Enhanced AES Cryptosystem by using Genetic Algorithm and Neural Network in S-box

K.KALAISELVI*
DEPT OF COMPUTER SCIENCE
KRISTU JAYANTI COLLEGE
BANGALORE.

Dr .ANAND KUMAR**
DEAN ACADEMICS,
HEAD,DEPT OF MCA,
M.S ENGINEERING COLLEGE,BANGALORE

Abstract

Cryptography based on block ciphers use Key-dependent ciphers for encryption and decryption. The efficiency of these systems depends on the security and the speed of the algorithm. The encryption process needs to be adaptive and dynamic in order to face any cryptanalytic attacks. Increasing the complexity of the algorithm is one way to prevent the attacks. The introduced complexity increases the execution time of the algorithm which leads to timing attacks. This paper attempts to propose two enhanced AES cryptosystem by employing Genetic algorithm (GA) in SP-boxes and modification of AES by implementing nonlinear neural network (NN) in SP network to increase the security against timing attack and reduce the computational time of the proposed system. Both GA and NN are used in key expansion and key distribution of the AES algorithm.

Keywords: AES, Genetic algorithm, SP-boxes,Neural Network, timing attack

I. INTRODUCTION

Data communication through a network is secured using an efficient technique, Cryptography. Encryption and Decryption are the basic operations performed by efficient algorithms. These algorithms may be symmetric or Asymmetric in nature. Symmetric cryptosystems uses identical key (secret key) for both encryption and decryption. These algorithms are classified either as Stream ciphers or as Block ciphers. Advanced Encryption Standard (AES) is an efficient block cipher which comprises of AES-128, AES-192 and AES-256 block ciphers. Each cipher uses 128 bits, 192 bits and 256 bits keys for encryption and decryption. The key size used in the cipher specifies the number of rounds repeated to convert the plain text into cipher text. AES-128 has 10 cycles of repetition rounds, AES-192 has 12 cycles of repetition rounds, AES-256 has 14 cycles of repetition rounds for encryption. Each round has four stages of processing steps which includes Substitution, Transposition, input plaintext mixing and transforming it into ciphertext [1].

To transform the ciphertext into plain text, reverse rounds are applied using the same secret key. AES relies upon techniques of confusion and diffusion. Confusion is accomplished through substitution and the diffusion is accomplished through permutation. Permutations and substitutions (S-boxes) are based upon the key and the original text [5]. The overall working structure of AES is shown in Fig 1.

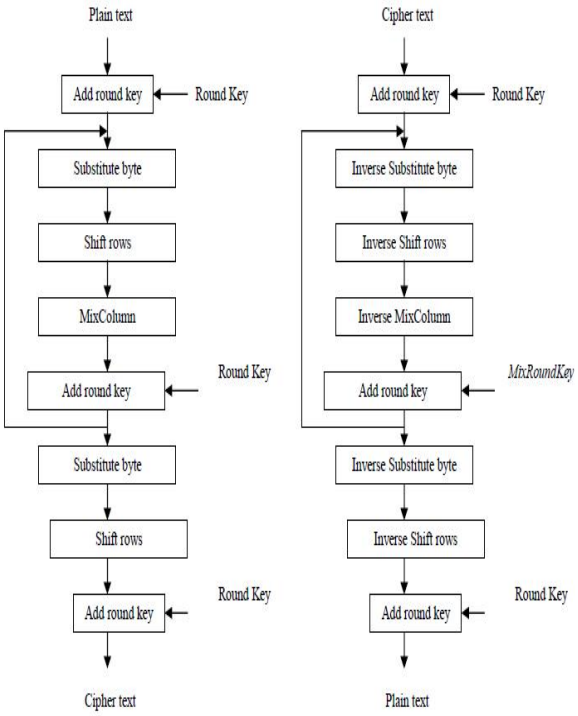

Fig 1: Working structure of AES

* Research scholar Bharathiar University
** Research supervisor Bharathiar University

978-1-5090-1936-6/16/$31.00 ©2016 IEEE

The conventional AES [2] and number of rounds r performed are designed as follows:

Description of ‘r' rounds in AES:

1. For a given input plaintext X, the initial state is taken to be X. XOR the round key with the state to perform AddRoundKey operation.

2. For each of the first r-1 rounds,

2.1 perform SubBytes substitution operation on the state using substitution box (S-box)

2.2 Shift the rows to perform permutation operation, ShiftRows on state

2.3 Mix the columns on state to perform MixColumns operation

2.4 Perform AddRoundKey

3. Perform SubBytes,ShiftRows and AddRoundKey.

4. Define the ciphertext Y to be state.

The operations in AES are byte oriented operations, the variables used are formed with an exact number of bytes. The plaintext X consists of 16 bytes. Each state is represented as 4 *4 arrays of bytes.

A. Areas of AES:

AES is mainly used to provide safe transmission of the data from the sender to the authenticated receiver. The area of application includes

1. Application Archive and compression tools like RAR and WINZIP
2. File encryption and Disk or Partition encryption
3. Security for communications in LAN - IEEE 802.11i-2004, or 802.11i Wireless networks
4. Provides confidentiality and authentication for IPsec protocol
5. SPN Substitution -Permutation Networks uses the stages and rounds in AES.

B. Security of AES

AES is designed to have resistance against all known attacks. It has the speed and platform independent code capability. Different variants of AES has specific implementations that provides security against specific attacks. A side-channel attack is any type of attack based on information gained from the implementation of a cryptographic algorithm. These channels can be exploited and attacked , if the information collected can be correlated to the secret key.

Potential information leaks in the channel includes power analysis attacks , differential power analysis and correlation power analysis attacks due to the power consumption. A vulnerable attack, Timing attack in which the attacker compromise a cryptosystem by analyzing the time taken to execute the algorithm. Execution time of an algorithm is based on the input and the logical operations . A cryptosystem can be attacked by tracing back to the input. The time taken to respond to the queries can leak the vital information about the system. Many criteria which includes design of the cryptosystem , CPU time, throughput time leaks the information for side-channel attacks in AES. There is some criticism that the mathematical structure of AES leads to computational timing attacks [3].

C. Performance of AES

The performance evaluation of AES is discussed in this section. Six criteria are taken into considerations to evaluate the performance of AES [3].

Software Implementations :

AES performance is low for the larger key size ,since the number of rounds are increased for substitution and permutation. AES's parallel processing, facilitates efficient usage of processor which results in high software performance.

Memory Usage:

AES requires restricted space , low RAM and ROM for implementing both encryption and decryption. But the ROM requirements will be increased if both encryption and decryption are performed simultaneously. To overcome this ,the schedule key is kept separate for encryption and decryption.

Throughput time:

The throughput of AES-192 and AES-256 are affected due to the increase in the number of keys and the additional increase in the rounds. If the S-boxes are pipelined the throughput will be unaffected.

Encryption vs. Decryption:

The decryption process rounds are inverse of the encryption process. But implementation of both the process requires about 60% more space than the encryption process alone. The key setup performance is faster for encryption than decryption.

Key Agility:

AES generates the subkey individually for the encryption. But ,all the subkeys are generated prior to the decryption with a specific schedule key. This increases the resource utility of the algorithm.

Flexibility :

AES structure can accommodate any block and key sizes which are multiples of 32. Accordingly the number of rounds will be increased for the encryption and decryption

II. EVOLUTIONARY APPROACHES TO ENHANCE THE PERFORMANCE OF AES

An enhanced AES implemented using evolutionary approach is expected to improve the performance of the AES which are mentioned above.AES is a symmetrical block cipher which uses Substitution box (S-box) and Permutation box (P-box) for the process of encryption and decryption. Substitution box (Sbox) is a keystone of AES symmetric cryptosystem [7][8]. A P-box is a permutation of all the bits in the incoming data blocks. It takes the outputs of S-boxes of one round, permutes the bits and feeds them into the next stages of transposition. P-box has the property that the output bits of any S-box are distributed as possible. Substitution-permutation network (SPN) brings nonlinearity to cryptosystem and strengthens their cryptographic security [3][4]. A strong Confusion technique is adapted that maintains the relationship between the statistics of the cipher text and the value of the encryption keys as complex as possible. Evolutionary approaches like Genetic Algorithm (GA), Neural Network (NN) and other optimization techniques can also be applied in the SPN for generating and distributing the cipher keys for ciphering and deciphering. Previous researches have shown that these approaches increases the efficiency of the cryptosystem in terms of speed and security [10][11][12].

GAs is well suitable for providing security for data transmission [10] used genetic algorithm for cryptanalysis. GA is used in simple transposition ciphers and in substitution [15]. Various researchers used GA in different level of transposition such as in mono-alphabetic substitution [15]. GAs is used to generate a block of cipher and schedule keys which are used for encryption and decryption in AES [14].Neural networks are combined with AES to enhance the security of the traditional AES cryptosystem [9]. Artificial Neural Network is trained in AES for key generation and key distribution which provides added security for the conventional AES , since the opponent has to know the topology of NN[12].Most popular Feed-Forward NN called Multi-Layer Perceptron (MLP) is applied in AES to achieve the expected speed and increased security[13]. This research proposes the use of GA and NN in the S-box and P-box for cryptography process.

III. AES WITH GENETIC ALGORITHM

A genetic algorithm is a randomized search that has proven to be reliable and powerful optimization technique which follows the principle of natural selection. It can be applied to both texts and images. Genetic algorithm is secure, since it does not utilize the natural numbers directly. The results obtained for generating keys using genetic algorithm should be good in terms of coefficient of autocorrelation. Generally genetic algorithm has three basic operators namely selection, crossover and mutation. In this research proposal, crossover and mutation operators are used for encryption and decryption. GA is applied in key generation in the s-box and key distribution in the p-box. Pseudo random number generators (PRNG) are used to generate a sequence of numbers that simulates random numbers. These random numbers are used to generate the initial population [16].The basic Genetic algorithm operators are discussed as follows:

SELECTION: It is the process of choosing the chromosomes from the initial population generated by PRNG based on fitness value.

CROSSOVER: This operator combines the chromosome of one generation with another to reproduce a new set of values. Single point crossover, Two point crossover and uniform crossover are the three types of crossover operators in GA.

MUTATION: This provides a genetic diversity of a chromosome in one generation. The chromosomes are flipped and a new chromosome is generated for a new generation.

The initial population is generated; the fitness function is applied to the population to select the first generation chromosomes. The crossover, mutation, reproduction are performed and the generated result is added to the next generation. This process continues until the optimized result is achieved. The iteration continues for all the generations [16][17].

The basic working principle [16] of GA technique is illustrated in Fig: 2.

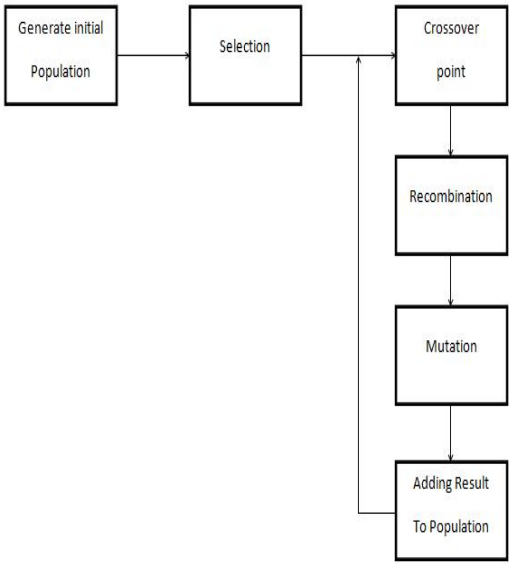

Fig 2: Basic principle of Genetic Algorithm

A. Proposed Algorithm with GA

In this proposed method GA will be used in the S-box to perform substitution, shift the rows, mix the column and to perform AddRoundKey in the AES rounds. The PRNG is used along with the crossover and mutation operators in S-box increase the speed of the algorithm and to provide more security to the data. The modified AES will use the basic operators of GA for all rounds in S-box as follows:

The input data is represented as string of chromosome.
Step 1:The initial population is generated using PRNG
Step 2:Initialize a random population of cipher keys
Step 3:Apply random crossover operation.
Step 4:Generate the set of cipher keys by mutation.
Step 5: Repeat the steps for the entire population.

All the keys generated will be used to encrypt the data, since only the strong keys are chosen for reproduction. The above mentioned steps are applied in all the 10 rounds of AES in the S-box to encrypt the given input data. The inverse operation is performed for decrypting the data.

Fig: 3 shows the application of GA in SP-boxes for ciphering the data.

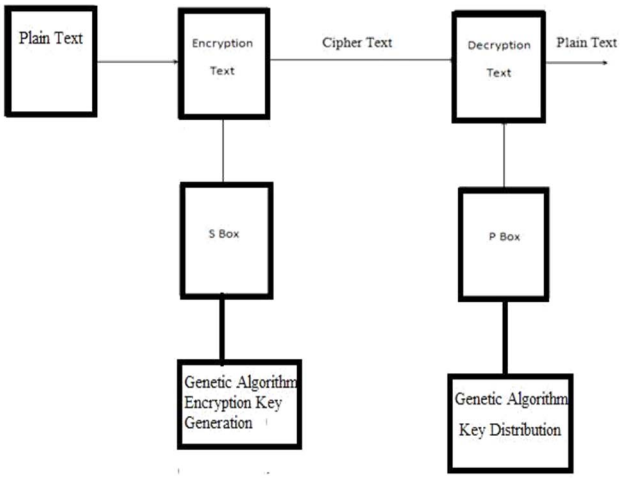

Fig: 3 Block Diagram for AES with GA

B. Expected Outcome

An enhanced approach is proposed in this research paper to increase the complexity of AES by applying GA in S-box. The proposed method is expected to increase the efficiency of the algorithm in terms of Avalanche effect [6] ,small change in the plain text or a key, shows a drastic change in the cipher text, computational time and the strong against timing attack . The algorithm is expected to reduce the computational time, since GA handles the key management efficiently in S-box. Implementing GA in S-box with AES symmetric key algorithm for encryption is expected to increase the overall efficiency of the cryptosystem against the attacks. MATLAB tools will be used for implementation.

The major advantage of GA is that it can solve every optimization problem which can be described with the chromosome encoding. The problems are solved with multiple solutions. Sometimes choosing the encoding and fitness function may be difficult. This may increases the computational time of the algorithm. To overcome this problem, another best resulted evolutionary approach namely, Neural network is implemented in S-box and the result is compared with AES - GA cryptosystem.

IV. AES WITH NEURAL NETWORK

Artificial Neural network (ANN) is a computational intelligence method that exhibits the ability to learn from the new situations generalize, discovers, associates and abstract the data [11]. Neural network is augmented with knowledge elements and designed to mimic the biological nervous system and intelligence. It is comprised of a large number of

processing elements called Neurons which are interconnected and working with each other to solve a specific problem. ANN learns from the environment through the learning process, stores the knowledge and communicates to the neuron in the network through inter-neuron connection strength called neuron weights. Each neuron receives a set of inputs, taken as vector and is associated with a set of weights .NN has basically 3 layers which can be multiple in nature. Input layer, multiple hidden layers and output layers [12]. The basic structure of NN is shown in Fig.4

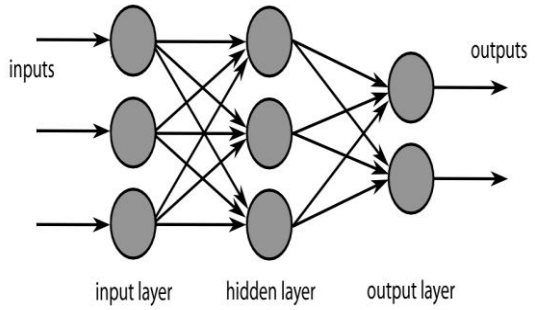

Fig 4: Basic structure of NN

A. Proposed AES Cryptosystem with Neural Network

In the proposed AES algorithm, the neural network performs the substitutions in the S-boxes. This research work takes AES -128 version, so the length of the data block is 128 bits for both encryption and decryption. So, both the input and output will be of 16-bytes.NN must have atleast one hidden layer of 16 neurons to achieve the input key length of 16 bytes. NN is applied in key expansion and key distribution in the S-box of AES. This research proposes a cryptosystem which implements the feed forward method of neural network which performs all partial substitutions in S-box. [12]. Multi-Layer Perceptron (MLP) is applied in S-box for encryption. The training process of NN has 16-16-16-1 topology. It takes a input vector of 16 bytes and generates 16 bytes vector as a trained text.

The encryption steps are expected to follow the basic settings as below:

1. Plain text is taken to be the Input vector or input layer
2. Cipher text is the targeted output from the AES Neural Network.
3. Initial weights of the neuron are taken to be the key generated for encryption process.
4. Each neuron will have a non-linear activation function, which gives the output.

Decryption process is the inverse of the encryption process. The block diagram of Feed forward NN with AES is shown in Fig 5.

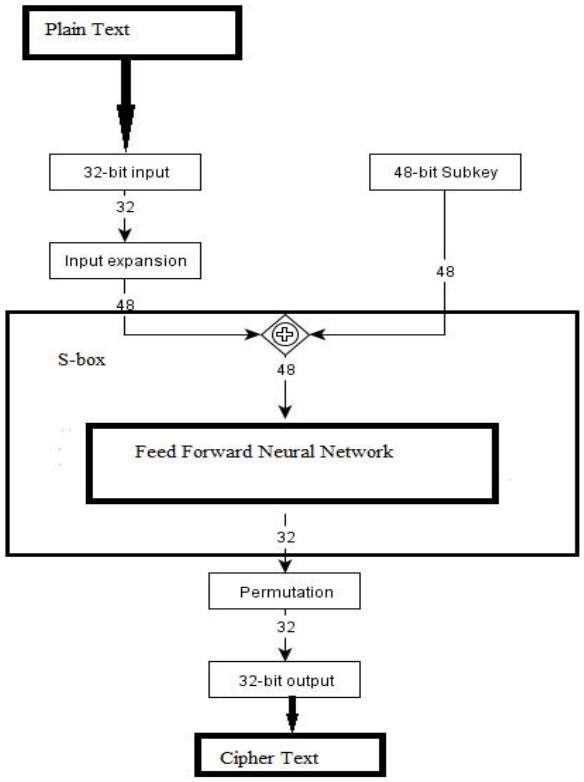

Fig 5: Structure of AES with Feed forward NN

B. Expected Outcome

The functionality of proposed AES algorithm will be verified and realized using Matlab tools. The AES with NN is tested against the same evaluation criteria as Genetic algorithm AES. Performance evaluation with respect to avalanche effect, computational time and cryptanalytic attack is evaluated. Both encryption and decryption are expected to perform using the feed-forward neural network.

V. CONCLUSION

This research paper has proposed two methods to enhance the performance of conventional AES, using Genetic algorithm and Neural network. This will make the existing cryptosystem more complex and stronger against cryptanalytic attacks. But the complexity lies in choosing the fitness function of GA, number of adaptive iterations and the weight of the neuron in NN. A comparative study will be realized for determining the increase in the efficiency of AES, from the point of view of avalanche effect,

computational time and timing attack. Both the proposed algorithms will be implemented and verified using Matlab tools. The comparison made between feed forward NN AES and the genetic algorithm based AES will result in the stronger and efficient symmetric cryptosystem.

Finally, hybrid approach by combining both Genetic algorithm and Neural network in designing the Substitution-permutation network will be taken as the continuation of this research proposal after the implementation of AES with GA and AES with NN.

REFERENCE

[1].W.Stallings“Cryptography and Network Security: Principles and Practice”, Prentice Hall, 3rd Edition, 2007.

[2].Kazys KAZLAUSKAS,Jaunius KAZLAUSKAS "Key-Dependent S-Box Generation in AES Block Cipher System" INFORMATICA, 2009, Vol. 20, No. 1, 23–34.

[3].Jingmei Liu, Baodian Wei, Xiangguo Cheng, Xinmei Wang "An AES S-box to Increase Complexity and Cryptographic Analysis" Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA’05) 1550-445X/05 $20.00 © 2005 IEEE.

[4].Runtong Zhang, Like Chen"A Block Cipher Using Key-Dependent S-box and P-boxes" 978-1-4244-1666-0/08/$25.00 '2008 IEEE.

[5]. Rashmi Ramesh Rachh, B.S.Anami, P.V.Ananda Mohan, "Efficient Implementations of S-Box and Inverse SBox for AES algorithm", 978-1-4244-4547-9/09/$26.00 ©2009 IEEE.

[6].Hui Shi Yuanqing Deng Yu Guan Analysis of the Avalanche Effect of the AES S Box" 978-1-4577-0536-6/11/$26.00 ©2011 IEEE.

[7]. Raja Jitendra Nayaka, R. C. Biradar, "Key Based S-Box Selection and Key Expansion Algorithm for Substitution-Permutation Network cryptography" 978-1-4673-5149-2/13/$31.00©2013 IEEE.

[8].Julia Juremi Ramlan Mahmod Salasiah Sulaiman Jazrin Ramli," Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 183-188 2012 (ISSN: 2305-0012).

[9]. Roman Zálusky, Daniela Ďuračková, Vladimír Sedlák, Tomáš Kováčik "The Use Of Neural Network For Data Encryption Standard(Des)" http://kf.elf.stuba.sk/~apcom/apcom13/proceedings/pdf/266_Zalusky.pdf.

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

[11]. Seema Rani , Dr Harish Mittal, "A Compound Algorithm Using Neural and AES for Encryption and Compare it with RSA and existing AES" Journal of Network Communications and Emerging Technologies (JNCET), Volume 3, Issue 1, July (2015) .

[12].Yasin Kh. Yasin, Prof.SiddeeqY.Ameen, Dr.Hassan Awheed Chiad,"Advanced Encryption Standard (AES) Enhancement Using Artificial Neural Networks" International Journal of Scientific & Engineering Research, Volume 5, Issue 10, October-2014 ISSN 2229-5518.

[13].Siddeeq. Y. Ameen and Ali H. Mahdi "AES Cryptosystem Development Using Neural Networks" International Journal of Computer and Electrical Engineering, Vol. 3, No. 2, April, 2011 1793-8163.

[14].A. Tragha,F. Omary,A. Mouloudi 2006.”ICIGA: improved cryptography inspired by genetic algorithms”at IEEE.

[15].S. Goyat 2012, “Genetic Key Generation For Public Key Encryption Cryptography”, (IJSCE) ISSN: 2231-2307, Volume-2nd, issue-3rd, July 2012 231

[16].Abdullah Abdali Rashed"Using Modified Genetic Algorithm to Replace AES Key Expansion Algorithms" Conference on Information Technology (ICIT'2007) 2007.

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