GENERATION OF NUMEROUS S-BOX FOR ADVANCED ENCRYPTION STANDARD

S.ARUNA, Dr.G.USHA

Abstract*: Substitution box is the non-linear part in Symmetric Encryption Algorithm. It gives the various alternate methods for the construction of S-Box by taking AES Substitution Box as base or modified version of AES S-Box. Hence it is proving that either AES S-box or modified version such as Gray S-Box, S8 S-Box is also satisfying the important parameters of S-Box such as nonlinearity, SAC, Bit Independence Criterion, Diffusion Strength, Differential Approximation probability while we are encrypting both the text and image.

Index Terms*: Strict Avalanche Criterion, Bit Independence Criterion, Diffusion Approximation Probability

I. INTRODUCTION

The greatest widespread and active encryption algorithm falls under symmetric key which is applied in different applications of cryptography that is Advanced Encryption Standard(AES). This Symmetric encryption Algorithm has been legally acknowledged by the NIST[1]. The two novel originators Deamen and Rijmen of AES algorithm (named as Rijndael) submitted the proposal with further analysis of other algorithms, after the analysis with another algorithm which leads to the accepted one. This algorithm is accompanied with a nonlinear module capable of producing misunderstanding ability in encryption procedure. To get more knowledge about the nonlinear component of encryption algorithm that is substitution box (S-Box) in which the cryptanalyst will show great interest in understanding the functionality of the nonlinear component in encryption process. The information of basic assets of nonlinear component(S-box), which plays a vital role in the inspection of their performance, which has given some of the valuable metaphors[2]. A rigid algebraic examination of the Substitution box was initiated in Murphy [3] and it disclosed its own strategy assets and structure. The usage of polynomials are defined in the structure of AES Substitution boxes which includes nine terms. The shattered features that surround the Substitution box condense the encrypted text which is susceptible to attack such as interpolation and algebraic. In current years, scholars have been concentrating on the proposal and expansion of approaches in Substitution boxes by increasing the degree of polynomials.

II. RELATED WORKS

Revised Manuscript Received on July 05, 2019.

S.Aruna, Research scholar, Assistant Professor(Sr.G), School of Computing, , SRM Institute of Science and Technology, Chennai 603203,India (arunas@srmist.edu.in)

Dr.G.Usha , Associate Professor School of Computing, , SRM Institute of Science and Technology, Chennai 603203,India (arunas@srmist.edu.in)

a. Efficient and secure chaotic s-box for WSN

Constructing s-box using (i)cascading piecewise linear chaotic map(ii)discretized Lorenz map and logic-tent map it will produce s-box suitable for WS node, proving more secure than AES s-box in some of the security parameter and the it has Lorenz map has less power consumption than some of s-boxes. It is implemented with a simulator which supports WSN test bed which is suitable for T1MSP430f1611.WSNs will have limited memory and limited energy to measure the energy consumption they used WSim and WSnet. All 106 IC's are producing different results after n iterations (produce s-box) it is measured by ranking method using non recursive and fast sorting algorithm: comb sort. In Lorenz map lowest iteration is 124 and highest is 233 and most probable minimum iteration is 151. In logistic - tent - map the most probable minimum iteration is 320 to produce 16 × 16 s-box. Thus, the constructed s-box is having (i)less linear approximation probability of combinations of two chaotic maps for both methods, tent map, Lorenz map are 0.0625,0.0705,0.0881,0.0976 which is close to literature of chaotic map, spatiotemporal map, chaotic map for block cipher, hash function based on chaotic s-box. hence it is secure from linear attacks. (ii)SAC also within threshold limit that is 0.5125,0.4993,0.4972,0.4923,0.5048 using dependency matrix. (iii)Differential Approximation probability is based on disproportion in input and output of xor table. If the value is less than or equal to 12 then it is secure from differential attacks.

b. Generation of S-Box using key dependent and its quality analysis [4]

This paper did the analysis about the generation of s-box using pseudo random key dependent method. Four algorithms were proposed and eight distance metrics were considered to do the quality analysis. All four proposed algorithms with decent cryptographic strength and also with good resistance of both linear and differential crypt analyst. The newly generated s-box using four algorithms can be used in AES algorithm. The experiment shows that it will generate random number using random permutation of 256! using Matlab. The complexity of encryption is more and the process of cryptanalysis is difficult. With negligible time delay the algorithm 1 is generating 1000 s-boxes in 0.0940 sec. All these four algorithms are generating s-boxes with eight times faster than the other methods. In all the four algorithms input is AES S-box and the newly generated substitution box according to algorithms are compared with distance metrics using mat lab functions. They have

compared the distance metrics of correlation and Pearson in which Correlation is eight times more accurate than Pearson metrics. The following eight distance metrics are calculated (i)hamming distance(ii)sperman's(iii)squared sperman's(iv)The t distance(v)Kendall distance(vi)correlation coefficient distance(vii)Pearson's distance(viii)longest common subsequence distance.

c. Generating new Substitution Box to increase the security of AES and analyzing diffusion strength [5]

The strength of any cryptographic algorithm is calculated using strength of diffusion and how the values of cipher text is related to plain text. Xoring two cipher text will give you Hamming weight which in turn gives Hamming distance. Higher Hamming distance will give nigh avalanche values. All cryptographic algorithm should satisfy the diffusion level by calculating Strict Avalanche Criteria which can be categorized into two SAC, First order SAC and High order SAC. Constructing an s-box using affine transformation will give constant value for s-box. Proving confusion and diffusion analysis of AES is more secure than DES s-box. SAC is measured by (i)changing single bit of key and keeping Plain Text as constant, number of bits changed in cipher text is 72 with SAC value as 56 after 10 rounds. (ii) changing single bit of Plain Text and key as constant, in which number of bits changed in cipher text is 66 with SAC value as 51 after 10 rounds.(iii) changing many bits of key and Plain Text as constant in which number of bits changed in cipher text is 66 and SAC value is 51 after 10 rounds (iv) changing many bits of PT and key as constant which changes 66 bits in cipher text and gives 51 as SAC value. In the proposed substitution box after the 10thround number of bits changed in cipher text is 67 and SAC value is 52. It is proving that AES substitution s-box have good confusion and diffusion.

d. Majority logic Criterion – Statistical Analysis of Substitution Box of Image [6]

The Substitution box strength is calculated on the basis of statistical and algebraic properties of advanced encryption standard (AES), affine-power-affine (APA), gray, Lui J, residue prime, S8 AES, SKIPJACK, and Xyi S-Boxes in the parameters of image such as entropy, contrast, homogeneity, energy and MAD analysis [6]. Entropy analysis helps in the analysis of the randomness of texture of image .7.9447 is the entropy value of S8 AES substitution box. In Contrast analysis, the viewer analyzes the object of texture in encrypted image in which Affine Power Affine S-box gives higher contrast value and S8 Substitution box is also gives good contrast value. Homogeneity will do the analysis about the closeness in elements of distribution in occurrence matrix of Grey Level. It gives brightness of color and grey image in which S8 gives higher Homogeneity value. In energy analysis, value is calculated by analyzing the co occurrence matrix by counting and squared the gray level. In energy analysis Xyi S-box gives 0.0188 followed by S8 Substitution Box as 0.019 .MAD calculates the difference of pixels of original image and pixels encrypted image in which APA Substitution box is giving 62.066 and S8 s-box gives 58.389. The outcome of these examines are more inspected then a majority logic criterion is cast-off to measure the correctness of an Substitution box to image in which both AES and S8 are satisfying all necessary parameters for Substitution box. AES, APA, S8,gray is having high non-linearity: 112.The proposed paper helps the user to determine the suitable algorithms which satisfies both cipher image and s-box performance indices parameter.

e. Construction of new AES S-box using Evolutionary algorithms [7]

Construction of an AES s-box by composite field arithmetic and will be optimized by any one of the genetic algorithms. AES sbox is constructed using multiplicative inverse of GF (2^8). By using composite fields arithmetic Galois Field of 28 is decomposed into Galois Field of (2^2) ^2 and Galois Field of 24 reduces the area from 59.23% to 57.69%. Evolutionary algorithm is compared with CMOS technology which reduces in area and power of s-box by 11.27%,6.65% to reduce the complexity of hardware. Galois field of ((2) ^4) ^2 for the multiplicative inverse based on Cartesian of genetic programming, optimization is done by Genetic Algorithm by the selection of 200 people among 500 people, probability of mutation is 0.03 and the probability of crossover is 0.8. Using two logic gates as input, optimized results of Multiplicative inverse of Galois field is 2^4 , one hundred circuits are created successfully. Among these minimum, maximum and average evolution time in seconds are 20.724,476.466,186.297 and the minimum, maximum, average generations are 186,4407, 1709.9. Using three logic gates as input Multiplicative inverse of Galois field 2^4, one hundred circuits are created successfully. Among these minimum, maximum and average evolution time in seconds are 65.488,703.011,232.988 and minimum, maximum, average evolution generations are 615, 6602, 2188.6. By comparing multiplication over Galois field of 24 using Galois Field of (2^2)^2 with(i) AES s-box generation with algebraic normal form in inversion of sub field uses 21 xor gates,9 AND gates and 306 transistors,(ii)construction of high throughput AES s-box using composite arithmetic field uses 20 xor gates,9 AND gates and 294 transistors ,(iii)AES compact s-box uses 18 xor gates,12 AND gates and 288 transistors (iv) our proposed optimized algorithm uses 18 xor gates,12 NAND gates and 264 transistors. by comparing multiplicative inverse over Galois Field of 2^4 using Galois Field of (2^2)^2 (i) AES s-box generation with algebraic normal form in inversion of sub field uses 13 xor gates,8 AND gates and 204 transistors,(ii)construction of high throughput AES s-box using composite arithmetic field uses 13 XOR gates,9 AND gates and 210 transistors ,(iii)AES compact s-box uses 14 xor gates,12 AND gates and 240 transistors (iv) our proposed optimized algorithm uses 4 xor gates,4 AND,1 NOT,4 NAND,2 OR gates and 102 transistors. To increase the security in the circuit, by generating unique AES key for each device using Physically Unclonable function.

f. Construction of Improved DPA resistivity S-Box with good Bijective [8]

Transparency is considered as a parameter for the robustness of s-boxes for DPA. If the value of transparency order is low then the resistance is high. Generated 8 × 8 random s-boxes with high nonlinearity and good GAC. It is proved that s-box with lower transparency order required more number of power traces than s-box with higher transparency order to perform

attacks using DPA. 220 random s-boxed generated according to the algorithm searching for optimal s-box which is having good cryptographic properties from the pool of s-box using mono objective optimization algorithm took 5 hrs. 37 min on 2.3GHz Intel Core i5-2410M processor with 4GB RAM. Number of power traces required to perform correlation analysis DPA on s-boxes. No. of power traces for AES s-box is 700 whereas no. of power traces for proposed s-boxes are in the range 1500- 2000.In the proposed Substitution Box, DPA of correlation analysis is more when compared with AES algorithm.

g. Evaluation of Power Analysis Attacks on Asynchronous S-Box [9]

Construction of Asynchronous substitution box is referred as self-time logic, null convention logic s-box for AES algorithm which is highly resistant from SCA in FPGA board which is used to design both synchronous and asynchronous s-box. NCL provides properties such as dual -rail encoding, mono code transitions, clock free which will prove that, for the attacker it is more difficult to find the secret keys which is embed in cryptographic circuit on FPGA board. It is proved that power consumption on S-box using NCL circuit is less than the existing s-box. Countermeasures for SCA - DPA attack on synchronous circuit and asynchronous circuit is referred. There are four methodologies to measure the power they are (i) using CAD tools (ii)using regular FPGA board (iii) SASEBO-GII FPGA board (iv) using application specific integrated chip. It is proven that the third method is more efficient than the other methods. Hardware implementation of proposed NCL s-box is highly resistant from DPA and CPA attacks. It is proved that the informed leakage from the proposed s-box is less and it reduces the power the consumption by 22%-26%. In future we can try this DPA and CPA resistant in other methodologies.

h. Construction of Gray Substitution Box for Advanced Encryption Standard [9]

Gray AES S-box is constructed by taking initial AES S-box in adding with binary gray code transformation as preprocessing. It inherits all the properties of AES algorithm. To rise the complexity of algebraic gray augmentation is introduced. The nonlinearity of Gray substitution box is 112. The Gray AES S-Box helps the AES Substitution Box with more resistance from Linear cryptanalysis. Differential Uniformity of Gray S-Box is as same as the AES S-Box which is 4. The SAC Gray S-Box is also satisfying the constraints. Conclusion:

III. CONCLUSION

In this survey we completed the analysis about different methods to construct the substitution box for AES. And with various parameters of AES algorithm, which is more resistant from Linear Cryptanalysis, Differential Cryptanalysis, Interpolation attack and algebraic attack. In generating secure Substitution box for WSN by using tent map, Lorenz map, chaotic map in which chaotic map is more efficient. Diffusion strength of modified AES S-Box is having good SAC. Image Encryption done with different kinds of Substitution box considering Majority Logic Criterion. We can carry on with more researches on image encryption, audio encryption with improved Strict Avalanche Criterion, Bit Independence Criterion.

REFERENCES

1. National Institute of Standards and Technology, Advanced Encryption Standard FIPS197 [S] November 26, 2001.

2. N. Ferguson, R. Schroeppel, D. Whiting, A simple algebraic representation of Rijndael, in: Selected Areas in Cryptography SAC01, NCS2259, 2001, pp. 103–111.

3. S. Murphy, M.J. Robshaw, Essential algebraic structure within the AES, in: Crypto'02, in: LNCS, vol. 2442, 2002, pp. 1–16.

4. K.Kazlauskas,R. Smaliukas, G. Vaicekauskas, A Novel Method to Design S-Boxes Based on Key - Dependent Permutation Schemes and its Quality Analysis, IJACSA, vol 7, No.4 ,2016 pp 93- 99.

5. H.S. Mohan,A. Raji Reddy, Generating the New S-Box and analyzing the Diffusion strength to improve the Security of AES algorithm, IJCNS Vol 2, No.9,2010 pp 51- 56

6 T. Shah, I. Hussain, M. AsifGondal, H. Mahmood, Statistical Analysis of S-box in image encryption applications based on majority logic criterion, IJPS, Vol6, No.16,2011, pp 4110-4127.

7. L.Yaping, W. Ning, Z. Xiaoqiang, Z. Fang, Geffen, A Compact implementation of AES S-Box using Evolutionary Algorithm, CJE, Vol 26, No.4 ,2017, pp -688-695.

8. B. Mazumdar, D. Mukhopadhyay, I. Sengupta, Constrained Search for a class of Good Bijective S-Boxes with Improved DPA Resistivity, IEEE transactions on information Forensics and security, vol 8, No.12,2013, pp-2154-2163

9. M.T. Tran, D.K. Bui, A.D. Duong, Gray S-Box for Advanced Encryption, ICCIS, IEEE computer society,2008 pp 253-258