International Journal of VLSI System Design and Communication Systems

ISSN 2322-0929
Vol.02, Issue.10,
November-2014,
Pages:1019-1024

www.ijvdcs.org

High-Performance VLSI Architecture for AES-GCM Algorithm with Sub Pipelining

B. LOHITHA[1], K. PADMA VASAVI[2]

[1]PG Scholar, Dept of ECE, SVECW, Bhimavaram, AP-India, E-mail: lohithanithya@gmail.com.
[2]Professor, Dept of ECE, SVECW, Bhimavaram, AP, India, Email: padmavasaviece@svecw.edu.in.

Abstract: The need for high speed data transmission along with efficient security to the data ia progressing day by day. This motivated the research in the development of high performance algorithms for data transmission. However the VLSI architectures for the implementation of encryption algorithms are relying on LUT and pipeline operation for implementation. Such algorithms their by reduce the efficiency of performance of the encryption algorithm in terms of speed and authentication. In this paper a high performance for AES-GCM algorithm is proposed to increase the speed and efficiency of algorithm. The efficiency in throughput is achieved by dividing composite field architectures into number of stages by making use of sub pipelines. The resultant architecture can achieve high frequency, high throughput as well as low power consumption. The architecture is simulated using Modelsim, design verification done using XilinxISE XC4VLX200 FF1513. The proposed architecture is compared with AES-GCM architecture using pipeline.

Keywords: Advanced Encryption Standard, Galois/Counter Mode, Pipeline, Subpipeline.

I. INTRODUCTION

Cryptography plays an important role in the security of data transformation. There are many algorithms for provide security to data by transformation to which include RSA, DEA, Triple DEA, and AES etc. The AES algorithm was accepted by the National Institute of Standard and Technology (NIST) in 2001 as the replacement for the previous cryptographic standards [1]. Since then, it has been included in wireless standards of Wi-Fi [2] and Wi-MAX [3] and many other applications, ranging from the security of smartcards to the bitstream security mechanisms in FPGAs. The Galois Counter Mode (GCM) was finalized as a new mode of operation of AES by National Institute of Standard and Technology in 2007. The Advanced Encryption Standard -Galois Field Counter provides authentication and confidentiality for sensitive data simultaneously. The authentication of the AES-GCM is provided by the Galois/Counter Mode (GCM) [6] using a universal hash function. The AES-GCM is being used for a number of applications such as the new LAN security standard WLAN 802.1AE [4] and Fiber Channel Security Protocols [5]. Of the transformations in the AES encryption, the S-box is the only nonlinear, requiring the highest area and consuming much of the AES power.

Therefore, the performance metrics of the S-box affect those for the entire AES encryption significantly. For low complexity implementation, the S-box can be realized using logic gates in composite fields. Different GCM architectures have been presented in literature. The sequential GCM method is area efficient [7] ; it needs many clock cycles, reducing the performance of the architecture. Because of the low throughput of the sequential method, a parallel method is proposed [9], which uses two GF (2128) multipliers to perform this operation in parallel. This parallel implementation has been generalized in [10] Recently, a high high-performance approach for computing the GHASHH function for long messages has been proposed [11]. In AES pipelined composite field of S-box takes more power and working with low frequency. These S-boxes can also Sub-pipeline for achieving high performance [8]. On the other hand, the S-boxes based on lookup tables could be area efficient when implemented utilizing the memory resources available on FPGAs. In this paper High- performance Advanced Encryption Standard – Galois Counter Mode using Sub-Pipeline architecture is implemented on software Vertex-4. The rest of the paper is organized as followed as follows: section 2 presents the preliminaries of AES-GCM algorithm, section 3 discusses the subpipeline of AES-GCM methodology, section 4 discusses results and comparisons, and section 5 draws the conclusion.

II. PRELIMINARIES

In this, section preliminaries for the AES-GCM algorithm are presented. AES-GCM is an encryption algorithm which uses symmetric key for network security (confidentiality), and the GCM which uses hash key for authentication. To increase the AES-GCM algorithm in network a pipeline AES-GCM is used which is described below:

A. Pipeline AES-GCM

Pipeline AES-GCM is a block cipher with counter mode of operation. AES algorithm is utilized with the input, key and the output blocks of 128 bits. Based on the security requirements, the key size determined as AES-128 bits (with 10 rounds), AES-196 bits (with 12 rounds), and AES-256 bits (with 14 rounds). In AES encryption all the rounds have 4 transformations of Sub bytes, Shift rows, Mix columns and Addroundkey, except for the last round. For the last round, mix column is eliminated. The pipelined architecture is realized by inserting rows of registers between each round unit. Pipeline architecture for AES is presented in Figure 1.(a) and Figure 1.(b) presents the architecture for each round unit.

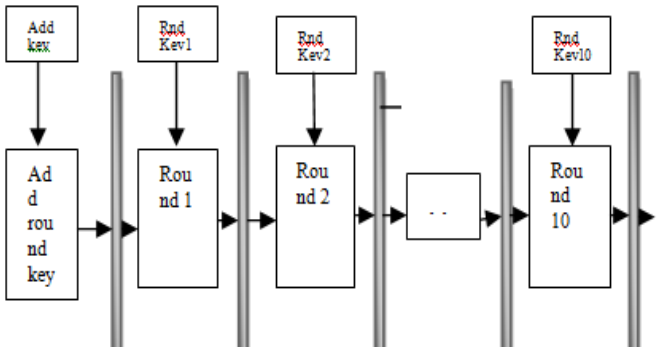

Fig.1(a). Pipeline Architecture

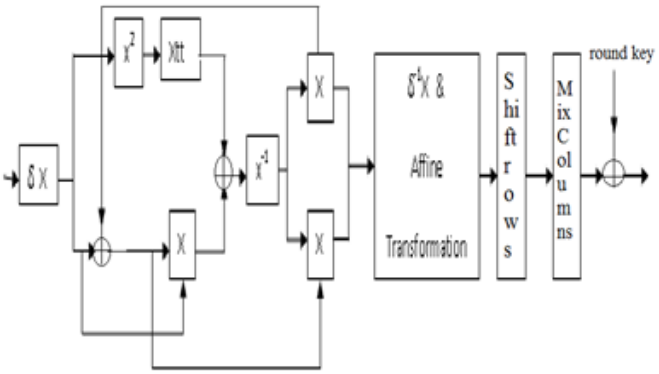

Fig.1(b). Composite field Architecture of Round Unit

B. Composite field S-box

The implementation of the composite field S-BOX shown in Figure 1.(b) is accomplished using combinational logic circuits rather than using pre-stored S-BOX values. S-BOX substitution starts by finding the multiplicative inverse of the number in GF (2^8), and then applying the affine transformation. Implementing a circuit to find the multiplicative inverse in the finite field GF(2^8) is very complex and costly, therefore, the finite field GF(24) is used to find the multiplicative inverse of elements in the finite field GF(2^8).

C. Shift rows, Mix columns, Addroundkey

The input signal to the shift row is the inverse affine transformation of 128-bit. In Shift rows, the first row of the state remains intact and the four bytes of the last three rows of the input state are cyclically shifted. Shift row is used to route the information. In the Mix columns transformation, each column is modified individually, it is applied to columns of the state matrix, each column being considered as a polynomial over GF(2^8). The result is multiplied with fixed polynomial by using XOR instead of the multipliers. The input signal to "Addroundkey" is outputs of "Mixcolumn" and key schedule. Round Key generated by the Key Scheduling module are XORed with "Mixcolumn". The final transformation "Addroundkey", the input state and the key of the corresponding round is performed. In pipeline each round is driven by a cycle, total encryption will take 10 clock cycles.

D. Galois Counter Mode

The authenticated encryption performs two tasks, encrypting the confidential data and computing an authentication tag. The data flow of the authenticated encryption operation is shown in Figure 2. In GCM operation plain text, key, additional authenticated data (AAD) and Initial Vector (IV) are the inputs. GCM performs the block cipher counter mode by using the counter which generates the function incr. it increments the 128-bit of initial counter value and resultant acts as an input to the Ek. Input signals of the multH module are XOR operation of ciphertext [0:127], previous multiplication output [0:127] is XORed and generate the input signal to next multH. This function is constructed by GF (2128) multiplications with a fixed parameter, called the hash subkey (H) which provides authentication encryption. It is implemented in design to achieve high speed at a low area. The number of plaintexts gives more secure encryption output, and final result of the tag is generated by using this multH XORed with E_k.

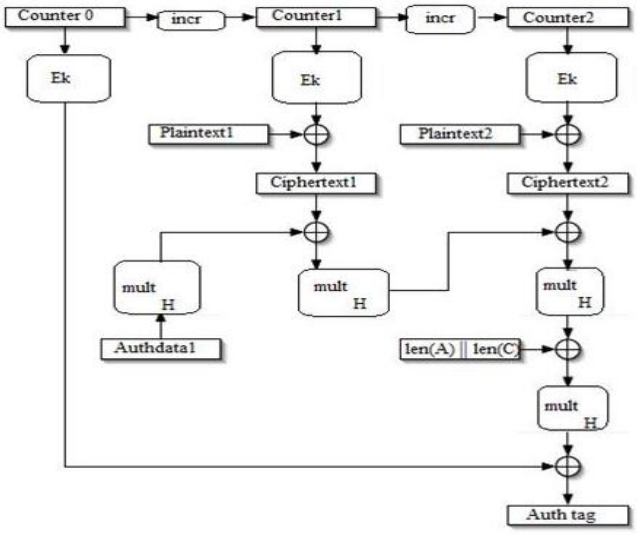

Fig.2 The GCM Authenticated Encryption

III. PROPOSED ARCHITECTURE

Subpipeline Advanced Encryption Standard is similar to the pipeline AES as shown in Figure 3. Additionally each round is divided into 6 stages with equal delay to speed up

the implementation. The sub pipelined architecture is realized by inserting rows of registers between each round unit and sub stages of inside each round unit is block mode operation, each block is divided into 16 bytes, and each byte is considered as an element of GF(2^8). The composite of GF(2^8) can be built iteratively from GF(2^8) using the irreducible polynomials. The composite field of GF(2^8) consists of isomorphic mapping (δ), multiplicative inversion and inverse isomorphic mapping (δ-1).

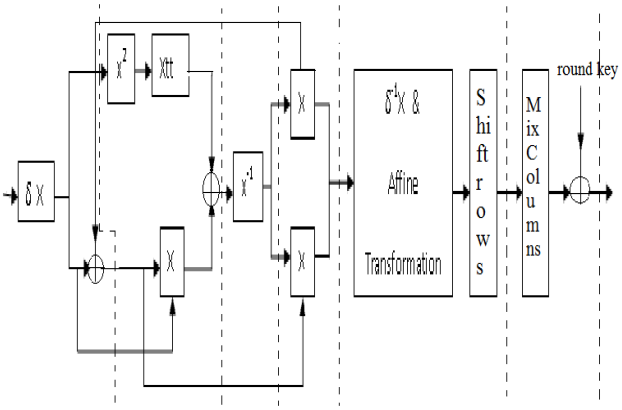

Fig.3. Proposed block diagram of Sub Pipelined Composite field Architecture of a round unit.

Isomorphic mapping is used to change from binary field 8-bit to composite field. Multiplicative inversion consists of square in GF(2^4), multiplier in GF((2^2)^2), constant multiplier (x^{λ}), multiplier in GF(2^2) and inversion in GF(2^4). The multiplier in GF(2^4) can be future decomposed into multiplications in GF((2^2)^2) to reduce complexity. Inverse isomorphic mapping is used to transformation from polynomial basis to binary field. In this composite field 8-bit input of isomorphic divides the output into two 4-bits to operate square in GF(2^4) and multiplicative in GF((2^2)^2). The result of 4-bit multiplication in GF((2^2)^2) is multiplied with a constant λ. The output of xλ and multiplicative in GF((2^2)^2) are XORed , to give 4-bit result to inversion in GF(2^4). Two Multiplier in GF((2^2)^2) generates 8-bit data out in fourth stage. According to the AES algorithm affine transforms is applied to inverse isomorphism that is given to shift rows in fifth stage. In final stage mix column and add round key operations are performed. In this subpipeline each stage will take a cycle, when one stage is complete, the next stage is triggered by incrementing the number of these sub stages, the critical path and clock pulse width of system decreased and as a result the throughput is increased. The proposed architecture is substituted in AES-GCM encryption process to get high performance. Comparisons of pipeline and proposed architecture are discussed in section 4.

IV. RESULTS AND COMPARISION

AES-GCM has the capability of securing the data from unauthorized snoopers. It takes less time to encrypt the data and generated a tag. The results are shown from Figure 4. to Figure 6. Respectively.

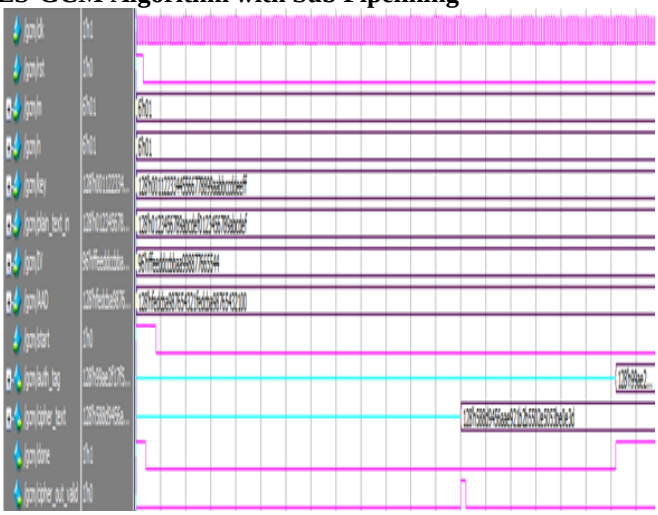

Fig.4 Output of Subpipelined AES-GCM Encryption

In Figure4. we considered the plain text, key, AAD and IV values. The encryption process begins, when rst and start are in low state. The final cipher text is obtained after 122 cycles and result authenticated tag is obtained in186 cycles.

Considering the values as input:

Plain text= 0123456789abcdef0123456789abcdef

Key= 00112233445566778899aabbccddeeff

Obtained output values:

Cipher text=588d9456aae921b2b5502e5053be0e3d

Tag= 99ae2f17f5ba23f761a02eb510df8007

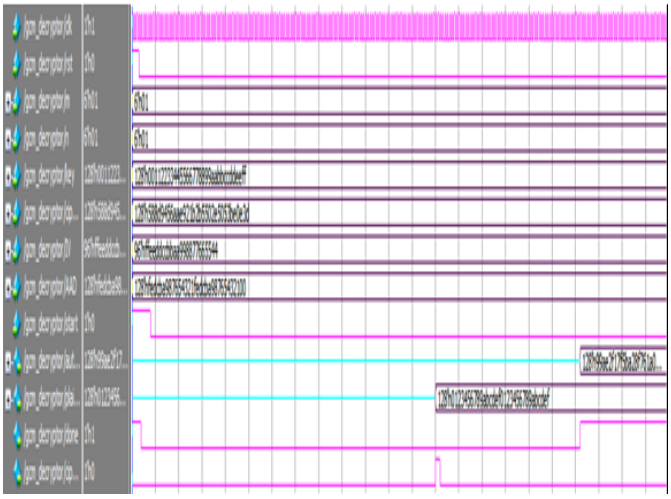

Fig.5 Output of Subpipelined AES-GCM Decryption

In Figure5. we considered the ciphertext, key, AAD and IV values. The decryption process begins, when rst and start are in low state. The final plain text is obtained after 122 cycles and result authenticated tag is obtained in186 cycles. Here the authenticated decryption function decrypts the confidential data and verifies the tag.

Considering the values as input:

Cipher text= 588d9456aae921b2b5502e5053be0e3d

Key= 00112233445566778899aabbccddeeff

Obtained output values:

plain text= 0123456789abcdef0123456789abcdef

Tag= 99ae2f17f5ba23f761a02eb510df8007

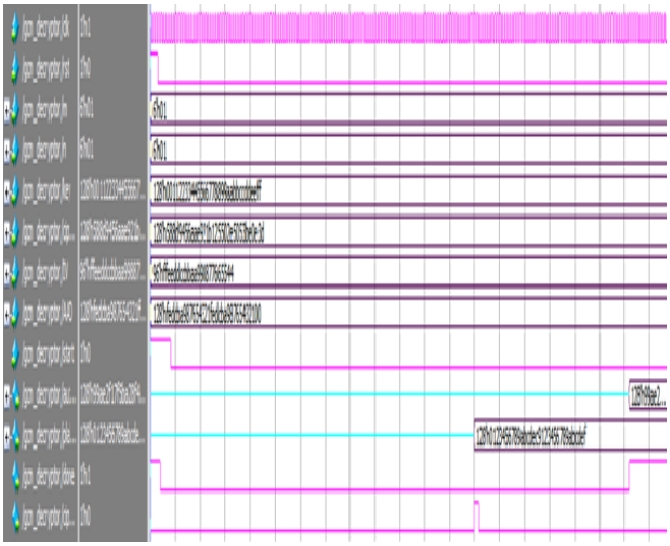

Fig.6 Output of Subpipelined AES-GCM Decryption

In Figure 6. we considered the cipher text, key, AAD and IV values. The encryption process starts, when rst and start are low. The final plain text is obtained after 122 cycles and result authenticated tag is obtained in186 cycles. If we change any value in input, we will get different tag value.

Considering the values as input:

Cipher text= 588d9456aae921b125502e5053be0e3d

Key= 00112233445566778899aabbccddeeff

Obtained output values:

Plain text= 0123456789abcdec9123456789abcdef

Tag= 99ae2f17f5ba28f42199235203b6a4a

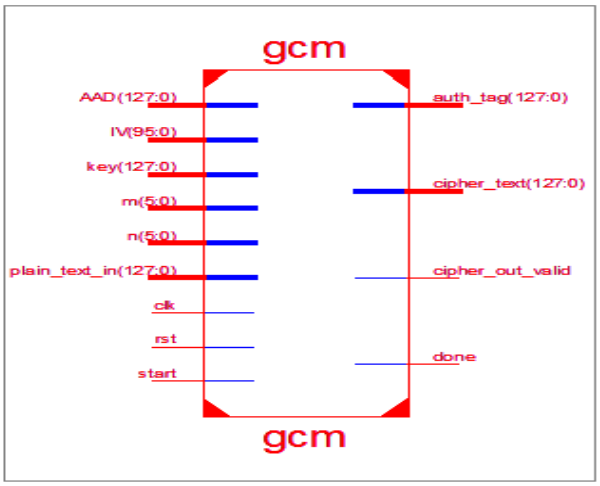

Fig.7 RTL Schematic of AES-GCM

In Figure 7. RTL schematic shows input and output signals. AAD, Plain text of 128 bit, IV of 96 bit, m, n, clk, rst and start are inputs. Cipher out, cipher text, tag of 128 bit and done are outputs.

Table1: Sub Pipelined AES-GCM Result

Plain_text	Key	Cipher_text	Tag
0123456789abcdef0123456789abcdef	00112233445566778899aabbccddeeff	588d9456aae921b2b5502e5053be0e3d	99ae2f17f5ba23f761a02eb510df8007
abcdef0123456789abcdef123456789	00112233445566778899aabbccddeeff	2633e3000078bd41fbe8436f950a45b	117c0b8c8a716e2c9ea2bbff60563a22
09876543210fedcbaabcdef123456789	0123456789abcdef0123456789abcdfe	56891774ff99b212144c6079500dfc8a	fe02e54a6b0c4cf2c034f3fadfbb0dcd
43210fedcba98765abcdef5678901234	0123456789abcdef0123456789abcdfe	1c2f7dda153fd8bc153d51de0bd88937	b4fdae7bb413260b7a301f1f54b69fad

Considering the values as input:

Plain text=09876543210fedcbaabcdef123456789

Key= 0123456789abcdef0123456789abcdef

Obtained output values:

Cipher text= 56891774ff99b212144c6079500dfc8a

Tag= fe02e54a6b0c4cf2 c034f3fadfbb0dcd

For entire table 1 considered the same AAD and IV values as

AAD= fedcba987654321fedcba98765432100

IV= ffeeddccbbaa998877665544

Table2: Design Summary of subpipeline AES-GCM

S.No.	PARAMETER	VALUE
1.	No.of registers	12930
2.	Min.clock period	6.998µs
3.	Frequency	142.902MHZ
4.	Total IOs power	0.179µW
5.	On-chip logic	1.730
6.	Dynamic power	0.009µW
7.	Quiescent power	3.813µW

AES-GCM is compared with Subpipeline AES-GCM in various parameters like clock period, dynamic power, quiescent power, and frequency. The implementation results give the same outputs, but in power consumption is less and high frequency compared with pipelined AES-GCM.

Table3: Comparison between pipeline and sub pipeline of AES and AES-GCM

S. No	Parameters	AES pipeline	AES Sub pipeline	AES-GCM pipeline	AES-GCM Sub pipeline
1.	Min.clock period	8.421µs	1.365µs	9.611µs	6.998µs
2.	Frequency	118.7 MHZ	732.654 MHZ	104.043 MHZ	142.902 MHZ
3.	Dynamic power	0.031 µW	0.003 µW	0.102 µW	0.009 µW
4.	Quiescent power	1.243 µW	1.241 µW	3.817 µW	3.813 µW

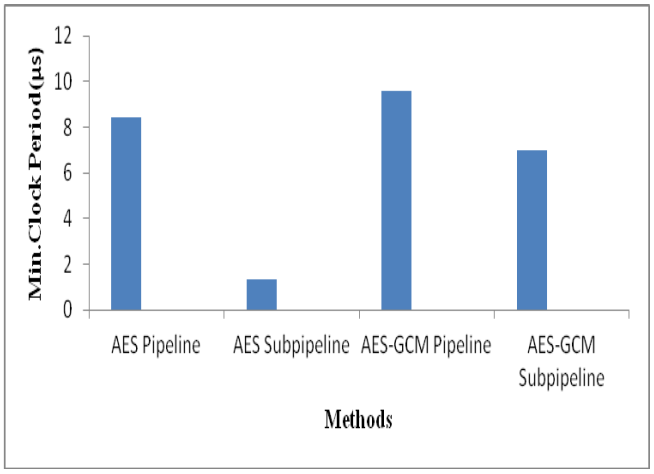

Fig.8 Comparison of Min. clock period of pipeline and sub pipeline AES and AES-GCM.

From Fig.8 we understood the Min. clock period of AES Sub pipeline is less compared with AES pipeline and AES-GCM Sub pipeline is less compared with AES-GCM pipeline. It says that the output of AES-GCM sub pipeline is obtained as fast as compared to AES-GCM pipeline.

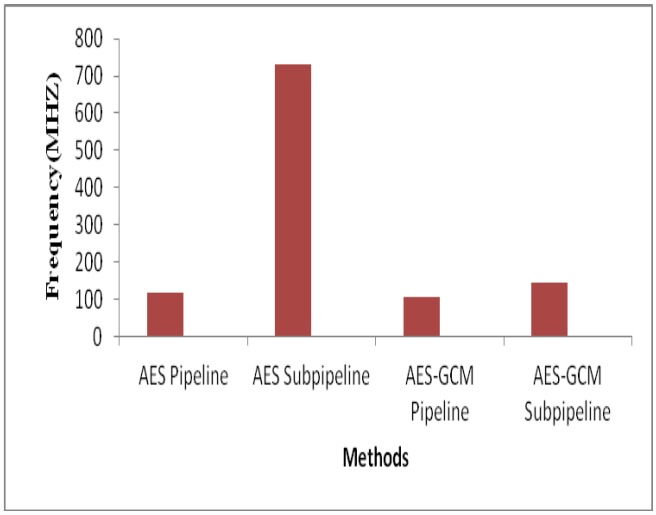

Fig.9 Comparison of Frequency of pipeline and sub pipeline AES and AES-GCM.

From Figure9. we understood the Frequency of AES Sub pipeline is high compared with AES pipeline and AES-GCM Sub pipeline is high compared with AES-GCM pipeline. It says that the speed of AES-GCM sub pipeline is increased as compared to AES-GCM pipeline.

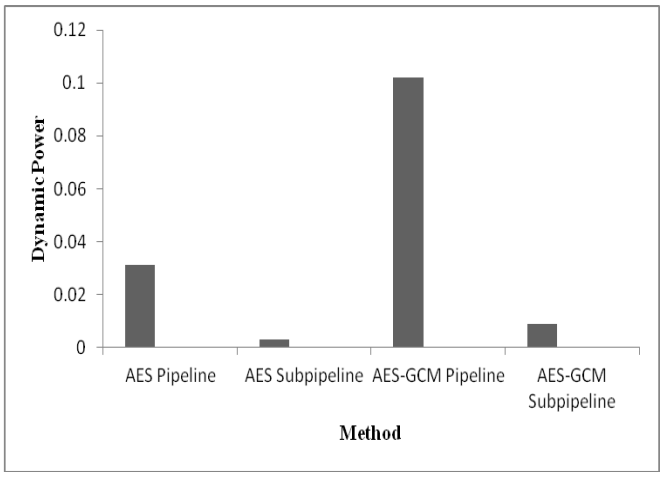

Fig.10 Comparison of Dynamic Power of pipeline and sub pipeline AES and AES-GCM.

From Figure10. we understood the Dynamic power of AES Sub pipeline is low compared with AES pipeline and AES-GCM Sub pipeline is low compared with AES-GCM pipeline. The power consumption of AES-GCM sub pipeline is decreased as compared to AES-GCM pipeline; it says that the AES-GCM sub pipeline architecture performance is increased.

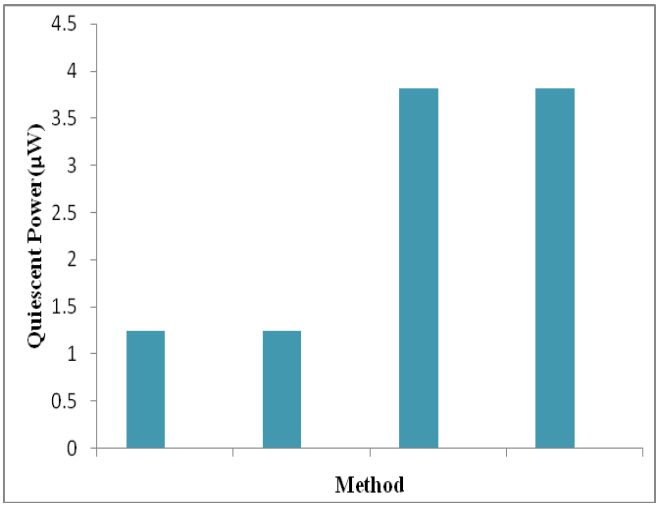

Fig.11 Comparison of Quiescent Power of pipeline and sub pipeline AES and AES-GCM.

From Figure11. we understood the Quiescent power of AES Sub pipeline is low compared with AES pipeline and AES-GCM Sub pipeline is also low compared with AES-GCM pipeline. The power consumption of AES-GCM sub pipeline is decreased as compared to AES-GCM pipeline; it says that the AES-GCM sub pipeline architecture performance is increased.

V. CONCLUSION

For securing the data research is progressing very fast and various researchers from various fields are focusing to increase the speed of encryption for security. We have obtained optimized building blocks for the AES-GCM to give high performance. High performance is obtained by dividing the AES composite field into 6 stages for each round. We have evaluated and compared the performance of pipelined and sub pipelined AES-GCM architectures. Proposed architecture works with the high frequency at 142.9MHZ, gives high throughput.

VI. REFERENCES

[1]. Nat'l Inst. Of Standard and Technologies "Announcing the Advanced Encryption Standard (AES)," Fed. Information Processing Standards Publication, no. 197,Nov. 2001.

[2].Wi-Fi, http://standards.ieee.org/getieee802/ download/ 802.11-2007.pdf,2011.

[3].WiMAX, http://standards.ieee.org/getieee802/download/ 802.16e-2005.pdf,2011.

[4]. IEEE Standard for Local and Metropolitan Area Networks, Media Access Control (MAC) Security, 2006.

[5].Fiber Channel Security Protocols (FC-SP), http://www. t10.org/ftp/t11/document.06/06-157v0.pdf. 2006.

[6]. M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," NIST SP, 800-38D, 2007.

[7]. B. Yang, S.Mishra, and R. karri, "High speed Archetecture for Galois/ counter Mode of Operation (GCM)," Cryptology eprint Archive: Report 2005/146 June 2005.

[8].X.Zhang and K.K. Parhi,"High-Speed VLSI Architectures for the AES Algorithm," IEEE Trans. Very Large Scale Integration (VLSI) Systems, vol. 12, no. 9, pp. 957-967, sept. 2004.

[9]. .D.A. McGrew and J. Viega, "The Galois/ counter mode of operation (GCM)," NIST Modes Operation Symmetric Key Block Ciphers, http://csrc.nist.gov/groups/ST/ toolkit/ BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf. 2005.

[10]. A. Satoh, S. Morioka, K. Takano, and S. Muntoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," Proc.Int'l Conf. Theory and Application of Cryptology and Information Security: Advance in Cryptology (ASIACRYPT '01), PP. 239-254, Dec.2001.

[11]. N. Meloni, C. Negre, and M.A. Hasan, "High Performance GHASH Function for Long Messages," Proc. Int'l Conf. Applied Cryptography and Network Security (ACNS '10), pp. 154-167, 2010.