Grenze International Journal of Engineering and Technology, July 2018

Performance Analysis of AES-128 Bits, 192 Bits and 256 Bits using Reversible Logic

Rohini S. H[1], Nikhita M[2], Pooja A[3] and Rajashekar B.Shettar[4]
[1]Dept. of E&C, B.V.B CET, Hubli,Karnataka India,
[2]Dept. of E&C, K.L.E.Technological University, Karnataka,India,
[3]Dept. of E&C, K.L.E.Technological University, Hubli,Karnataka India,
[4]Dept. of E&C, B.V.B CET, Hubli,Karnataka India,
{ Rohini H,Rajashekar.Shettar, rohini_sh,raj}@bvb.edu, { Nikhita M,Pooja A, nikhitamatti,242pooja}@gmail.com

***Abstract*—The reduction of power dissipation remains one of the major goals in the VLSI circuit design for many years. Classical circuits shows power dissipation for every bit lost in computation. But, reversible circuits do not dissipate power as no loss of bits in the information. It has an application in diverse fields like low power CMOS design, optical communication, cryptography, quantum computing and nanotechnology. Cryptography is a vital part of securing private data and preventing it from being stolen. Cryptography algorithms are either symmetric or asymmetric depending type of secret keys used. Among existing symmetric cryptography algorithms, AES(Advanced Encryption Standard) widely used as it is non fiestal, symmetric, faster with good security. One of the important feature of AES algorithm is that, it supports both hardware and software implementation, which is not true in other algorithms. But AES do have attacks like brute force attack and side channel attack, which occurs mainly due to power dissipation and can be well addressed by using reversible logic as it gives zero internal power dissipation. The paper is intended to design AES with different key lengths (128 bit, 192 & 256) to increase the security level using reversible gates. The AES algorithm of 128, 192, 256 bits key length for cryptographic procedure has been simulated and verified on FPGA Virtex 5 ML505 board using Xilinx chipscope. Proposed 128bit AES uses less number of garbage, gates , ancilla inputs and reduced quantum cost in comparison with existing work (only for 128bit). Also design of 192bit & 256bit AES is proposed and analyzed for performance parameters, but no such work found in literature for comparison using reversible logic. Power and time consumed are also compared for different key lengths in this paper.**

***Index Terms*— Reversible logic, DES, 3DES, AES, BLOWFISH.**

I. INTRODUCTION

In recent years ,it is clear that quantum computing is proof of principle demonstrations to emerging as a technology. Landauer in the year 1960 demonstrated that, every information is lost in one bit, will dissipate kT*ln (2) joules of energy where, k defines Boltzmann's constant and k=1.38x10 -23 J/K, T is absolute temperature in Kelvin [12]. Heat energy is dissipated in basic combinational logic circuits for every bit, hence there is a loss of information. Therefore, energy conservative devices are needful in present day.

Grenze ID: 01.GIJET.4.2.507

Unconventional form of computing is called as reversible computing. Reversible computing is used for many applications like nanotechnology, quantum computer, low power CMOS, DNA computing, optical computing, computer graphics and communication. The reversible logic are also called lossless circuits as they dissipates no power. Future low power circuits are expected to use reversible logic to reduce power consumption. In a circuit, if there exists one to one mapping between inputs and outputs [1] then it is said to reversible.

In this work application chosen to apply the concept of reversible logic is in cryptography. Cryptography is required to achieve Confidentiality, integrity, and authentication. In the other words, it gives security against all threats. But history says there is constant struggle between the trade-offs of lowest implementation cost versus the required level of security. Algorithms are designed accordingly to provide highest degree of security. Some commonly used algorithms are DES, tripple DES, RSA, Blowfish, AES, Twofish, IDEA etc. The comparison of different algorithms is shown in Table 1. in terms of application, attack and features. Amongst all the AES is chosen to demonstrate the use of reversible logic to counter act the threats seen in **Table I**. AES is non fiestal, symmetric algorithm, which supports both hardware and software design. The type of attack which makes it insecure is brute force and side channel attack. Side channel attack is mainly due to the study of power dissipation pattern during the encryption process. As reversible logic results in low power, if AES is implemented using Reversible logic, side channel attack can be reduced. AES uses different round of operation depending on key length (128bit, 192bit, 256bit) i.e addround, byte substitution, shift rows and mix columns. And key expanded to generate new key in each round. Intermediate result is called as state at the end of each round [7].

TABLE I. COMPARISON OF DIFFERENT ALGORITHMS

	Features	Applications	Attacks
DES	16 Rounds (64bit message, 56bit key), fiestal Structure, Symmetric, slow and less power	Key storage and Encrypting indexed data	Differential and Linear Cryptanalysis and Brute
AES	128 bit plaintext, key: 16,24,32 Bytes, rounds: 10,12,14, non fiestal, symmetric algorithm, faster speed, good security and low power	File encryption, security for communication, LAN, Archive and Compression tool	Brute force attack and side channel attack
3DES	DES is repeated 3 times to enhance security, symmetric algorithm, slower, adaquate security and less power	Online Banking, Card swapping, cellular telephony, wireless LAN, Personnel communication	Key attack based on Operation
RSA	Asymmetric algorithm, faster and low security	Key exchange and digital signature	Brute force, mathematical, timing and cipher attack
Blow- fish	64 bit block size, 32 bits to 448 bits key,fiestal structure, symmetric algorithm, high speed, low power and high security	Audio file Encryption	Birthday attack and Brute force Attack

A. Reversible Logic

The special feature of reversible logic gate is that, it uniquely maps between input and output vectors. It means, the inputs can be uniquely recovered from the outputs. Also in reversible circuits fan out is not allowed as one to-many concept is not reversible. However fan-out can be achieved using Feynman gates [6]. Feynman gate which is a 2*2 matrix is shown in Figure 1. Quantum cost of a Feynman gate is 1. Since a fan-out is not allowed in reversible logic, this gate is useful for duplication of the required outputs.

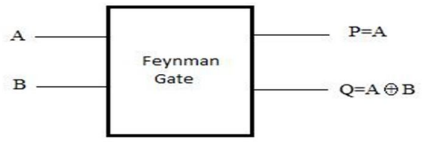

Figure 1. Feynman Gate

II. Design Implementation

Round Keys are required in both the encryption or decryption process. Rounds keys can be generated by expanding the initial key [4] or taken from look up table. The linear array 'W' is used to represent initial key. The AES standard supports different key length like 128bit, 192bit, 256bit but input block size remains as 128bit.

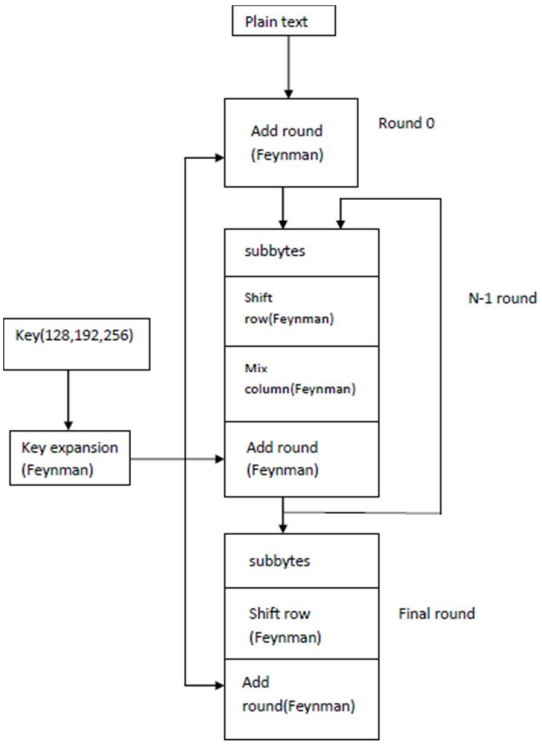

Figure 2. AES Flow chart

The 4 rounds are implemented using Reversible logic gates as shown in **Figure 2**. Each round are further shown in **Figure 3.** for Shift rotate round. **Figure 4.** for add round and mix column is intern a combination of left shift and xor operation. S box substitution, a memory is created as shown in **Figure 5.** where a value is taken and based on that a respective row and column substitution is taken [9].

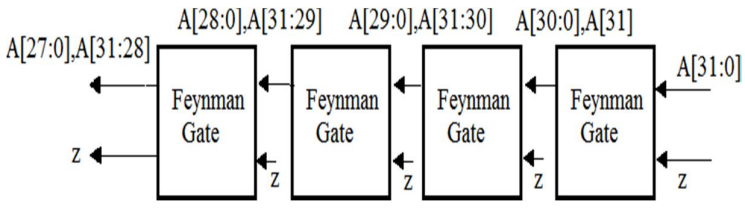

Figure 3. Reversible 4bit left shift register

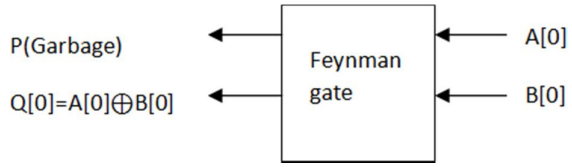

Figure 4. Reversible add round

III. Simulation Results

The reversible logic design of AES 128, 192 ad 256 bit is implemented and verified using verilog code on FPGA Virtex 5(ML505) board using Chipscope.

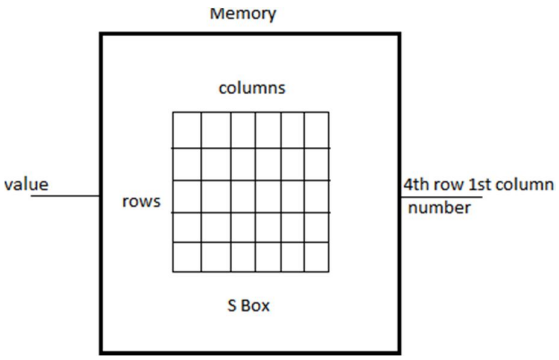

Figure 5. S-box

The simulation of 128 bits key length of AES algorithm using reversible logic gates in shown in the **Figure 6**.Input text 544F4E20776E69546F656E772020656F and key 5473206768204B20616D754674796E75 are taken and cipher text 2957401AC3142202502099D75ff6B33A is obtained and verified. Analysis of 128 bit key length is shown in the **Table II**. and is compared with a existing paper [9] as shown in **Table III**. The proposed method of 128 bit results in lesser number of gates, low garbage and QC.

The simulation of 192 bits key length of AES algorithm using reversible logic gates is shown in the **Figure 7**. Input text 004488cc115599dd2266aaee3377bbff and key 004488cc115599dd2266aaee3377bbff are considered and encrypted data dd866eeca94caf0d7cdf7071a4e0a091 is obtained. Analysis of 192 bit key length in terms ancilla, garbage, number of gates, quantum cost and gate used is shown in the **Table IV**.

The simulation of 256 bits key length of AES algorithm using reversible logic gates is shown in the **Figure 8**. Input text 004488cc115599dd2266aaee3377bbff and key 004488cc115599dd2266aaee3377bbff are taken and cipher text 8e51ea4ba267fc49b7454960b7454960cabf90b9 is obtained. Analysis of 256 bit key length in terms ancilla, garbage, number of gates, quantum cost and gate used is shown in the **Table V**.

No work found with respect to 192 and 256 bit AES using reversibile logic for comparison. Comparison with respect to Power and timing between 128, 192 and 256 bits is given in **Table 6**. It is observed that power consumed for 192 bits and 256 bits are more or less same. Therefore with same power more security can be achieved using 256 bit key length AES.

TABLE II. ANALYSIS OF 128 BIT KEY LENGTH

Rounds	Gate used	Garbage	Ancilla	Cost	No of gate
Key Expansion	Feynman	6400	0	6400	6400
Add Round 0	Feynman	128	0	128	128
Left Shift	Feynman	1280	0	1280	1280
Add Round 1	Feynman	1280	0	1280	1280
Mixed Column	Feynman	2304	0	2304	2304

TABLE III. 128 BIT AES COMPARISON WITH RESPECT TO GARBAGE AND QUANTUM COST(QC)

Rounds	Garbage (Paper [9])	QC (Paper [9])	Garbage (Proposed)	QC (Proposed)
Add Round	1408	1408	1280	1280
Left Shift	0	0	1280	1280
key generation	48320	1857600	6400	6400
Mixed Column	6624	17568	2304	2304

TABLE IV. ANALYSIS OF 192 BIT KEY LENGTH

Rounds	Gate used	Garbage	Ancilla	Cost	No of gate
Key Expansion	Feynman	10752	0	10752	10752
Add Round 0	Feynman	192	0	192	192
Left Shift	Feynman	2304	0	2304	2304
Add Round 1	Feynman	2304	0	2304	2304
Mixed Column	Feynman	4224	0	4224	4224

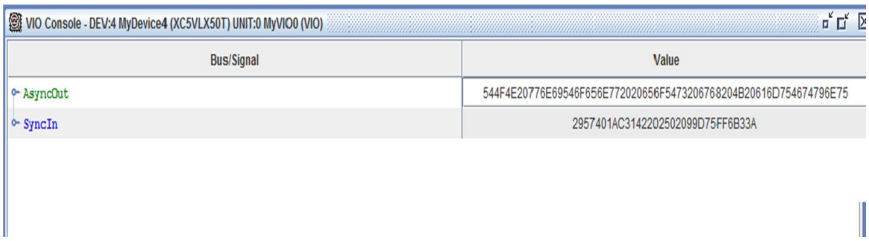

Figure 6. 128 bits Key length

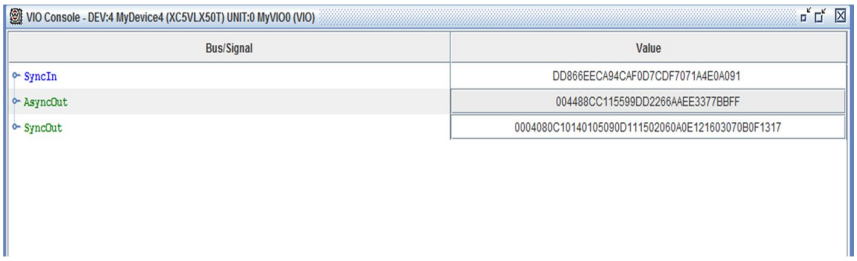

Figure 7. 192 bits Key length

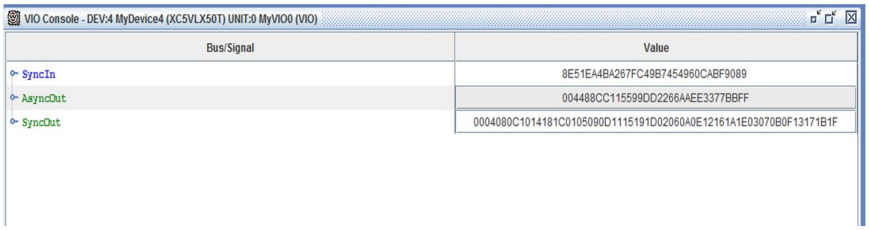

Figure 8. 256 bits Key length

TABLE V. ANALYSIS OF 256 BIT KEY LENGTH

Rounds	Gate used	Garbage	Ancilla	Cost	No of Gate
Key Expansion	Feynman	17920	0	17920	17920
Add Round 0	Feynman	256	256	256	256
Left Shift	Feynman	3584	0	3584	3584
Add Round 1	Feynman	3584	0	3584	3584
Mixed Column	Feynman	6656	0	6656	6656

TABLE VI. ANALYSIS OF POWER AND TIME IN TERMS OF DIFFERENT KEY LENGTHS

	128bit	192 bit	256 bit
Power (Watts)	0.503	0.523	0.524
Time (in sec)	6.073	34.404	40.137

IV. CONCLUSION

The reduction of power dissipation remains one of the major goals in the VLSI circuit design for many years. In this paper, the reversible logic is used to implement AES algorithm of 128, 192, 256 bits to reduce the power attacks. The results are verified on FPGA Virtex 5 ML505 board using Xilinx chipscope. Comparison of different key lengths w.r.t garbage, number of gates used, constant inputs and quantum cost is done. The proposed method of 128 bit results in lesser number of gates, low garbage and QC in comparison with existing work , as our work uses only Feynman gate in each round. No work found for comparing 192 and 256 bit AES implementation using reversible logic. Power consumed by 128bit AES found to be 0.5w and time taken for computation is around 6sec. Power calculated for 192bit and 256bit found to be around 0.523w and time taken around 36sec.

ACKNOWLEDGMENT

The authors wish to thank, head of the department, staff members, teaching and non–teaching staff for the successful completion of the paper.

REFERENCES

[1] Kosaraju, Naga M, " A VLSI architecture for Rijndael, the advanced encryption standard," National Conference on Information and Communication Technology., vol. 2003.
[2] Heron, Simon, " Advanced encryption standard (AES)," National Con- ference on Information and Communication Technology., vol. 2009.
[3] Yelekar, Prashant R and Chiwande, Sujata S and others, " Introduction to reversible logic gates & its application," National Conference on Information and Communication Technology., vol. 2011.
[4] Berent, Adam, " Advanced Encryption Standard by Example," National Conference on Information and Communication Technology., vol. June 2013.
[5] Verbauwhede, Ingrid and Schaumont, Patrick and Kuo, Henry, " Design and performance testing of a 2.29-GB/s Rijndaelprocessor ," IEEE Journal of Solid-State Circuits, vol.28 , 2003.
[6] Stallings, William, " Cryptography and network security: principles and practices", Pearson Education India , vol. 2006.
[7] Singh, Gurpreet, " A study of encryption algorithms (RSA, DES, 3DES and AES) for information security ", Foundation of Computer Science, vol.67, 2013.
[8] Bala, T and Kumar, Y, Asymmetric Algorithms and Symmetric Al- gorithms: A Review, International Journal of Computer Applications (ICAET), vol, 2015.
[9] Datta, Kamalika and Shrivastav, Vishal and Sengupta, Indranil and Rahaman, Hafizur, Reversible logic implementation of AES algorithm, Design &Technology of Integrated Systems in Nanoscale Era (DTIS), 2013 8th International Conference, vol, 2013.
[10] M.Bharathi, K.Neelima "Scope of reversible engineering at gate level, fault tolerant combinational adders" International Journal of VLSI design & Communication Systems (VLSICS),vol.03, No 02 , Apr 2012.
[11] B.Raghu kanth, B.Murali Krishna, M. Sridhar, V.G. Santhi Swa- roop "A distinguish between reversible and conventional logic gates"International Journal of Engineering Research and Applications (IJERA),Vol.02, Issue 2, Mar-Apr 2012.
[12] R. Landauer "Irreversibility and heat generation in the computational process"IBM Journal of Research and development ,Vol.02, Issue 5, 1961.
[13] H.Thapliyal, N. Ranganathan "Design of reversible sequential circuits optimizing quantum cost, delay and garbage outputs" ACM Jour- nal of Emerging Technologies in Computing Systems,Vol.06, Issue 4, pp.14:114:35, 2010.