can be handled easily in single algorithm. To obtain above security, AES is used in Counter (CTR) mode and Cipher Block Chaining-Message Authentication Code (CBC-MAC) mode. The advantages of counter mode and CBC mode are as follows. AES CTR mode ensures uniqueness of the message. The authentication is performed by the AES algorithm in CBC-MAC mode and provides additional capabilities; CBC-MAC is an integrity method that ensures that every cipher block depends on every preceding part of the plain text, where ciphering two identical blocks results in different cipher blocks [13].

4. Advanced Encryption Standard

AES is a symmetry key block cipher cryptography algorithm, which means it uses the same secret key for both encryption and decryption, and the operation is carried out by the block. The block contains 128 bit data information. For encryption process, the plain text is input and cipher text is output where as in decryption it is reverse. In AES, we use different size of keys depending upon the round used in AES operation. It uses 128,192,256 key bits for 10, 12, 14 rounds [14] [15].

Unlike the DES, AES uses entire block for each round of operation. In DES, fisetal structure uses half of the block for each round of encryption. To implement the AES, each round of operation is divided into four functional modules, namely AddRoundKey (ARK), SubByte Transformation (SBOX), MixColumnTransformation (MCT), and ShiftRow (SR), whereas Decryption operation, They are replaced by its inverse module as inverse SubByte transform (InvSBOX) and Inverse MixColumn (InvMCT), Inverse ShiftRow (InvSR). For both encryption and decryption operations, key expansion units are used to generate ten different keys for ten rounds. In each round, the new key has been derived from previous round key with the help of key expansion unit. For all of these operations inputs are assigned as state array matrix. In Rijndael AES, it uses only 128 bit key and 10 round operations [14] [15]. In this paper, we proposed optimized MAC security layer using Rijndael AES. This is shown in **Figure 2**.

4.1. SubByte Transform

This is the non linear transformation, which consumes more power and more delay .In the SBOX operation, the input byte is considered as an element of Galois Field (2^8). To implement the SBOX, the given input is passed through two stages, namely multiplicative inverse and an affine transform. For this operation, either all the SBOX value will be pre calculated and stored in the memory or combinational logic equation is used as on fly calculation. Here, the 128 bit input data are being treated as byte format of 4 × 4 matrix [14] [15].

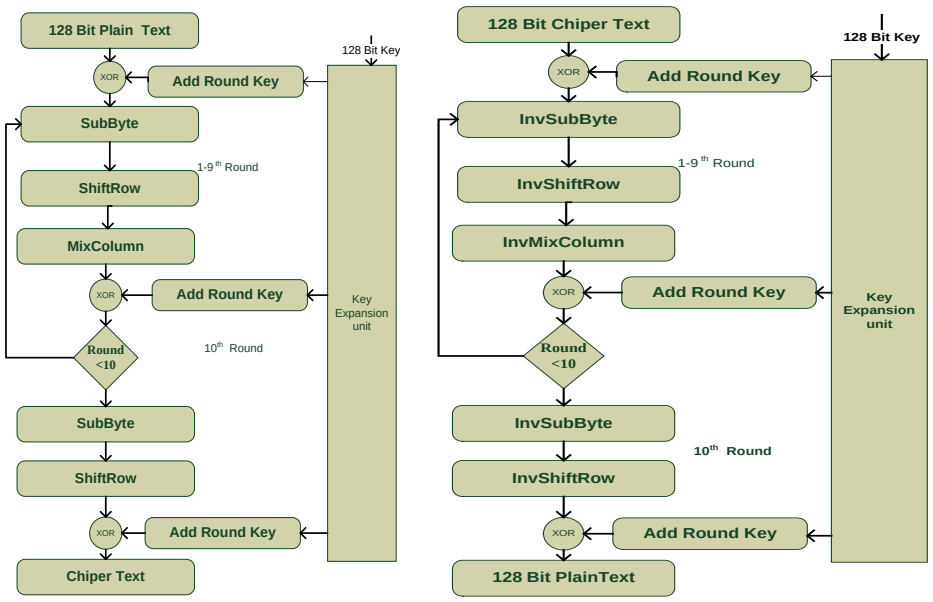

Figure 2. AES encryption and decryption.

4.2. MixColumn Transformation

MixColumn operation is also one of the power consuming nonlinear operation blocks because multiplication is carried out by Galois field (GF) by inter byte mixing. In this operation, we use the constant 4 × 4 matrix for forward operation and another one for inverse operation. The column value is treated as the polynomial function as the polynomial modulo $X^4 + 1$ with the coefficient in $GF(2^2)$ [14] [15].

4.3. ShiftRow Transformation

The ShiftRow operation is carried out row by row, incorporating a change in position of each byte in each row. That is there is no shift or position change of bytes in 0^{th} row. But in 1^{st}, 2^{nd}, 3^{rd} of each byte is shifted by 1, 2 & 3 times respectively. This is the simple operation but is also one of the shuffling operations that increases the complexity of AES rounds [14] [15].

4.4. AddRoundKey

In an addition of a round key to the state, XOR operation of MixColumn output and key expansion unit output is carried out. For each round, key has been generated as per key expansion procedure [14] [15].

4.5. Key Expansion

Key expansion unit takes 128 bit Cipher Key, and performs a Key Expansion routine to generate a key schedule for each round. The key expansion unit contains the Subword(), Rootword(), RCon(i), i, represents the round number. In each round, Rcon(i) value is assigned and processed it. In sub word operation, sub byte transformation operation that produces an output word. The function RotWord() gets a word in the format of $a_0a_1a_2a_3$ as input, which performs a cyclic permutation, and returns the word in the format of a_1, a_2, a_3, a_0 [14] [15].

5. Modes of Operation

AES block cipher can be implemented in different modes of operation based on their requirement such as complexity, authentication factors, and implementation issues. The different modes used for enhancing security and minimizing cryptanalysis attacks are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feed Back (CFB), Output Feed Back (OFB), and Counter (CTR). In our design we use counter mode to enhance the security in MAC layer of 802.16e standard for WiMax

The CTR mode avoids the data dependency of the Cipher block chaining mode; the value of the counter sequence is incremented by one in encryption. But in decryption process, the receiver maintains the same counter sequences. It is very difficult task to maintain against the differential cryptanalysis attack.

5.1. AES in CTR Mode

In AES-CTR mode, before encrypting the plaintext, we use the AES algorithm to encrypt an arbitrary block called as the nonce and counter, then XOR the result with plaintext to create the cipher text. The nonce contains the random number and counter block. The same nonce is used for the entire 128 bit AES block; whereas counter value is incremented by one in each block. The number of block depends as length of the MAC payload [16]. The cipher block is not identical even if we have same plain text. This is because of the counter involves in encryption. The output cipher gets more diffusion, due to SBOX's non linearity concept, thus preventing the attackers from observing patterns of repetition in the cipher text. AES-CTR has the advantage of making the decryption process exactly the same as encryption, since XORing the same value twice produces the original value, thereby simplifying the implementation. Furthermore, AES-CTR is also suitable for parallel encryption of several blocks. These advantages make AES-CTR algorithm a popular choice for AES implementation. In this paper, modified AES counter mode is adapted. It uses the modified SBOX [17] [18] and modified MixColumn Transformation (MCT) [19]. The block diagram model is shown in **Figure 3**.

5.2. MAC Protocol Implementation

This modified AES CTR is in the MAC protocol. **Figure 4** shows the MAC implementation using modified

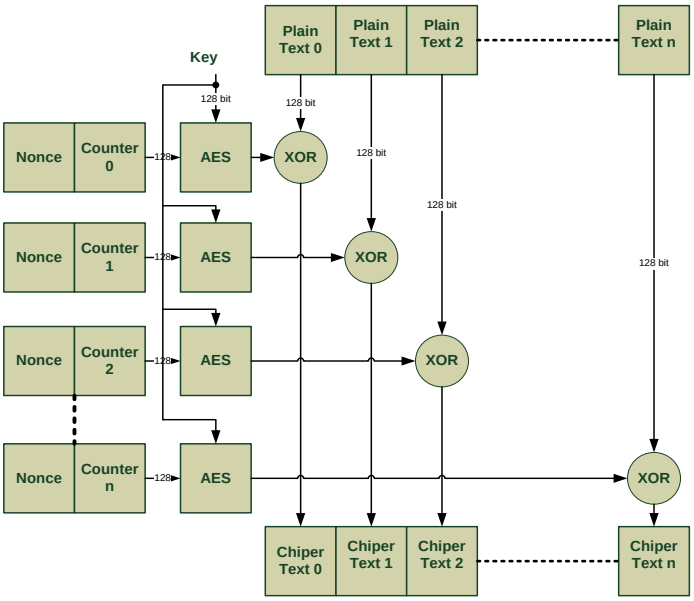

Figure 3. AES counter mode.

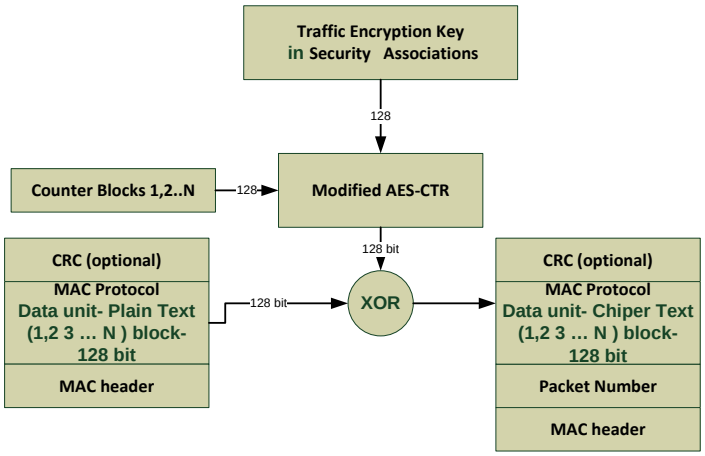

Figure 4. MAC protocol implementation.

AES CTR. CBC mode is used for obtaining the message authentication code. For this, the plain text is extracted from the MAC payload. After that we apply encryption operation using AES CTR algorithm with 128 bit TEK. Now the resultant cipher text is an encrypted version of authentication code. The resultant cipher text is transmitted. In the receiver end both encrypted message and authentication message are decrypted using reverse process. Now the receiver will compare the received message and authentication code. It checks whether they are identical. If identical the message is accepted otherwise discarded [20].

6. Simulation/Synthesis Result

The proposed architecture is simulated using Xilinx 14.1 project navigator tool and synthesized using Xilinx VIRTEX devices xc5vsx50t-ff1136-3, xc5vlx50t ff1136-1, xc5vlx50t-1 lfgg900, xc6slx150l-ff1136-1 xc6slx-150l-1 lfgg900. For the proposed architecture model, the simulation waveform of encryption model is shown in **Figure 5**. In this **Figure 5**, the waveform shows that the list of input and output parameters of AES CTR mode. The encryption or decryption process are started when the load signal is active *i.e.* "1". The design has been proposed as asynchronous reset which controls the process of AES encryption at any time irrespective of clock signal. The 128 bit of key and 128 bit data are loaded while the load signal is an active. In every round the inner

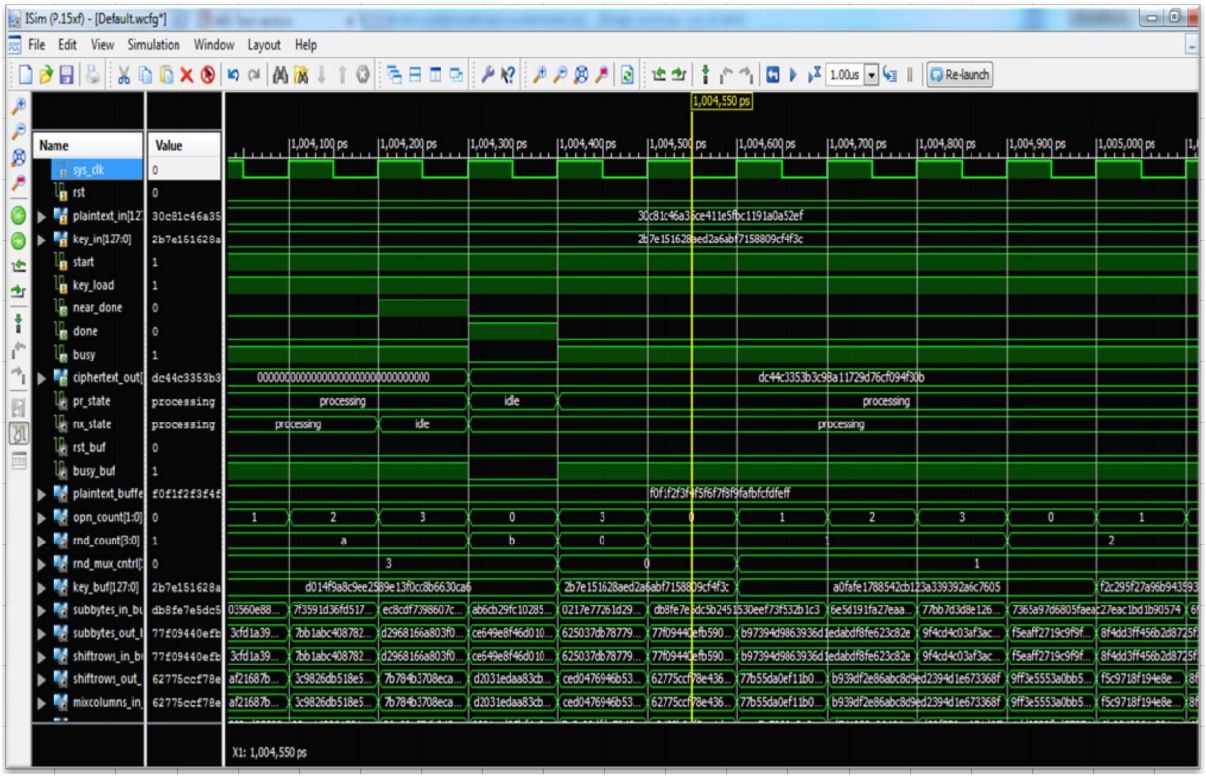

Figure 5. Rijndael AES 128 CTR mode encryption.

round counter will be reset and used to generate the key for next round. The process done infers to validate the cipher output. In intermediate round, the SBOX, MCT, ARK and SR are verified using theses intermediate round signal which are all shown in the **Figure 5**.

It can be observed from **Table 1**, the delay total power of various Xilinx devices. The comparison of power, delay, and clock frequency of different devices are shown in **Table 1**. The device xc5vsx50t-ff1136,-3 operates the clock frequency of 144.071 MHz but it consumes too much power as 1248.02 mw. At the same time device xc6slx150l-1 lfgg900 consumes total power 313.26 mw, but clock frequency 35.363 MHz. From these we conclude that high throughput takes high power and low throughput consumes low power. It is observed that from **Table 1**, device xc5vlx50t-1 lfgg900 is optimized in terms of both power and clock frequency. This value is compared with the reference design. The number of slice LUT also analyzed here which takes optimum value. The optimum value of slice LUT is 1947.

The **Table 2** shows that the comparison of various parameters of the proposed system to the reference design. The power consumption of encryption module is an important to in mobile devices. From the **Table 2**, the power has been reduced as much as of 41% compared with the reference designs. Further analysis, this shows number of slice and LUT as minimized 80% against reference design [21], and minimized 40% by reference design [22]. This provides an area optimization in mobile handheld devices. The second analysis, we discussed the signal power, logic power, and clock power comparison with the reference design, which shows that the design has been improved in minimizing power of 18%, 43%, 10% respectively.

Figure 6 shows that the power comparisons graph of proposed architecture with reference architectural model. We observed that both total and quiescent powers are low compared with reference design. The no of slice resource, no of slice LUT and no of IOB utilization are also shown in **Figure 7** for comparison.

The **Figure 8** shows that the Xilinx XPower analysis report of proposed system whereas **Figure 9** shows the detailed power analysis and consumption result of proposed architecture. In our proposed architecture

7. Discussion and Conclusion

The proposed architecture model of AES128 CTR mode cryptography algorithm is implemented in MAC layer

Table 1. Comparison of resources, power, and delay and clock frequency for proposed Rijndael AES 128 in various Xilinx devices.

Device	Clock Frequency (MHz)	Total Power (mw)	Static Power/ Quiescent (mw)	Dynamic Power (mw)	Logic Power (mw)	Clock Power (mw)	No of Slice	No of Slice LUT	Max Delay (ns)
xc5vsx50t-ff1136-3	144.071	1248.02	1080.81	167.21	39.72	43.70	874	1853	1.731
xc5vlx50t ff1136-1	128.849	876.29	722.06	154.23	39.06	38.73	837	1852	1.549
xc5vlx50t-1 lfgg900	133.743	814.67	722.06	92.61	20.04	32.16	955	1947	1.531
xc6slx150l-ff1136-1	53.084	355.67	269.51	86.17	32.35	8.63	679	2939	3.507
xc6slx150l-1 lfgg900	35.363	313.26	269.51	43.75	16.14	5.09	1124	2856	3.621

Table 2. Comparison of Rijndael AES 128 CTR mode-resources, power.

Architecture Model	No of Slice	No of Slice LUT	No of IOB	Total Power (mw)	Clock Power (mw)	Logic Power (mw)	Signal Power (mw)	Quiescent Power (mw)
M. Litochevski *et al.* Design [21]	1533	3635	523	1454	38	35	38	1343
H. Sathyanarayana's Design [22]	789	11275	262	1473	28	28	74	1343
Proposed Design	955	2202	391	815	32	20	37	722

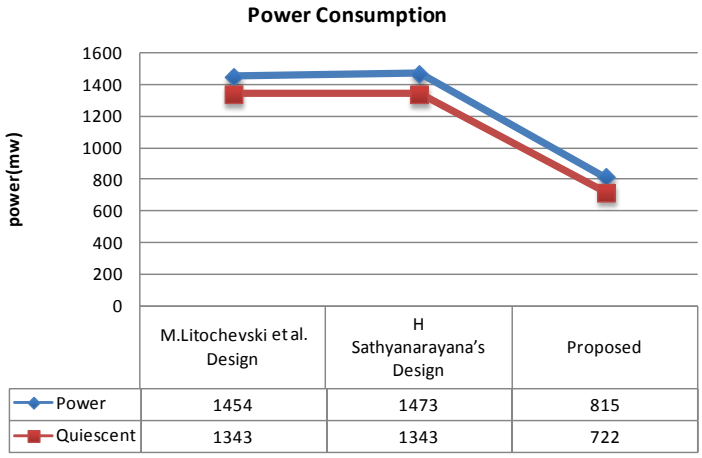

Figure 6. Comparison of total power and quiescent power.

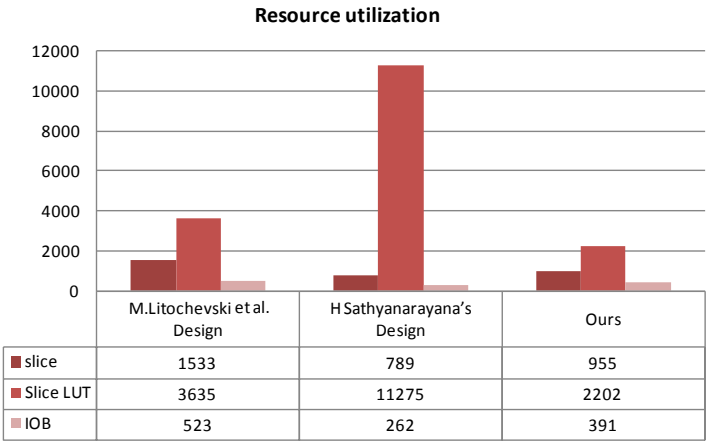

Figure 7. Resource utilization.

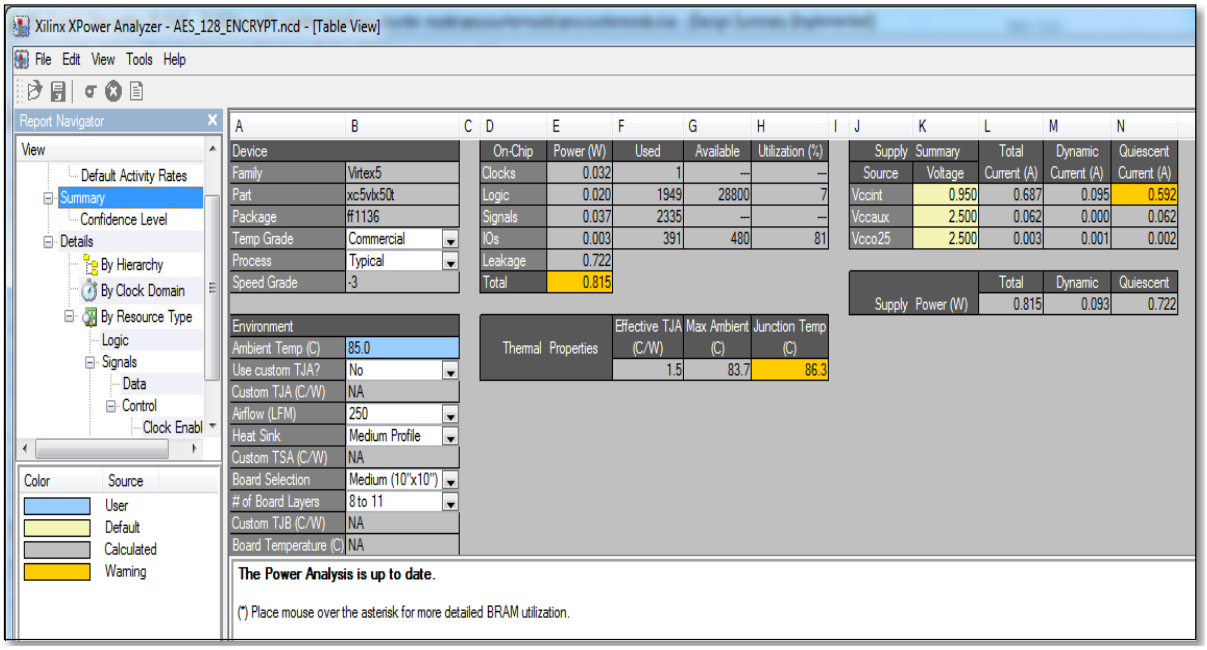

Figure 8. Power report using Xilinx XPower analysis.

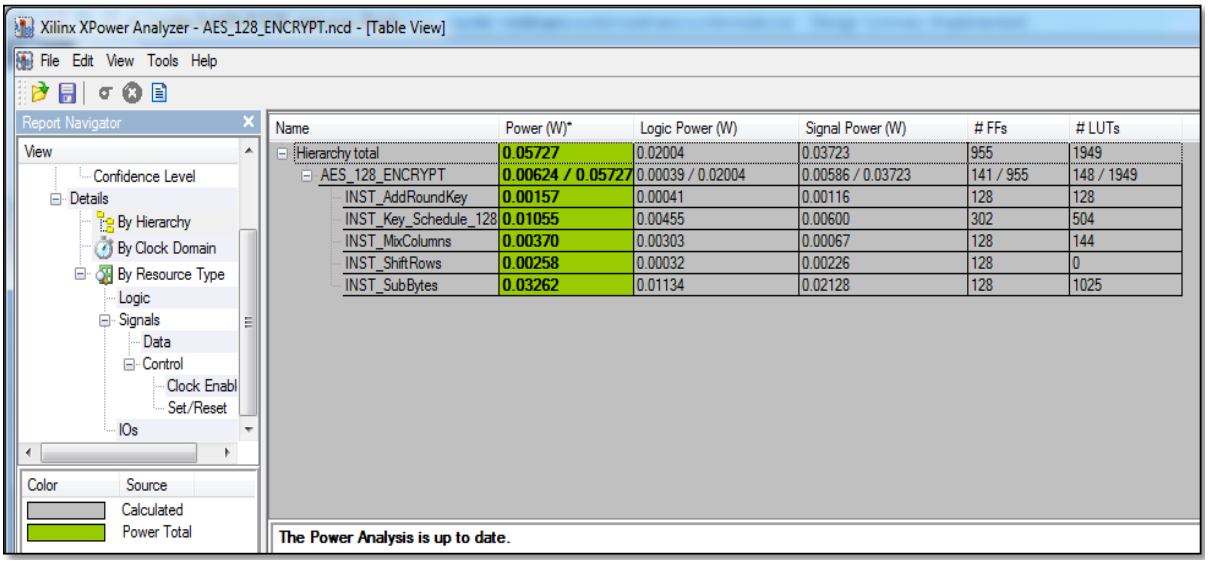

Figure 9. Power report of different modules in proposed Rijndael AES 128 CTR mode.

of WiMax. The vertex 5-xc5vlx50t-1 lfgg900 low power device has been used to compare the existing design with proposed model. The modification has been carried out in SBox and MixColumn which takes more power due to nonlinearity function. This modification architecture is used in proposed AES CTR design. This finding shows that vertex 5vlx50t can provide smallest area as well as power. These characteristics are important for handheld devices and have tremendous improvement of mobile WiMax devices.

References

[1] Khan, A.S., Fisal, N., Bakar, Z.A., Salawu, N., Maqbool, W., Ullah, R. and Safdar, H. (2014) Secure Authentication and Key Management Protocols for Mobile Multihop WiMAX Networks. *Indian Journal of Science and Technology*, **7**, 282-295.

[2] Luo, C.L. (2009) A Simple Encryption Scheme Based on WiMAX. *International Conference on E-Business and Information System Security*, Wuhan, 23-24 May 2009, 1-4. http://dx.doi.org/10.1109/ebiss.2009.5137899

[3] Rais, M.H. and Qasim, S.M. (2009) FPGA Implementation of Rijndael Algorithm Using Reduced Residue of Prime Numbers. 4*th IEEE International Design and Test Workshop* (*IDR*09), Riyadth, 15-17 November 2009, 1-4. http://dx.doi.org/10.1109/idt.2009.5404130

[4] Fan, C.P. and Hwang, J.K. (2008) FPGA Implementation of High Throughput Sequential and Fully Pipelined AES Algorithm. *International Journal of Electrical Engineering*, **15**, 447-455.

[5] Samiee, H., Atani, R.E. and Amindavar, H. (2011) A Novel Area Throughput Optimized Architecture for AES Algorithm. *International Conference on Electronic Devices, Systems and Applications* (*ICEDSA*), Kuala Lumpur, 25-27 April 2011, 29-32. http://dx.doi.org/10.1109/ICEDSA.2011.5959055

[6] Hodjat, A. and Verbauwhede, I. (2004) A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA. 12*th Annual IEEE Symposium on Field-Programmable Custom Computing Machines*, Los Angeles, April 2004, 308-309. http://dx.doi.org/10.1109/FCCM.2004.1

[7] Daemen, J. and Rijmen, V. (1998) The Block Cipher Rijndael. Smart Card Research and Applications. *Third International Conference, CARDIS'*98, Louvain-la-Neuve, Belgium, 1998, 288-296.

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

[9] Ranjeeth, K.D., Alukaidey, T., Salman, K. and Alzaabi, M. (2013) Security Algorithms for WiMax. *International Journal of Network Security & Its Applications* (*IJNSA*), **5**.

[10] Yu, N. and Heys, H.M. (2005) Investigation of Compact Hardware Implementation of the Advanced Encryption Standard. *Canadian Conference on Electrical and Computer Engineering*, Saskatoon, 1-4 May 2005, 1069-1072.

[11] Algredo-Badillo, I., Feregrino-Uribe, C., Cumplido, R. and Morales-Sandoval, M. (2008) FPGA Implementation Cost and Performance Evaluation of the IEEE 802.16e and IEEE 802.11i Security Architectures Based on AES-CCM. 5*th International Conference on Electrical Engineering, Computing Science and Automatic Control* (*CCE* 2008), Mexico City, 12-14 November 2008, 304-309. http://dx.doi.org/10.1109/ICEEE.2008.4723408

[12] Hasan, J. (2006) Security Issues of IEEE 802.16 (WiMAX). 4*th Australian Information Security Management Conference*, Perth, 5 December 2006.

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

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

[15] Forouzan, B.A. and Mukhopadhyay, D. (2012) Cryptogrpah and Network Security. 2nd Edition, Tata McGraw-Hill, New Delhi.

[16] McLoone, M. and McCanny, J.V (2001) High Performance Single-Chip FPGA Rijndael Algorithm Implementations. In: Koç, Ç.K., Naccache, D. and Paar, C., Eds., *Cryptographic Hardware and Embedded Systems—CHES* 2001, Springer, Berlin Heidelberg, 65-76. http://dx.doi.org/10.1007/3-540-44709-1_7

[17] Shanthini. N., Rajasekar, P. and Mangalam, H. (2014) Design of Low Power S-Box in Architecture Level Using GF. *International Journal of Engineering Research and General Science*, **2**, 268-276.

[18] Rajasekar, P. and Mangalam, H. (2015) Design and Implementation of Low Power Multistage AES S Box. *International Journal of Applied engineering Research*, **10**, 40535-40540.

[19] Rajasekar, P. and Mangalam, H. (2016) Design of Low Power Optimized MixColumn/Inverse MixColumn Architecture for AES. *International Journal of Applied Engineering Research*, **11**, 922-926.

[20] 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. http://dx.doi.org/10.5120/2405-3199

[21] Litochevski, M. and Dongjum, L. (2012) High Throughput and Low Area AES: Core Specifications. HT LA AES Core Specifications, OpenCores, 1-9.

[22] Sathyanarayana, H (2012) AES 128. Open Core Projects.