ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Design of Block Ciphers and Stream Ciphers Using Cryptographic Algorithm

M.G.Ajithra[1], A.Muthumanicckam[2], R.Sornalatha[3]

PG Student, Dept. of Electronics and Communication Engineering, Shanmuganathan Engineering College

Pudukkottai, India[1]

Assistant Professor, Dept. of Electronics and Communication Engineering, Shanmuganathan Engineering College

Pudukkottai, India[2,3]

ABSTRACT: AES (Advanced Encryption Standard) encryption standard, designed in the feedback mode to handle two independent 128-bit input blocks. This paper presents a compact and FPGA based implementation of AES. The protocol used is CCM protocol with two modes of operations. The CCM protocol provides the data authentication on the output. The two independent data streams lead to the low resource efficiency. The process with the adequate FPGA component usage with proper scheduling of data a compact and efficient dual block AES derived in FPGA. Overall efficiency of 30% higher than other related work.

KEYWORDS: Dual Block AES; CCM protocol; CBC-MAC; Authentication;FPGA.

I. INTRODUCTION

In this information age, the security of the information being transported is most vital. Existing research activities have been on the cards for secure transfer of information. Security becomes an important with the rapid development of the wireless communication networks. Secret data and individual privacy data may be contained in the propagating information. For securing of the information transmission, safe encryption algorithms are needed.

The AES specifies a FIPS approved cryptographic algorithm used to protect electronic data. AES was published in December 2001 as FIPS 197 in Federal Register, included the standard of ISO/IEC 18033-3. It specifies the Rijndael standard. AES needed to achieve a demand of wireless communication network by adding a protocol. AES adapt to different sets of requirements like speed, resource usage and security. The protocol used is Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP), provides smaller area, resources and better throughput.

The CCM protocol is an encryption protocols, it improves the data encapsulation mechanism for data confidentiality. It contains two modes of operations namely CBC-MAC and Counter. It executes two related processors namely generation encryption and decryption verification. AES structure with very high performance suitable for CCMP. The use DSPs, LUT and several resources are utilized by FPGA resources. AES with CCMP achieves computational characteristics and exploring the target technology. The CCMP uses the dual block for computation and adequate placement of pipelined structure, path delay minimization. It utilizes the advanced features of FPGA resources. AES implementation is done by the folded structure with 32-bit data path, mapping of intermediate by the look-up operations and T-Box for data path simplification.

Experimental results are obtained on Xilinx FPGA, namely vertex 7. An encryption is done by 4 BRAMs, 4 input LUTs. The overall efficiency is 30% and the resources fully utilized.

The paper is organized as follows: An introduction to AES cipher and CCM protocol in section II and III. An implementation of the proposed system is presented in section IV. The result of the proposed system is presented in section V. The conclusion is in section VI.

Copyright to IJAREEIE
DOI:10.15662/IJAREEIE.2017.0605080

II. AES ALGORITHM

The AES algorithm is non-Feistel cipher that encrypts and decrypts with fixed 128-bit blocks and key size of 128, 192 and 256-bits depends on the rounds as 10, 12 and 14. AES uses the term data block before and after each stage, the data block is referred as a state. It is made up of 16 bytes but normally treated as 4X4 bytes [11].

Four functions are included in each round of iteration, which are Sub-Bytes, Shift rows, Mix columns and Add round key.

Sub-Bytes: Uses S-Box to perform a byte-by-byte substitution of the block. It is a nonlinear substitution system. The substitution is defined by either a table lookup process or mathematical calculation in Galois Field, GF (2^8) field.

Shift Rows: Second round is shifting which permutes the bytes. The left round shifting is used in encryption process, the number of shifts depends on the row number (0, 1, 2, 3) of the state matrix.

Add Round Key: It adds a round key word with each state column matrix. The operation is matrix addition.

Mix Columns: It makes a linear conversion of the plaintext information. The mixing transformation changes the contents of each byte by taking four bytes at a time and combining them to recreate four new bytes. Each state is multiplied with GF (2^8) field, the input mix column conversion is *a*, the output mix column conversion is *r*, by the following matrix:

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \qquad (1)$$

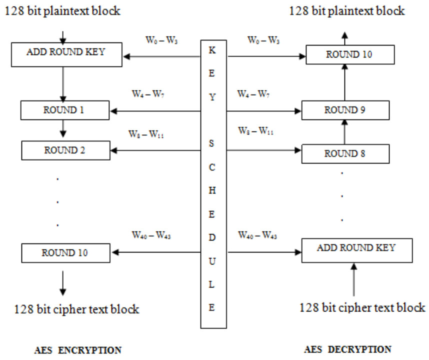

Fig .1 Overall AES Structure for 128-bit

The last round of the cipher has only three transformations (Mix Column is not used).

The key expansion, if the number of rounds is N_r then the key expansion is N_r+1. The round keys are obtained from an input. AES uses the concept of word for generation of key. A word is made up of four bytes. The round keys are generated word by word from W_0 to W_{43} in Fig.1.

The decryption of AES algorithm is performed identical to the encryption but with the inverse operations.

III. CCM PROTOCOL

The CCMP is an encryption protocol for Wireless LAN (WLAN). WLAN products implemented the standards of IEEE 802.11i to an original IEEE 802.11 standard. CCM is an authentication encryption algorithm to provide both authentication and confidentiality during the transferring of data.CCM protocol designed for high data confidentiality and depends on AES standard. The CCM protocol utilizes a single 128-bit key for Message Integrity Code (MIC) computation encryption.

CCMP is based on the two modes of operation namely counter and Counter Block Chaining Message Authentication Code (CBC-MAC).

The input of the CCM protocol is plaintext (128-bit), nonce value, payload and temporal key. The algorithm executes two related processes: generation encryption and decryption verification. The encryption can be generated by Initialization vector (IV). The common approaches of IV include incrementing a counter [3].

The CBC-MAC process starts with AES block cipher and data integrity keys, it performs a XOR operation of the input and key. The next is adding MIC ‘T’ over the 128-bit block. The result of the block is with MAC code ‘T’ block with 64-bit.

The Counter mode (CTR) produces different cipher blocks, which used based on nonce value rather than starting it for a fixed value. The mode provides authentication by adding extra capabilities. CTR ciphering is parallel, decryption is the same process as encryption and the message is not required to break into exact number of blocks [9]. The failure of the counter mode will result collapse of whole security mechanism.

The counter starts with an inputs of payload, TK and counter blocks of 128 bits [10]. The result produces by the XOR operation between the result of ‘T’ of the CBC-MAC and produces the 64-bit cipher text block ‘U’ is explained in Fig.2.

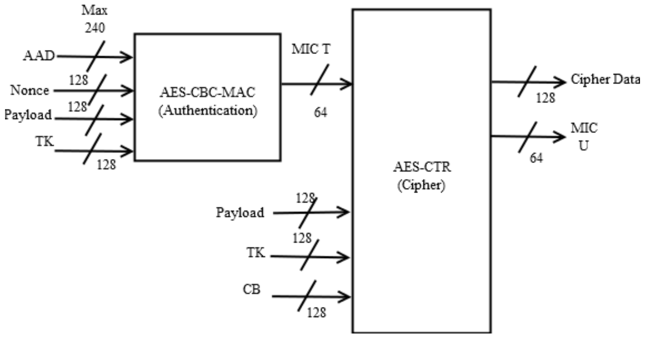

Fig.2 Block Diagram of AES-CCM Protocol

The CCMP does not require the AES decipher mode, in counter mode the decryption is performed by XORing the cipher text with the encrypted nonce from the counter. In decryption process the counter mode is applied to cipher text to recover the MAC and the corresponding payload then CBC mode is applied to the payload and the nonce to verify the correctness of the MAC. The successful verification is the payload and its associated data are from the same source with the access to key that a MAC provides high level of authentication [6].

IV. PROPOSED ARCHITECTURE AND IMPLEMENTATION

The AES with CCMP produces compact structure by a 32-bit data path with T-Box and Shift Register approach. The structure with two different 128 bit data path send by 32-bit loaded sequentially. In an initial step XOR the plaintext with the input keys, 32 bit XOR operation is considered [2].

The second stage is shift rows operation. The shift register approach is considered on FPGA using SRL32 LUT mode. The two distinct states are addressed and used for temporary storage. The main computation is substitution bytes using look up tables and its coefficient multiplications on T-Box. The substitution byte uses GF (2^8) that are performed in the stage 4. The last computation is XORing data with message block produces the output. If the key ‘A’ input is set to zero then the data is fed back to the shift register.

The last process of AES is Mix column operation which is not performed in the last round of the AES algorithm, it performed by the different set of T-Boxes mapped with different memory sections of BRAMs in order to perform the SubBytes operations [8].

In CCMP, the modes need the additional data block for an efficient addition operation. The additional block is performed only at the last stage. After an encryption of AES, the message block is added with a MIC value. MIC value is computed of source address, destination address, priority field, reserved octets and payload data.

A. TBoxes into BRAM

AES requires SBox operation by a matrix multiplication. The output is multiplied by GF(2^8) by the coefficients {3,1,1,2} for encryption. BRAM FPGAs process between 18Kb to 36 Kb.

B.Implementation Details

The proposed architecture is designed and implemented based on target technology. The computation is divided into 6-input blocks.

Fig.3, Stage 1 is adding Round key, stage 2 uses SRL32 LUT computation. Stage 3 explains BRAM, BRAM is considered for TBox implementation and key storage. The data path consists of the dual port BRAM [5]. The first 8bit is address of the state and 9th address bit is differentiating between the rounds.

C. Deciphering in CCMP

CCMP does not require the AES decipher mode, in counter mode the decryption is performed by XORing the cipher text with the encrypted nonce from the counter. In the decryption process the counter mode is applied to cipher text to recover the MAC and the corresponding payload then CBC mode is applied to the payload and nonce to verify the correctness of the MAC [7]. The successful verification is payload and its associated data are from the same source with the access key that a MAC provides higher level of authentication.

V. RESULT ANALYSIS

The proposed architecture is designed using Verilog HDL and the design is designed, placed and route in Xilinx ISE 14.7 design suite. The results are exposed in throughputs, slices, TPA and power.

The utilization of the slices is reduced due to the ISE software it is ultra fast and reduces the overall efficiency of the encryption. The key expansion is done by two ways namely computing locally with dedicated logic or computing off chip and storing in local memory [4].

The previous work of AES explains that the use of dedicated shift rows operation reduce the area resources of dual-port BRAMs to implement AES algorithm based on

TBoxes in fig.3. The last round of AES computation is unitary coefficient multiplication from TBoxes. The 128-bit dual data path proposes the folded round structure with four cycles per round and memory based SBoxes [1], it preferred the distribution of SBoxes into LUT based memories.

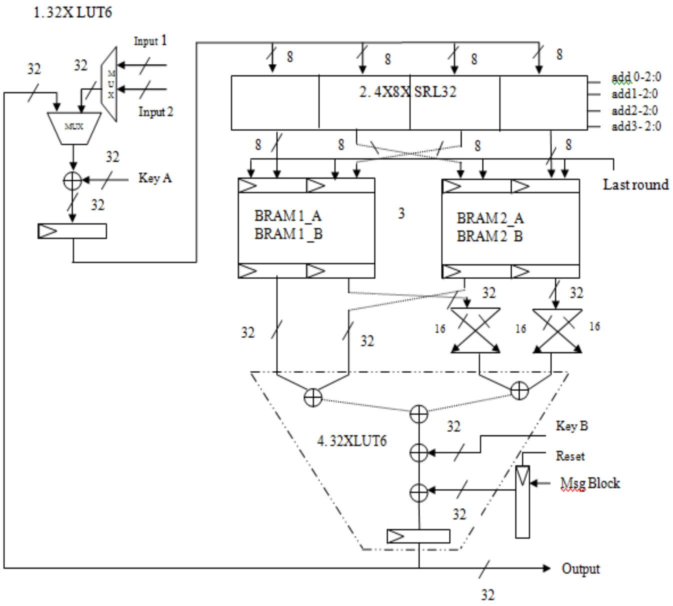

Fig.3 Block Diagram of Dual block AES

DOI:10.15662/IJAREEIE.2017.0605080

The CCM protocol with AES based on two distinct parallel components used for CBC-MAC and counter modes, they are folded architecture. Considering the 32-bit data path with Shift registers and BRAM based TBoxes and usage of DSP. It is cascaded by performing XOR operation and mix column is used in LUT/Slice structure in fig.4.

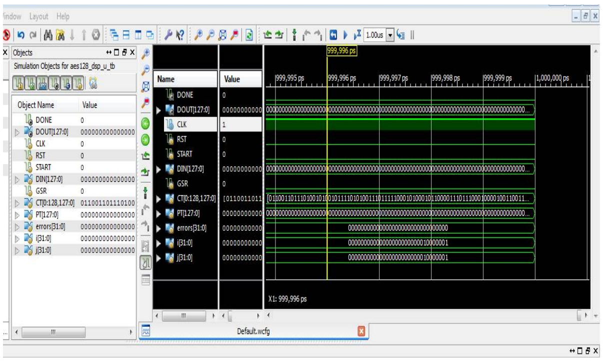

Fig.4 AES 128-bit

The output of the cipher text is produced by the plaintext and the temporal key. The CBC-MAC is used to produce the message authentication code by discarding the cipher text except the last one. CBC-MAC is vulnerable for message extension attack where the message length is not fixed or checked. CMAC's last is unique, if the block is evenly separated then key K_1 is used and M_n is appended with the predefined blocks with K_2. The only difference in K_1 and K_2 will need to zero and intermediate value C_i is output in fig 5.

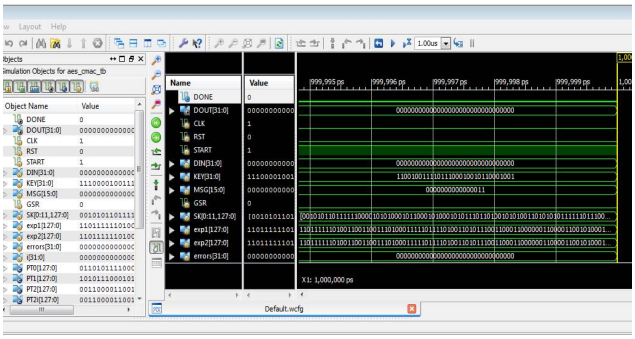

Fig.4 CCM Protocol with input

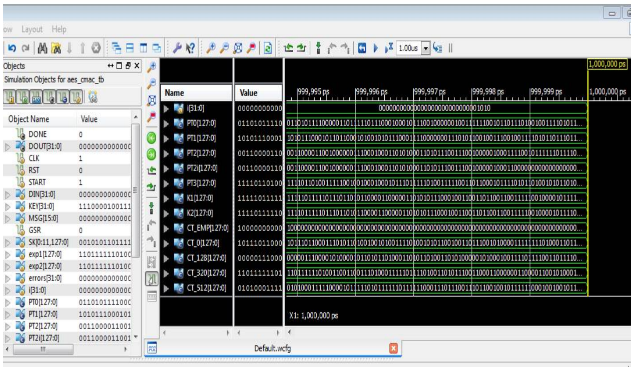

Fig.5 CCMP with Output

The AES with Electronic Code Book (ECB) produce 128-bit with unrolled structure with more Slices and BRAMs. The resource utilized is four times than CCMP.

VI. CONCLUSION

In this paper AES with two independent streams of data such as CBC-MAC and Counter is proposed by Xilinx ISE design technologies. The presented work is considering the modern technologies of Xilinx FPGA to achieve efficient resources. The method used is LUT based addressable shift registers and BRAM block memory, the efficiency is achieved by the proper scheduling and mapping architecture. The experimental results produced by CCM protocol with AES, the maximum frequency required is 174.98 MHz. The efficiency produced is 30% of the related work. The future work is extended by generating the IP for the message authentication code. It also extended by remote configuration of FPGA using AES.the secure updates of data for secure AES architecture for the secure updates, by using the system or the data gets updated and stores the bit streams in Non Volatile memory (NVM) and programs, it start up the process without online [12].

REFERENCES

[1] Thi-Thansh-Dung, Van-phuc Hoag and Van-Lan Dao, “An efficient FPGA implementation of AES-CCM authenticated encryption IP core” 3rd National foundation for science and development conference on Information And Computer Science (NICS), pg. 202-205,Sep 2016.

[2] Muzaffar Rao, Thomas Newe and Ian Grout, “ AES implementation on Xilinx FPGAs suitable for FPGA based WBSNs”, IEEE 9th International Conference on Sensing Technology (ICST).

[3] Ignacio Algredo-Badillo, claudia Feregrino-Uribe, Rene cumlido and Miguel Morales-Sandoral, “Compact Implemenation and performance evaluation for AES-CCM cores for wireless networks” International Conference on Reconfigurable computing and FPGAs, pg.421-426, Dec 2008.

[4] Jaos Carlos Resende and Ricardo Chaves, “Compact dual block AES core on FPGA for CCM protocol”, IEEE 25th International Conference on Field Programmable Logic and Application(FPLA), october 2015.

[5] NIST, “ FIPS 197: Advanced encryption standard (AES)”, Federal Information Processing Standards Publication, Vol.197, pp. 441-0311, 2001.

[6] Q.Liu, Z.Xu and Y.Yuan, “A 66.1 Gbps single-pipeline AES on FPGA”, International conferrence in Field Programmable Technology (FPT),pg.378-381,2013.

[7] M.El Maraghy, S.Hesham and M.A.Abd El Ghany, “ Real-time efficient FPGA implementation of AES algorithm”, 26th International Conference in SOC, pp.203-208,2013.

[8] Saar Drimer, Tim Guneysu and christofPaar, “DSPs, BRAMs and a Pinch of Logic: New Recipes for AES on FPGAs”, 16th IEEE International Symposium on Field Programmable Custom Computing Machines, pp. 99-108,14-15 April 2008.

[9] NIST, “ FIPS 197: Advanced encryption standard (AES)”, Federal Information Processing Standards Publication, Vol.197, pp. 441-0311, 2001.

[10] Behrouz A.Forouzan, “Cryptography and Network Security”, Tata McGram-Hill Publishing Company Limited, Special Indian Edition 2007.

[11] Luca Henzen and Wolfgang Fichtner, “ FPGA Parallel-Pipelined AES-CCM Core for 100G Ethernet Applications”, IEEE Proceedings of ESSCIRC, 14-16 September 2010, pp. 202-205

[12] Yuanchi Tian and Howard M.Heys, “ Hardware Implementation of a High Speed Self-Synchronizing Cipher Mode”, 28th IEEE Canadian Conference in Electrical and Computer and Computer Engineering, Halifax, Canada, 3-6 May 2015.