International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

Novel Advanced Encryption Standard (AES) Implementation approach using Genetic Algorithm

Amit Nevase[1], Nagnath Hulle[2]

[1]*Student, Department of Electronics & Telecommunication, GHRIET, Pune, Maharashtra, India*
[2]*Vice Principal, Department of Electronics & Telecommunication, GHRIET, Pune, Maharashtra, India*

Abstract - *During the last few years, in the field of electronic data transmissions cryptography has vital importance. Advanced Encryption Standard (AES) designated by National Institute of Standards and Technology (NIST), to overcome the disadvantages of Data Encryption Standard (DES). The AES is widely used encryption algorithm in different security applications. The AES standard uses key size of 128, 192 and 256 bit to provide more secure data. AES generates keys through the properties of the Rijndael Algorithm instead of conventional method of the key generation. This paper introduces a new encryption technique where the Genetic Algorithms are used for key generation, this generated key is used for formation of S-Box. This new approach for AES S-Box to enhance the complexity of the structure of S-Box, making AES stronger by using Dynamic S-Box. In the hardware aspect, larger key size also means large area and minimum throughput. Advance Encryption algorithm can be relatively efficiently implemented in software on general-purpose processors, there is still a need for selection of better architecture for implementation of Advanced Encryption Standard.*

Key Words: **Advanced Encryption Standard (AES), Genetic Algorithm, Dynamic S-Box**

1. INTRODUCTION

"Cryptography" refers to the change of information presentation from its unique structure into one another distinctive structure. The main goal is to make information more secured. The two main procedures are involved in Cryptography; the principal procedure is the encryption and decryption. Data Encryption Standard (DES) [12], the Elliptic Curve Cryptography (ECC) [12], the Advanced Encryption Standard (AES) [12] are the different cryptographic algorithm. The brute force were attempted to break such algorithms. Also some and side channel attacks are used to break such algorithms. The brute force attacks break the data encryption standard and made it uncertain algorithm. To replace Data Encryption Standard, National Institute of Standards and Technology (NIST) searched for another algorithm and Rijndael Algorithm is selected as next AES.

Nowadays, Advanced Encryption Standard was most secured cryptographic algorithm, used by NIST after Data Encryption Standard. The Advanced Encryption Standard algorithm has widely used in RFID cards, firewalls, routers, firmware, UART, ATM machines, cellular phones and big servers. The AES algorithm has vital importance and hence the main aim of project is to present new efficient and more secure hardware architecture implementation of AES algorithm. To implement hardware of AES algorithm, Field programmable Gate Arrays (FPGA) are used because they provide cryptographic algorithm agility, physical security, better performance. The main aim is high throughput which supports security and high bandwidth for various applications.

2. OBJECTIVES AND BLOCK DIAGRAM

The Advanced Encryption Standard is most secured cryptographic algorithm nowadays. After failure of Data Encryption Standard, National Institute of Standards & Technology adopts AES. It is widely used cryptographic algorithm. The main focus on high throughput which supports security and high bandwidth for various applications. Considering importance of this work following objectives are defined.

1. S-Box generation based on Round Key
2. Development of novel algorithm using Advanced Encryption Standard and Genetic Algorithm to increase security.
3. Study of different hardware platforms to select suitable hardware platform for implementation.

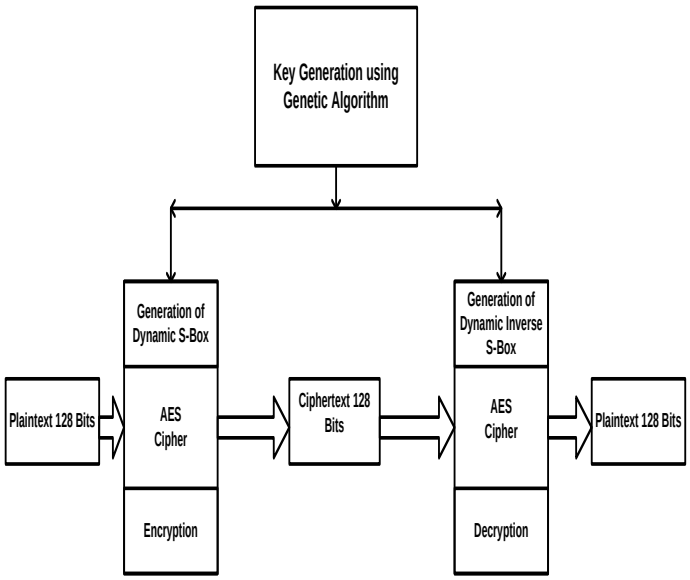

Figure 1 Modified Structure

3. LITERATURE REVIEW

In [5], author presents a new optimization algorithm. The Genetic Algorithm is used. It is used for problem solving through genetic operators.

In [6], author presents Genetic Algorithms for cryptanalysis. The classical cryptosystems are changed by using Genetic Algorithms. The different genetic operators are used to make more secure algorithm. The genetic operators are mutation, selection. The best fit key is selected by using fitness function.

In [7], author presents a new algorithm that focus on generation and expansion of encryption key of the Advanced Encryption Standard. The key generation is the most important process in cryptanalysis. Author presents a new architecture that generates different keys. The new key generator architecture includes Genetic algorithm and Linear feedback shift register. It improves performance and efficiency of new algorithm. To implement these Altera Cyclone II architecture is studied with VHDL language.

In [10], this paper author proposes a new method of use of genetic algorithms along with pseudorandom sequence for encryption. High data security is the features of this new algorithm. Also it provides high feasibility. Hence it is useful in commercial multimedia applications. Results indicate that proposed system gives high throughput and real time data security.

In [13], author discusses the enhancement of the AES algorithm and describes the process, which involves the generation of dynamic S-boxes for Advance Encryption Standard. The newly generated key dependent S box is more dynamic. It is difficult for the linear and differential cryptanalysis.

4. ADVANCED ENCRYPTION STANDARD

The two Scientists from Belgian Vincent Rijmen and John Daemen [1] was publish a cipher Rijndael in 1998. After the failure of Data Encryption Standard, the Rijndael [1] was selected as Advanced Encryption Standard. The AES overcomes the disadvantages of DES. Under the Federal Information Processing Standards Publication 197 (FIPS), the National Institute of Standards and Technology (NIST), discuses all the information of AES. The Advanced Encryption Standard has a data size 128 bits i.e. 16 bytes with different key sizes of 128 bits, 192 bits and 256 bits. The key size is depends upon the number of encryption rounds. The 128 bit key size for 10 round, 192 for 12 and 256 for 14 rounds. The 128 bit data is formed in 4 X 4 array, which is called State Array, is used in encryption process. The initial data is converted into state array during the encryption process, after each round these data is changing until reached to final cipher text. During the decryption process, these cipher text array is keep changing to obtain original data. In every round of encryption and decryption process, new round key is generated using the initial key applied. The round structure of Advanced Encryption Standard shown in fig. 2

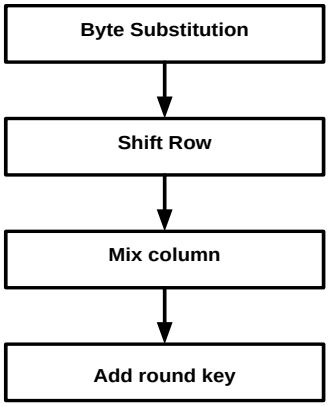

Figure 2 AES Round Structure

The Advanced Encryption Standard structure with round 0 through 10 is shown in Figure 3.

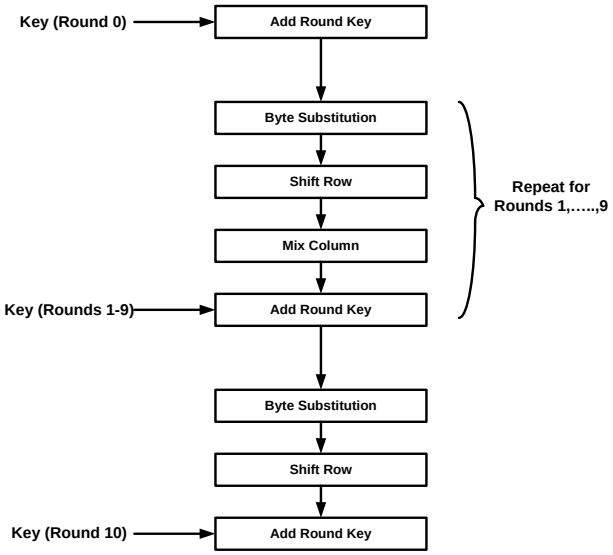

Figure 3 AES Structure

5. GENETIC ALGORITHM

In 1859 Charles Darwin (1809-82) [11] published an extremely controversial book of title is "On the origin of species by means of natural selection, or the preservation of favored races in the struggle for life", which is popularly known as The origin of species. Around the same time, Gregor Mendel (1822-84) [11] investigated the inheritance of characteristics, or traits, in his experiments with pea plants. By examining hybrids from different strains of plant he obtained some notion of the interactions of characters. In spite of the fact that Mendel's investigations established the frameworks for the investigation of genetics, it was not until 30 years after his demise that Walter Sutton (1877-1916)

[11] found that genes were a part of chromosomes in the nucleus. However, Darwin's theory emphasized the role of continuous variation within species. Conversely, particular contrasts between species are not uncommon in nature, i.e. discontinuous variation.

Hugo de Varis (1848-1935) [11] observed that in a population of developed plants, strikingly different variations would periodically show up. To clarify this discontinuous variation, de Varis built up a theory of mutation. Superficially, the new investigation of genetics appeared to support the mutation theory of advancement against conventional Darwinism.

The Genetic algorithms are random search and optimization methods based upon the analogy of natural biological origin. Genetic Algorithms are the part of the evolutionary algorithms which also includes evolutionary programming, evolution strategies and genetic programming. Evolutionary algorithms operates with a population of potential solutions to a problem. It uses principle of survival of best fit solution. Mutation and reproduction to produce solution. At every iteration of an Evolutionary Algorithm, a new generation of alternative solutions are created by the processes of selection and reproduction

a) Elements of Genetic Algorithm

The Goldberg evaluates simple genetic algorithm (SGA). It has three basic elements selection, crossover and mutation and is to illustrate in flow chart shown in figure 4.

1) Population Generation

The procedure of Genetic Algorithms, for the most part, begins with a populace which is arbitrarily created and is made out of a few chromosomes.

2) Selection

Selection is the process of finding the particular individual or number of offspring, alternative solutions for reproduction.

3) Crossover

After the generation of population, the important parameter of genetic algorithm is to connect generated population. Likewise there are distinctive sorts of crossover, for example, one point crossover or two point crossover or uniform crossover. Crossover operator is used to generate best fit generation than previous one.

4) Mutation

The mutation is arbitrary process where one factor of a gene is replaced by different to generate a new genetic structure.

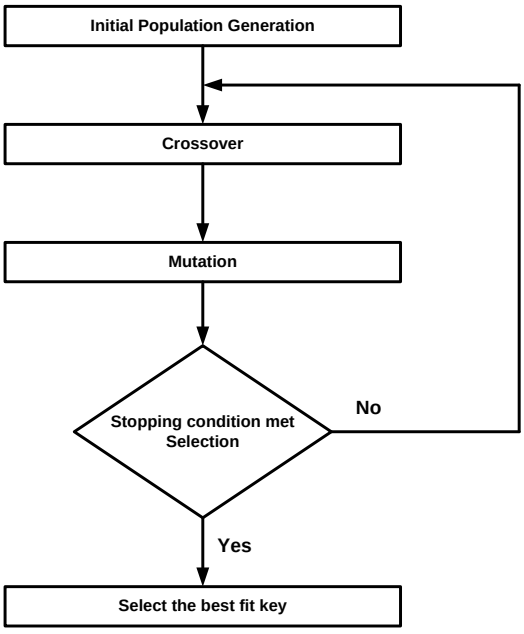

Figure 4 Elements in GA

6. RESULTS

The novel algorithm has been simulated and the results are shown in figure. The results are showing of key generation using genetic algorithm. The results satisfy the encryption and decryption methodology.

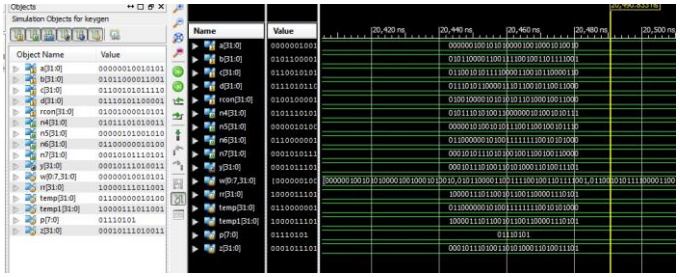

Figure 5 Key Generation using GA

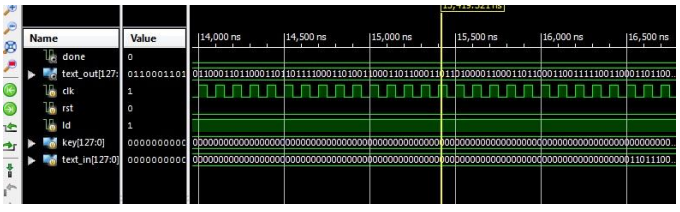

Figure 6 Encryption

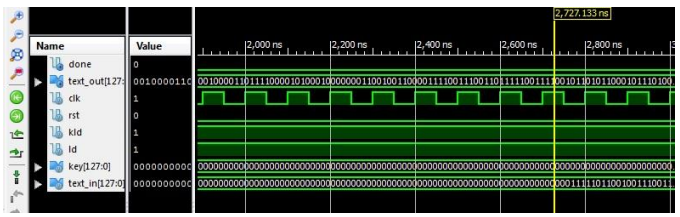

Figure 7 Decryption

7. CONCLUSIONS

In this paper we present the Novel Advanced Encryption Standard implementation approach using Genetic Algorithm. The key generation will be takes place by major elements of Genetic Algorithms like crossover, mutation and selection. The generated key is used for the making the byte substitution key dependent and these newly generated S-Boxes are used in the different rounds in Advance Encryption Standard (AES) process.

REFERENCES

[1] Joan Daemen and Vincent Rijimen. The Design of Rijindael. Springer,2002, pp-31-50.

[2] X. Zhang and K. K. Parhi, "Implementation approaches for the advanced encryption standard algorithm", IEEE Circuits Syst. Mag., vol. 2, no. 4, pp.24 -46 2002.

[3] Alireza Hodjat, Ingrid Verbauwhede. "Area-Throughput Trade-Offs for Fully Pipelined 30 to 70 Gbits/s AES Processors". IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 4, 366-372, APRIL 2006.

[4] K. Gaj and P. Chodowiec, "Comparison of the hardware performance of the AES candidates using reconfigurable hardware", Proc. 3rd AES Conf. (AES3), 2000 [online] Available: item>http://csrc.nist.gov/encryption/aes/round2/conf3/aes3papers.html</item>

[5] Bethany Delman, Genetic Algorithms in Cryptography, MS Thesis 2004.

[6] Karel P.Bergmann,Renate Scheidler, Christian Jacob. "Cryptanalysis using Genetic Algorithms", GECCO 2008.

[7] Sliman Arrag, Abdellatif Hamdoun, Abderrahim Tragha. "Replace AES Key Expansion Algorithm By Modified Genetic Algorithm". Applied Mathematical Sciences, Vol. 7, No. 144, 7161-7171, 2013.

[8] Sindhuja K , Pramela Devi S. "A Symmetric Key Encryption Technique Using Genetic Algorithm". (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1), 414-416, 2014.

[9] Sania Jawaid, Adeeba Jamal. "Generating the Best Fit Key in Cryptography using Genetic Algorithm". International Journal of Computer Applications, Volume 98 – No.20 33-39, July 2014

[10] Anil Kumar and M. K. Ghose, Overview of Information Security Using Genetic Algorithm and Chaos, Information Security Journal: A Global Perspective, 18:306–315, 2009.

[11] A.M.S.Zalzala and P.J.Fleming. Genetic Algorithms in Engineering Systems. IEEE Control Engineering Series 55,1997, pp-1-41.

[12] Serge Vaudenay. A Classical Introduction to Cryptography-Applications for Communications Security. Springer, 2006, pp-1-60.

[13] Ashwak alabaichi and Adnan Ibrahem Salih. "Enhance Security of Advance Encryption Standard Algorithm Based on Key Dependent S-Box", Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference. Sierre, 2015, pp-44-53.

BIOGRAPHIES

Amit Nevase received B.E. (2010) in Electronics Engineering from Walchand College of Engineering, Sangli, Maharashtra, India. He is currently a Post graduate student of Electronics and Telecommunication Engineering in G. H. Raisoni Institute of Engineering and Technology, Pune, Maharashtra, India.

Nagnath Hulle is currently Vice Principal of G. H. Raisoni Institute of Engineering and Technology, Pune, Maharashtra, India. He bagged second prize in Institution of Engineers (IE) Annual Technical Meet 2012. Also bagged First prize in Institution of Engineers (IE) Annual Technical Meet 2013. His research interests include Cryptography, Advanced Encryption Standard.