International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 1 Issue 5 ǁ Sep. 2013 ǁ PP.24-27

Generation of Dynamic S-Box Using Irreduceable Polynomial and the Secret Key Used

Pon.Partheeban[1], Prof. N. Nityanandam[2]
[1]ME Final Year Department of Computer Science and Engineering, KCG College of Technology, Chennai
[2]Professor Department of Computer Science and Engineering, KCG College of Technology, Chennai

Abstract- Advanced Encryption Standard (AES) is one of the best cryptographic algorithms that can be used to protect electronic data. Its security has attracted cryptographist's attentions. The result of new attack methods shows that there may be some lacuna in the design of S-box and key schedule with AES algorithm. The principal weakness in the AES algorithm is the problem of linearity in the S-box. In order to keep away from the new attacks and implement the AES for secure communication, a detailed analysis on the design of S-box is carried out and a new implementation scheme for increasing the complexity of S-box is designed by applying nonlinear transformations. For each composite field constructions, there exist eight possible isomorphic mappings. After the exploitation of a new common sub-expression elimination algorithm, the isomorphic mapping that results in the minimal implementation cost is chosen.
S-box is the only component to implement nonlinear transformation in AES. The cryptographic strength of the AES depends strongly on the choice of S-box. The S-box used in the traditional AES has the properties of short periods and bad distribution. In order to make up the weakness of the existing S-box we generate a dynamic S-box that is dependent on the key. Discrete logarithmic approach is used to improve non-linearity of the S-box. Also, Walsh Hadamard transform matrix is used to decide on the strength of the key and to find the most non-linear key.
Key words- Advanced Encryption Standard (AES), S-box, Dynamic S-box, SubBytes, ShiftRows, MixColumns, AddRoundKey, Walsh-Hadamard Transform.

I. Introduction

1.1 Cryptography

Cryptography is a method of storing and transmitting data in a form that only the intended destination can read and process. It is a science of protecting information by encoding the source data into an unreadable format. Cryptography is an effective way of protecting sensitive information whether it is stored in media or transmitted.

Although the ultimate goal of cryptography, and the mechanisms that make it up, is to hide information from unauthorized individuals, most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources [1]. So a more realistic goal of cryptography is to make very work-intensive to obtain the information so as to be worth it to the attacker.

1.2 Advanced Encryption Standard

AES is a symmetric encryption algorithm processing data in block of 128 bits. A bit can take the values zero or one, in effect a binary digit with two possible values as opposed to decimal digits, which can take one of 10 values. Under the influence of a key, a 128-bit block is encrypted by transforming it in a unique way into a new block of the same size. AES is symmetric encryption system since the same key is used for encryption and decryption. It is mandatory to keep the key secret so as to maintain strict confidentiality. AES may be configured to use different key-lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 to indicate the length in bits of the key. Each additional bit in the key effectively doubles the strength of the algorithm [1], when defined as the time necessary for an attacker to attempt a brute force attack, i.e. an exhaustive search of all possible key combinations in order to find the right one.

The fundamental operations that make the heart of AES algorithm are,

- KeyExpansion: Round keys are derived from cipher key using Rijndael's key schedule
- SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
- ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
- MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column

- AddRoundKey—each byte of the state is combined with the round key using bitwise XOR

II. IMPLEMENTATION

Our work can be precisely implemented in the AES algorithm such that the entire structure of the AES algorithm does get disturbed by the nonlinearity incorporated to the S-boxes. The primary objective of our work is to improve nonlinearity and dynamism of the S-Box. Our optimization step enhances the security of AES and removes all possible trapdoors in square algorithm.

2.1 Non-Linear S-box:

It is designed by composing three transformations:

1. Power of a primitive element in F_{257}^{*}. If the power of the chosen primitive element is 256, it is treated as 00.
2. Multiplicative inverse in the finite field GF(2^8). Element 00 is mapped to itself.

3. The second multiplicative inverse in the finite field GF(2^8) using the polynomial $x^8 + x^4 + x^3 + x + 1$

2.2 Finding inverse:

The first step in the S-box generating process is to search for the multiplicative inverses of all elements of the finite field GF(2^8). In other words: For all possible 256 byte values b,

- find the byte b^{-1} that satisfies $b * b^{-1} = 1$

where, '*' denotes the polynomial multiplication.
The standard algorithm to perform such an inversion is called extended Euclidean algorithm.

2.3 Key-Dependent Approach:

To make the entire process Key dependent the best letter in the symmetric key ie. the letter with the most nonlinear properties[8] is selected. The ASCII value of this letter is used as the constant in the affine transformation used in S-Box construction.

2.3.1 The Fast Walsh-Hadamard Transform:

A Hadamard matrix H is an n x n matrix with all entries +1 or -1, such that all rows are orthogonal and all columns are orthogonal . So if we map the values in the affine truth table: {0,1} -> {1,-1}, we find the same functions as in the Hadamard development[6]. These are the Walsh functions, and here both developments produce the same order, which is called "natural" or "Hadamard". Walsh functions have fast transforms which reduce the cost of correlation computations from n*n to n log n, which can be a very substantial reduction [7].
A Fast Walsh Transform (FWT) essentially computes the correlations which we have been calling the "unexpected distance" (UD). It does this by calculating the sum and difference of two elements at a time, in a sequence of particular pairings, each time replacing the elements with the calculated values.

III. SYSTEM DESIGN

Sub Bytes Transformation :

1. First, taking the multiplicative inverse in GF (2^8), with the representation defined in Section 2.1. '00' is mapped onto itself.
2. Then, applying an affine (over GF(2)) transformation defined by:

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Fig 3.1 Affine Transformation

- Rising an integer to the power of a prime and performing a modulo operation with prime number provides a good distribution.

The, next objective is to make the S-Box dynamic so that a new S-Box is generated every now and then using the Key dependent approach .The main concept employed is, the most non linear letter from the key is chosen and used as the constant in affine transformation. Correspondingly, the strength of the key is also tested.

- Key dependent approach – The S-box varies every time the user provides a new key for encryption.

3.1 S-Box Design Criteria:

- Invertibility
- Properties of Galois Field ($GF(2^8)$)
- Minimization of the largest non-trivial correlation between linear combinations of input bits and linear combination of output bits
- Complexity of algebraic expression in $GF(2^8)$
- The finite field $GF(2^8)$ is generated by the primitive polynomial $x^8 + x^6 + x^5 + x + 1$
- simplicity of description

3.2 S-Box Field Property:

A field is a set with two operations, addition and multiplication :

- both satisfy closure
- both associative
- both commutative
- each has identity (0 and 1)
- any element a has additive inverse a^{-1}

IV. FUTURE ENHANCEMENT

* Improving the nonlinearity of S-box by using the iterated hill climbing algorithm. This hill climbing method works on the incremental improvement of single output Boolean functions.
* The Mix Columns transformation used in AES can be improved by changing finite field polynomial.
* To improve the efficiency of the process, the inverses of all the corresponding 256 elements in the finite field can pre computed and stored in a lookup table.
* Increasing the nonlinearity of key schedule.

V. CONCLUTION

AES is a new cryptographic algorithm that can be used to protect electronic data. Its security has attracted cryptographist's attentions. The principal weakness is the problem of linearity in the S-box and key schedule. It is necessary to incorporate nonlinear transformations in the design of S-box and key schedule in order to protect from new attacks. Some measures against new attacks were adopted by improving the complexity of nonlinear transformation of S-box in our implementation scheme. Our implementation scheme does not affect the heart of the AES algorithm but makes it more non linear and dynamic ,thus making it unbreakable. The experimental results show the scheme of Java implementation is feasible in the networking environment, and has an acceptable speed of data encryption and decryption.

REFFERENCES

[1] **"**Advanced Encryption Standard", Federal Information Processing Standards Publications (FIPS PUB 197) (November 26 2001).

[2] V.Ch.Venkaiah, K.Srinathan and B.Bruhadeshwar, "Variations to S-box and Mix Column Transformations of AES", International Institute of Information Technology, Gachibowli, 2010.

[3] Xinmiao Zhang and Keshab K. Parhi, "High-Speed VLSI Architectures for the AES Algorith", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 12, NO. 9, SEPTEMBER 2004.

[4] Xinmiao Zhang and Keshab K. Parhi, "On the Optimum Constructions of Composite Field for the AES Algorithm", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS-II: EXPRESS BRIEFS, VOL. 53, NO. 10, OCTOBER 2006.

[5] D. Canright,"A Very Compact S-box for AES", Naval Postgraduate School, Monterey CA 93943, USA.

[6] S. Mathew, F. Sheikh, A. Agarwal, M. Kounavis, S. Hsu, H. Kaul, M. Anders, and R.Krishnamurthy, "53 Gbps native GF (24)2 composite- field AES-encrypt/decrypt accelerator for content-protection in 45 nm high-performance microprocessors," in *Proc. IEEE Symp. VLSI Circuits (VLSIC)*, 2010, pp. 169–170.

[7] V. Rijmen, "Efficient implementation of the Rijndael S-box," 2000. [Online]. Available: http://ftp.comms.scitech.susx.ac.uk/fft/crypto/rijndael- sbox.pdf

[8] A. Rudra, P. K. Dubey, C. S. Jutla, V. Kumar, J. R. Rao, and P. Rohatgi, "Efficient rijndael encryption implementation with composite field arithmetic," in *Proc. CHES*, 2001, pp. 171–184.

[9] J.Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC implementation of the AES S-boxes," in *Proc. RSA Conf.*, 2002, pp. 67–78. [5] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," in *Proc. ASIACRYPT*, Dec. 2000, pp. 239–245.

[10] N. Mentens, L. Batinan, B. Preneeland, and I. Verbauwhede, "A systematic evaluation of compact hardware implementations for the Rijndael S-box," in *Proc. Topics Cryptology (CT-RSA)*, 2005, vol. 3376/ 2005, pp. 323–333.
[11] C. Paar, "Some remarks on efficient inversion in finite fields," in *Proc. IEEE ISIT*, 1995, pp. 5–8.
[12] J. L. Fan and C. Paar, "On efficient inversion in tower fields of characteristic two," in *Proc. IEEE ISIT*, 1997, p. 20.
[13] D. R.Wilkins, "Part III: Introduction to Galois Theory," 2000. [Online]. Available: http://www.ercangurvit.com/abstractalgebr/galois.pdf
[14] M. M. Wong and M. L. D. Wong, "A new common subexpression elimination algorithm with application in composite field AES S-box," in *Proc. 10th Int. Conf. Inf. Sci. Signal Process. Their Appl. (ISSPA)*, 2010, pp. 452–455.
[15] M. Chen, "In Greedy Algorithms," in *A Greedy Algorithm With Look Forward Strategy*. Vienna, Austria: IN-TECH, 1998, pp. 1–16.
[16] W. W. L. Chen, "In Discrete Mathematics," in *Search Algorithms*. Australia: Macquarie Univ., 2008, pp. 1–8 [Online]. Available: http://rutherglen.science.mq.edu.au/wchen/lndmfolder/dm19.pdf