ISSN 2278-5612

A Review Paper on Comparative Study of FPGA Implemented AES, Rijndael AES and Pipelined AES Algorithms for Secure Adhoc Networks

Pooja Srivastava[1], Seema Verma[2], Abhilasha Agarwal[3], Pooja[4], Shradha Gupta[5]

[1]Assistant Professor, Department of Electronics, Banasthali University, India.
pooja_enn@yahoo.co.in
[2]Assosiate Professor, Department of Electronics, Banasthali University, India.
seemavema3@yahoo.com
[3]Student, M.Tech (VLSI Design), Banasthali University, India.
abhilasha.agarwal1@gmail.com
[4]Student, M.Tech (VLSI Design), Banasthali University, India.
poojadhingra7@gmail.com
[5]Student, M.Tech (VLSI Design), Banasthali University, India.
shradhagupta1289@gmail.co

ABSTRACT

Cryptographic techniques are necessary for the security of Adhoc Network. These cryptographic Algorithms are obligatory for protection of the user data so that only the permitted user are allowed to access it. This review paper outlines the comparison of various algorithms i.e AES, Rijndael AES and Pipelined AES. These algorithms estimate the performance on the basis of data throughput and clock frequency.

Indexing terms/Keywords

Adhoc Networks, Cryptography, VLSI, FPGA

Academic Discipline and Sub-Disciplines

Wireless Communication, VLSI Design

SUBJECT CLASSIFICATION

Security studies

TYPE (METHOD/APPROACH)

Conceptual paper

Council for Innovative Research

Peer Review Research Publishing System

Journal: International Journal of Management & Information Technology

Vol. 9, No. 3
editor@cirworld.com
www.cirworld.com, member.cirworld.com

INTRODUCTION

An adhoc network is formed by the combination of nodes without having access point and information are exchanged and passed from one node to another node. Communication between the nodes is possible even they are not in the transmission range of each other.

An adhoc networks offers many benefits as user mobility, rapid installation, flexibity and scalability. When the infrastructure is exploited by some unbalanced environmental conditions, in that case, an adhoc networking helps us to stabilize a temporary network. An adhoc network can be characterize with dynamic topologies, limited bandwidth, and limited physical security and decentralized administration. Movement between the nodes is possible due to dynamic topologies. Arbitrary movement of nodes at any time is responsible for the broken links in the network. This prominent feature of adhoc networks makes it difficult to set up secure key distribution. As opposed to wired networks, adhocs nodes are more often part of a frequent changing environment that is not maintained professionally so that network is exposed to attacks ranging from physical attacks to eavesdrop due to the transmission range which exceeds the area where the network is deployed. Secured data is becoming an important factor for many applications in wireless communication. An encryption algorithm is in need now days to provide resistance against attack. When a new attack is established as effective, the update of the encryption system is a real obligation to guarantee the security of data [1]-[3].

The National Institute of Standards and Technology (NIST) has published the specifications for the Advanced Encryption Standard (AES) in the Federal Information Processing Standards (FIPS) [1].

Different versions of AES algorithm exist today depending on the size of the encryption key. In this review paper, a hardware model for implementing the AES 128 algorithm has developed using the VHDL. DES (Data Encryption Standard) has come before AES and used as a cryptographic technique for security algorithm. AES provide the protected efficient data with good reliability. The key size is an important issue for determining the security of the system. According to the demand of market, it is very difficult to achieve area consumption, throughput and security all together at the same time [4]-[8].

Any encryption algorithm when implemented by software has significant disadvantages because of less parallelism in software and word size variation on dissimilar operating systems. In addition, it does not accomplish the necessary speed for time critical encryption applications. Due to the shortcomings in the software implementation, encryption algorithm had adopted the hardware implementation as an alternative. These algorithms provide the eventual secrecy to the encryption key, faster speed and more efficiency to the systems. In today scenario, to achieve the desired performance an FPGA implementation is still meeting their cost, timing and power goals. According to the time-to-market concern, FPGA technology offers good performance, flexibility and rapid prototyping capabilities.

AES ALGORITHM

AES is a symmetric block cipher which provides the encryption and decryption of the information. Encryptor converts the original data to a form which is not understandable by the user called cipher text and decryptor convert the data into its previous form known as plain text. There is a key associated with each cipher and inverse cipher operation. There are various key lengths are available for AES algorithm i.e., 128, 192 and 256-bits but the block size is fixed which is of 128 bits. Encryption consists of number of rounds depending upon the key size [9]. All the rounds in the AES algorithm are alike excepting the last round. Each round consists of an input state array and gives an output state array. All the operations are processed the state array and finally the output state array produced by the last round is converted back to the bits. AES decryption is not as same as encryption but corresponding to an inverse cipher uses the same method which has adopted for encryption process but the key will be determine by the different criteria. For the protection of the data, we have to highly depend on the key length. Higher will be key length of the algorithm, more will be the security of the system [10]-[11].

FPGA IMPLEMENTATION OF AES ALGORITHM

AES algorithm uses the key of 128-bit size i.e. 16 bytes which can be ordered as 4x4 matrix. This algorithm contains a Add round key and having nine regular rounds which consist of four modules and last round. These four module are named as- Sub-byte transformation, Shift rows transformation, Column mix and Add round key. The last round do not have column mix module.

The four modules are described as:

Sub-byte Transformation

It is a non-linear substitution of bytes which is operated on each state bytes independently. An S-Box is obtained from look-up table which provide the Sub-bytes transformation [12].

Shift rows Transformation

The transformations are carried out on each of row and the data is changing by different offsets. Decryption process is quite same except that the shifting offsets have altered their values.

Column mix Transformation

Each column is operated individually. It is a mixing process which combines the four bytes in each column and forms a new value. A Column mix operation is dot operation performed according to the Galois Field (GF) rule [11].

Add round Transformation

In this, Xoring operation is done between state and the round key with each has the size of 128-bits. This will effect the every bit of state. This transformation is operated as column wise between the one word of round key and four byte of a state column.

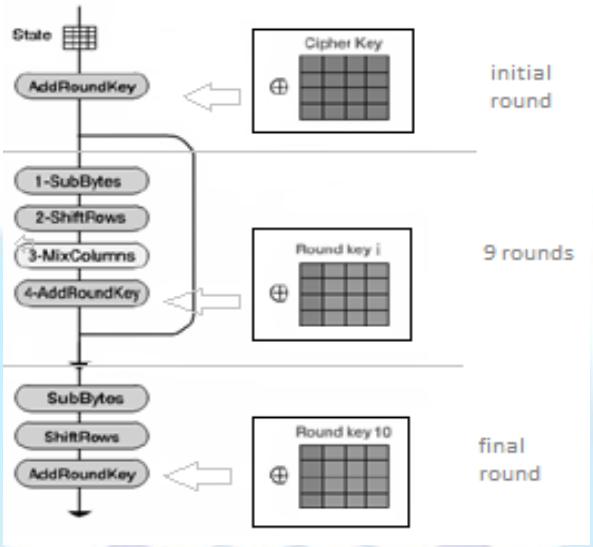

Fig 1. VLSI Architecture for Encryption of AES Algorithm [13]

RIJNDAEL AES ALGORITHM

Rijndael AES is also symmetric block cipher algorithm. The input/output sequences having the same length in Rijndael AES. Length referred to the number of bits in any sequence. In Rijndael AES algorithm, block size and key length can be of any allowed values. AES requires the block size of 128 bits but the Rijndael cipher can work with variant of block size which are the product of 32 bits, which are having the range between 128 to 256-bits. The state array for the different block size in the Rijndael cipher has four rows but the columns number vary according to the block size [14].

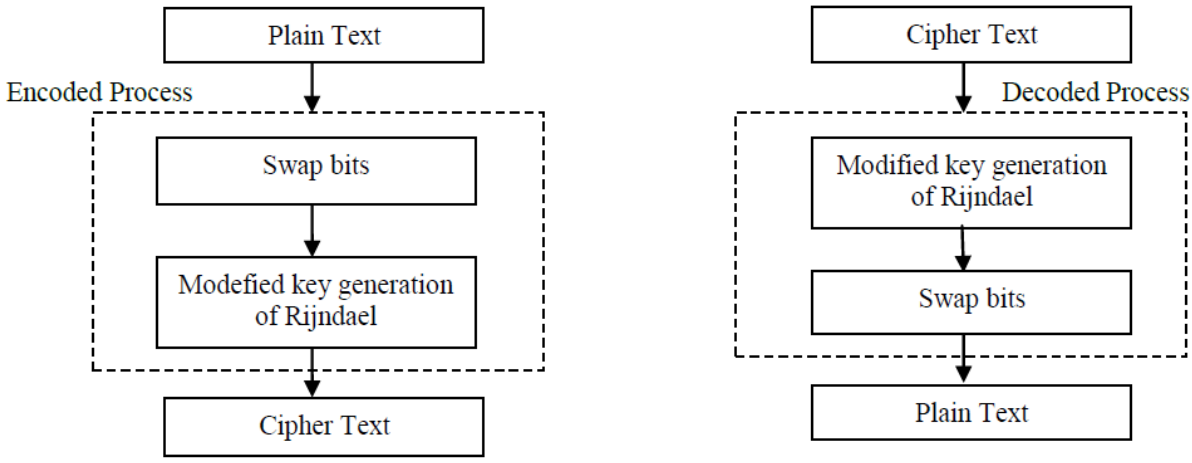

Fig 2. Flow Chart of Rijndael AES Algorithm [14]

FPGA IMPLEMENTATION OF RIJNDAEL AES ALGORITHM

Rijndael was selected for AES standard because of its various advantages of providing the secure data with high flexibility and quick response towards data. To provide good efficiency to the system we preferred to use the larger

block size. Rijndael AES algorithm has the good key scheduling capability while mainitaing the performance. It also requires less memory for implementation. Rijndael is same as an AES except having extra feature of variable block size. All transformations in algorithm operate on the state. 128-bit key has initial Data/Key Addition and 9 rounds transformation and the scheduling of key. This will provide key to all the 9 round so that a different round key is created for each iteration.

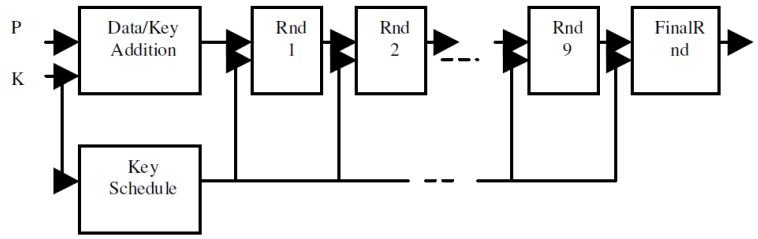

Fig 3. Rijndael Encryption Algorithm

PIPELINED AES ALGORITHM

The technique of pipelining is adopted in designing the network for maximising their throughput by using a number of parallel operations in a given time. AES algorithm emphasis on pipelining to increase its throughput. Parallel processing is being performed by several inputs which will process several outputs with increased sample rate. In pipelining, data transmission has changed in this design. All the data 128-bit plain text, 128-bit initial key and 128-bit final text key, splited into four 32-bits units which are guarded by the clock. The AES algorithm consists of four block, but here we are focussing on the design of high performance architecture for all these operations. In pipelined AES algorithm, we had adopted the high speed implementation of Sub-byte / Inverse Sub-byte transformation and hardware sharing implementation of Column mix / Inverse Column mix transformation [15].

FPGA IMPLEMENTATION OF PIPELINED AES ALGORITHM

AES algorithm has implemented on FPGA using VHDL as a programming language. In the implementation of the pipelined AES FPGA implementation of 128-bit AES provide the high speed and high throughput. By adopting the pipelining in the algorithm reduce the time of hardware. In non-pipelined architecture, time taken by the hardware is more than the pipelined. In AES 128 bits, there are 10 rounds and the data given as input has to pass through these 10 rounds. In pipelined AES algorithm, second data do not have any need to wait until first data completes its 10 rounds [13]. Different pipelining stage implementation of AES algorithm corresponding to the variation in throughput, area and power for both encryption and decryption.

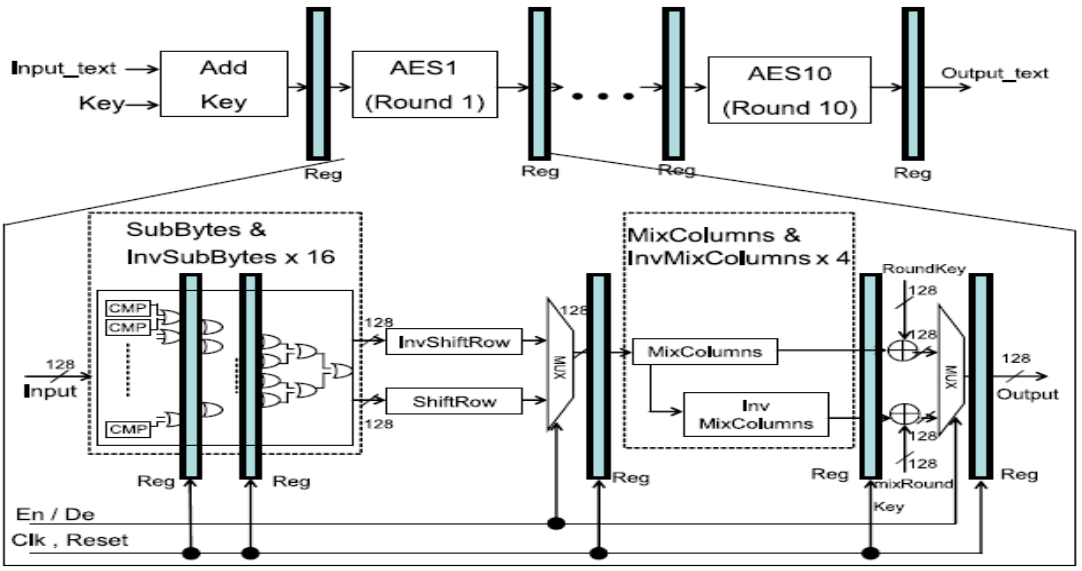

Fig 4. VLSI Architecture of Pipelined AES processor [16]

COMPARATIVE STUDY

In the following table, the comparison of these Algorithm according to data throughput and frequency as shown :

Table 1. Comparison Table[13],[16]

	AES	Rijndael AES	Pipelined AES
Data Throughput	31 Mbps	280 - 450 Mbps	28.4 Gbps
Frequency	21.2 MHz	64 MHz	222.2 MHz

CONCLUSION

An optimal AES, Rijndael AES and Pipelined AES has designed according to the high throughput and high clock frequency. The analysis has made the decision that the speed has increased by the use of pipelining in the sub-byte block. Pipelining provide the maximum frequency and high throughput as compared to others.

ACKNOWLEDGMENTS

This work is supported by Department of Electronics, Banasthali University, Rajasthan, India.

REFERENCES

[1] NIST (National Institute of Security and Technologies), Wireless Network Security 802.11, Bluetooth and Handheld Devices, Technical report.

[2] Shariful Islam. Stockholm, Sweden, 2005, "Efficient Key Management Scheme for Mobile Adhoc Network". Master of Science, Royal Institute of Technology (KTH) SecLab, Department of Computer and System Science (DSV).

[3] Paul Muhlethaler, 2005, Security Schemes for the OLSR Protocol for Adhoc Networks, doctoral thesis, University Paris.

[4] Daemen, J and Rijmen, V., June 1998, “AES Proposal: Rijndael NIST AES Proposal",Technical report.

[5] National Institute of Standards and Technology (U.S.), “Advanced Encryption Standard (AES)", Technical report.

[6] ANSI (American National Standards Institute), 1998, "Triple Data Encryption Algorithm Modes of Operation", Technical report.

[7] National Institute of Standards and Tehnology (U.S.),1999, "Data Encryption Standard (DES)". FIPS Publication 46-3, Technical report.

[8] Rubra A, Dubey P.K., Jutla C.S., Kumar V, Rao J.R. and Rohatgi P., "Efficient Rijndael Encryption Implementation with Composite Field Arithmetic", Lecture Notes in Computer Science 2162, 2001, pp. 171-184.

[9] Manjesh K.N., Karunavathi R.K., "Secured High Throughput Implementation of AES Algorithm"IJARCSSE, May, 2013.

[10] Prasanthi O., Reddy M. S., "Enhanced AES Algorithm", IJCAES, June, 2012.

[11] Prof. Venkateswarlu S., Deepa G.M. and Sriteja G., "Implementation of Cryptographic Algorithm on FPGA",IJCSMC, Vol.2, Issue. 4, April 2013, Pg. 604-609.

[12] Ahmad N., Hasan R. and Jubadi W.M., "Design of AES S-Box using comnbitional logic optimization",IEEE Symposium on Industrial Electronics & Applications (ISIEA), pp. 696-699, 2010.

[13] Sharmila D. and Neelaveni R., "Performance Evaluation of VHDL Implementation of Proposed SAFER+ Security Algorithm and Pipelined AES Security Algorithm for Bluetooth Security Systems", ICGST-CNIR Journal, Vol.9, Issue1, July 2009.

[14] HmoodDalalNaeem, "A Random Key Generation Approach for Rijndael Algorithm", Journal of Al-Nahrain University Vol.15 (3), September, 2012, pp. 190-195.

[15] Mg. Suresh and Dr. Nataraj. K.R, "Area Optimized and Pipelined FPGA Implementation of AES Encryption and Decryption", IJCER(online), November 2012, Vol. 2, Issue 7.

[16] Fan Chih-Peng and Hwang Jun-Kui, "FPGA Implementations of High Throughput Sequential and Fully Pipelined AES Algorithm",International Journal of Electrical Engineering, Vol.15, No.6, pp.447-455, 2008

Author' biography

PoojaSrivastava is currently working as Assistant Professor in Department of Electronics at Banasthali University, Rajasthan, India. She received her B.Tech. degree in Electronics and Communication Engineering from Uttar Pradesh Technical University, Lucknow, U.P., India in 2006 and M.Tech (VLSI Design) from Banasthali University, Rajasthan, India in 2009. She has five year research interest includes Adhoc Networks, Wireless Communication Systems, Turbo Codes, VLSI Design and Fabrication Technology.

Dr. SeemaVerma obtained her Master and Ph.D degree in Electronics from Banasthali University in 1999 &2003. She is currently working as Associate Professor of Electronics and Head, Department of Aviation Sciences at Banasthali University. She is Fellow of IETE, Life Member of Indian Science Congress, Life member of International Association of Engineers, (IAENG). She is in the Pearl edition of Who's Who in the World (2013). She is an active research supervisor and 4 Ph.Ds have been awarded under her guidance. She has been frequently invited to present invited or plenary keynote lectures at international conferences in India & abroad. She has presented many papers in various international conferences. She has published many research papers in various journals of repute. She has many projects from UGC (under R&D Major research project scheme, UGC Innovative Course Scheme) & AICTE to her credit. She is currently into the editorial board of many international journals in the field Wireless Communication and Coding. Her research areas are Coding theory, TURBO Codes, Wireless sensor networks, Aircraft Ad-hoc networks, Network Security& VLSI Design.

Abhilasha Agarwal received her B.Tech. degree in Electronics and Communication Engineering from Rajasthan Technical University, Kota, India in 2011. Currently, she is persuingM.Tech (VLSI Design) from Banasthali University, Rajasthan, India. Her research interest includes Adhoc Networks, VLSI Design and Wireless Communication Systems.

Pooja received her B.Tech. degree in Electronics and Communication Engineering from MaharashiDayanand University, Rohtak, Haryana, India in 2013. Currently, she is persuingM.Tech (VLSI Design) from Banasthali University, Rajasthan, India. Her research interest includes Adhoc Networks, VLSI Design and Wireless Communication Systems.

Shradha Gupta received her B.Tech. degree in Electronics and Communication Engineering from Banasthali University, Rajasthan, India in 2011. Currently, she is persuingM.Tech (VLSI Design) from Banasthali University, Rajasthan, India. Her research interest includes Adhoc Networks, VLSI Design and Wireless Communication Systems.