www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN: 2319-7242*
*Volume 4 Issue 12 Dec 2015, Page No. 15403-15405*

# A Review Paper on Effective AES Implementation

***Ayushi Arya***
Dept. of Electronics & Communication Engineering
Royal Institute of Management & Technology
Gohana, Panipat , India
aarya8999@gmail.com

*Abstract*—**Protecting information in potentially averse environments – is a crucial factor in the growth of information-based processes in industries, business, and administration as information is the most important asset of an organization. Cryptography is basically practice and study of techniques for secure communication in the presence of third parties (called adversaries). The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Like DES, AES is a symmetric block cipher. However AES is different from DES in a number of ways. The algorithm Rijndael allows for a variety of block and key sizes. It is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. This review paper concentrates on framing together efficient implementation of AES algorithms in number of fields. The study also focus on number of ways to expedite the encryption process by using different approaches.**

**Keywords- Cryptography, Encryption, Decryption, AES, DES**

## Introduction

Information security has assumed a significant importance in today's world, especially because minor breaches can lead to major risks in the fields of national security and other e-commerce applications and transactions. Now whole world is moving towards network. With the rapid spread of digital communication networks, there is a great need for privacy and security. Modern cryptography is the corner stone of computer and communications security. Its foundation is based on different concepts of mathematics such as number theory, computational-complexity theory, and probability theory. Cryptography is a process to hide/lock the data for security reasons. Five main aims of cryptography are: Authentication; Privacy; Integrity; Non-repudiation; Service reliability. Cryptography is categorized in two types : Symmetric and Asymmetric.
Symmetric (Private Key) Cryptography - Same key used for encryption & decryption.
Asymmetric (Public) Cryptography – Different keys are used for encryption & decryption.
**Advance Encryption Standards algorithm** - Amongst various cryptography techniques as DES, 3-DES, International data encryption algorithm & AES, AES is the most recent algorithm approved for federal in the United States by the National Institute of Standards and Technology (NIST) and widely accepted to replace old standard DES. Unlike DES, AES is not a Feistel cipher. It works in parallel over the entire input block. AES is defined to be efficient in both hardware as well as software across number of platforms. It's a block cipher which works in iterative manner. In AES algorithm block size can be 128, 192 or 256 bits. Key length can be 128,192 or 256 bits.

## Literature Review

Xinmiao Zhang and Keshab K. Parhi works on, "**Implementation approaches for the advanced encryption standard algorithm", IEEE Transactions 1531-636X/12©2002IEEE** and addresses efficient hardware implementation approaches for AES algorithm. Their work done revealed that as compared to software implementation, hardware implementations provides more physical security along with high speed.[1]
To increase the secrecy in communication **A Proposal for key dependent AES was proposed by A. Fahmy ,2005.** This work introduces a new, key-dependent Advanced Encryption standard algorithm, **KAES,** to expand the key-space to slow down attacks. KAES is block cipher in which the block length and the key length are specified according to AES specification: three key length alternatives 128, 192, or 256 bits and block length of 128 bits. In this paper, a key length of 128 bits is being used, which is likely to be the one most commonly implemented and the input to the encryption and decryption algorithms is a single 128-bit block, this block is depicted as a square matrix of bytes. So the algorithm improved the security of AES by employing the key to be the main parameter of the algorithm**.[2]**

In order to prevent the Advanced Encryption Standard (AES) suffering from differential fault attacks **Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard by C-H Hen (2006),** the technique of error detection can be adopted to detect the errors during encryption or decryption and then to provide the information for taking further action, such as interrupting the AES process or redoing the process. Because errors occur within a function, it is not easy to predict the output**.** In this work, several error-detection schemes have been proposed. These schemes are based on the (n+1,n) cyclic redundancy check (CRC) over GF(2^8**).[3]**

**Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul. Elminaam et.al., (2009)** which represents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results. First; in the case of varying packet size with and with out transmission of data using different architectures and different WLANs protocols, was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. DES and 3DES are known to have worm holes in their security mechanism, Blowfish and AES do not have any so far**. [4]**

Enhancing the performance of Rijndael algorithm **A Faster Version of Rijndael Cryptographic Algorithm Using Cyclic Shift and Bit Wise Operations by Fakiriah Hani Mhd. Ali in 2009.** This encryption standard uses KeyExpansion, ByteSub, Mixcolumn and Shiftrow functions which consists of XOR, inverse, multiplying and swaps modules. **[5]**

**New Comparative Study Between DES, 3DES and AES within Nine Factors by Hamdan O.Alanazi in 2010** represents a new comparative study between DES, 3DES and AES were presented in to nine factors, Which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, possible ACSII printable character keys, time required to check all possible key at 50 billion second, these eligible's proved that AES is better than DES and 3DES. **[6]**

Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani**, "A New Modified Version of Advance Encryption Standard (AES) Based Algorithm for Image Encryption" (2010) [7].**

**Performance Analysis of AES and MARS Encryption Algorithms by Mohan H.S. IN 2011** illustrates measured diffusion value of AES and MARS algorithms. As each cipher uses several rounds of fixed operations to achieve desired security level. The security level is measured in terms of diffusion and confusion. The diffusion level should be at least equal to strict avalanche criterion (SAC) value. Therefore, the numbers of rounds are chosen such that the algorithm provides the SAC value. Diffusion values are compared for both the algorithms: AES and MARS. **[8]**

The implementation of Advance encryption (AES) algorithm using parallel computing as performed in **Improved Performance of Advance Encryption Standard using Parallel Computing (2012)"**This paper presented. Most of the research for improving performance of AES is based on hardware implementation. This paper presents the parallel implementation of AES using JPPF (Java Parallel Programming Framework) which provides flexibility & performance improvement in terms of speed-up. In this implementation there are two approaches data parallelism and control parallelism**.[9]**

Chong HeeKim's **"Improved Differential Fault Analysis on AES Key Schedule" IEEE Transaction on Information Forensics and Security, Vol. 7, No. 1, Feb 2012.** Research on DFA has been diversified into several directions: reducing the number of required faults, changing fault models (from one-byte fault to multibyte fault and *vise versa*), extending to AES-192 and AES-256, and exploiting faults induced at an earlier round. This paper deals with all these directions together in DFA on AES Key Schedule. We introduce new attacks that find the AES-128 key with two faults in a one-byte fault model without exhaustive search and the AES-192 and the AES-256 keys with six and four faults, respectively**.[10]**

Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang and Cheng-Wen Wu proposed, "**A Highly Efficient AES Cipher Chip", IEEE ASP-DAC2003,pp.561-562.** In this author presented a high throughput, area efficient implementation of the AESalgorithm. The complexity of the S-box is greatly reduced by a basis transformation from Gf (28) to GF (24). There is a 64% area reduction in S-box and about 50% total area reduction as compared with the previous LUT approaches. The pipelined AES chip provides a very high throughput while keeping the area small. In addition, the design can also perform key expansion on-line. With the standard on-chip bus interface, the AES cipher can be plugged into the system chip easily. Finally, testability has been stressed in the proposed design**.[11]**

Mahdi Nazm-Bojnordi, Naser Sedaghati-Mokhtari and Seid Mehdi Fakhraie, has performed **"A Self-Testing Fully Pipelined Implementation for the Advanced Encryption Standard", IEEE ICM2005, pp. 260-263**. In this author implements a fast fully pipelined architecture for the AES encryption method is implemented that is suitable for securing data exchange in real-time applications such as video encryption. A brief analysis of AES implementations and a testable unrolled pipelined implementation for AES is presented. The design is synthesized using a 0.35 um ASIC library, for which a delay less than 20 ns is extracted for each pipeline stage of the design. Therefore it can achieve a

maximum throughput of 6 Gbps. With the added BIST architecture test coverage of about 98% is obtained.**[12]**

**FPGA Based Implementation of AES algorithm by Ashwini R. Tondey and Akshay P.Dhandhe in 2014** proposed FPGA based implementation of the Advanced Encryption Standard (AES) algorithm is presented in this paper. The design has been coded by Very high speed integrated circuit Hardware Descriptive Language. All the results are synthesized and simulated using Xilinx ISE and ModelSim software respectively.[**13]**

**128 Bit Advance encryption standard algorithm with fault detection by Ruchi R. Vairagade, Prof Shubhangini Ugale & Prof. Prachi Pendke in 2014 represents an** 128 bit AES algorithm since it will accepts 128 bits of plaintext and master key of size128 bits. The 128 bits cipher text block is produce afterplaintext block is processed by round function number of times. This algorithm uses a combination of Exclusive-OR operation (XOR), Substitution with S-Box, Row and Column rotation and a Mix column. Plaintext, ciphertext and intermediate state block can be depicted as 4*4 matrix form. In this paper, in the proposed work present the details of the 128 bits AES Encryption and Decryption structure and conduct afault injection attack against the unprotected AES. The methodology to be employed is VHDL. **[14]**

## Conclusion

In this paper the existing AES algorithm implementation is done at various platforms to achieve better results. AES with number of technologies are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the methods are useful for real-time encryption enhancing the performance parameters of AES algorithm. Each technique is unique in its own way, which might be suitable for different applications. Everyday new methods for implementing AES are evolving hence fast and secure conventional encryption techniques will always work out with high rate of security and improved performance parameters as encryption time, decryption time and through put at encryption or decryption end.

## References

[1] Xinmiao Zhang and Keshab K. Parhi works on, “Implementation approaches for the advanced encryption standard algorithm”, IEEE Transactions 1531-636X/12©2002IEEE

[2] Fahmy A., Shaarawy M., El-Hadad K., Salama G. and Hassanain K., “A Proposal For A Key-Dependent AES”, SETIT, Tunisia, 2005.

[3] Simple Error Detection Methods for Hardware Implementation of Advanced Encryption Standard by C-H Hen (2006),

[4] DiaaSalama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud,” Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices” International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009.

[5] Fakariah Hani Mohd Ali, Ramlan Mahmod, Mohammad Rushdan and Ismail Abdullah, “A Faster Version of Rijndael Cryptographic Algorithm Using Cyclic Shift and Bit Wise Operations” International Journal of Cryptology Research 1(2): 215-223 (2009)

[6] New Comparative Study Between DES, 3DES and AES within Nine Factors Journal of Computing, Volume 2, Issue 3, MHarch 2010, ISSN 2151-9617 by Hamdan O.Alanazi in 2010, B.B. Zaidan, A.A. Zaidan, Hmide zalab. M. Shabbir

[7] Seyed Hossein Kamali, Reza Shakerian, Maysam Hedayati, Mohsen Rahmani, “A New Modified Version of Advance Encryption Standard (AES) Based Algorithm for Image Encryption” (2010) [7].

[8] Mohan H.S and A RajiReddy,”Performance analysis of AES and MARS encryption algorithm” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[9] Improved Performance of Advance Encryption Standard using Parallel Computing (2012)

[10] Chong HeeKim,”Improved Differential Fault Analysis on AES Key Schedule” IEEE Transaction on Information Forensics and Security, Vol. 7, No. 1, Feb 2012

[11] Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang and Cheng-Wen Wu, “A Highly Efficient AES Cipher Chip”, IEEE ASP-DAC2003,pp.561-562

[12] Mahdi Nazm-Bojnordi, Naser Sedaghati-Mokhtari and Seid Mehdi Fakhraie “A Self-Testing Fully Pipelined Implementation for the Advanced Encryption Standard”, IEEE ICM2005, pp. 260-263”

[13] FPGA Based Implementation of AES algorithm by Ashwini R. Tondey and Akshay P.Dhandhe, International journal of advance research in computer and communication engineering, Volume 3, Issue 1, 2014

[14] 128 Bit Advance encryption standard algorithm with fault detection by Ruchi R. Vairagade, Prof Shubhangini Ugale & Prof. Prachi Pendke

[15]William Stallings “ Network Security Essentials (Applications and Standards)”, Pearson Education, 2004.

[16] National Bureau of Standards, “ Data Encryption Standard,” FIPS Publication 46, 1977.

[17] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.