Replacement and Structure of S-boxes in Rijndael

De WANG
Department of Computer Science
Jinan University
Guangzhou, China
Wangde_oo7@163.com

Shi-Liang SUN
Department of Computer Science
Jinan University
Guangzhou, China

***Abstract*—this paper describes the designation and structure of S-boxes which are the fundament of the Rijndael algorithm and finds the optimization of them using four kinds of testing methods. Firstly, it constructs different S-boxes by MATLAB using 30 irreducible polynomials the maximum power of which is eight in a finite field. Through taking their performance analysis, we find that they have the similar performances in differential testing and linear or correlation testing. But in avalanche testing and boolean expressions testing, the S-boxes which are constructed by No. 9 and No. 18 irreducible polynomial are optimal structure respectively.**

Keywords-replacement; s-boxes; rijndael

I. Introduction

Packet Cryptography which is an important branch of Cryptography has a lot of features that fast, easy to standardize and facilitate the realization of hardware and software. The S-box [1, 2] is the only non-linear component in many cipher algorithms. Therefore, S-box determines the strength of the security division cipher strength in some extent.

In this paper, we explain the structure of S-box in Riijndael algorithm firstly and then describe the ways to replace the S-box in details. Secondly, according to 30 irreducible polynomials the max power of which is eight in a finite field, we construct 30 different S-boxes. Finally, through four different testing methods to detect the performance of S-boxes and a comparative analysis of their performance, the No. 9 and No. 18 have the best performance in avalanche and Boolean expressions test, but the differences in differential testing and linear or correlation testing are similar.

II. The structure of S-box in Rijndael algorithm

The S-boxes in Rijndael algorithm are constructed in the round function of the bytes' substitution. It needs two steps as follows [3].

First of all, taking the bytes as the elements of GF(8) , we map them to their multiplication inverse and '00' is the mapping of its own.

Secondly, we take the bytes to do the following (and reversible) affine transformation:

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

The transformation of all the bytes in S-boxes above can be marked as: ByteSub(State). In fact, the S-box also can be expressed as a array of 256 elements.

III. The methods of the replacement on S-boxes in Rijndael algorithm

A. *The number of irreducible polynomials in finite field*

Definition 1: Let $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ a positive integer,

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & \prod_{i=1}^{k} \alpha_n > 1; \\ (-1)^k, & \text{others} \end{cases}$$

Here, $p_1, p_2, \cdots, p_k$: Different primes,

$\alpha_1, \alpha_2, \cdots, \alpha_k$: Positive integer.

It is called Mobius function [4]. For instance, $\mu(2) = -1, \mu(4) = 0, \mu(6) = 1$.

Lemma 1: For any positive integer n, there is

$$\sum_{d|n} \mu(d) = \begin{cases} 0, & n > 1; \\ 1, & n = 1. \end{cases} \text{[4]}$$

Lemma 2: The number of irreducible polynomials which the highest factor of are 1 in GF(q) is $I_q = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$, here q is the positive integer power of prime number.[4]

978-0-7695-3336-0/08 $25.00 © 2008 IEEE
DOI 10.1109/CSSE.2008.296

B. *The construction and replacement of S-boxes*

In ascending order, we rank 30 irreducible polynomials as Table 1[5, 6]:

TABLE I. THE IRREDUCIBLE POLYNOMIALS IN GF(2^8)

Order Number	Irreducible Polynomials
1	$x^8+x^4+x^3+x+1$
2	$x^8+x^4+x^3+x^2+1$
3	$x^8+x^5+x^3+x+1$
4	$x^8+x^5+x^3+x^2+1$
5	$x^8+x^5+x^4+x^3+1$
6	$x^8+x^5+x^4+x^3+x^2+x+1$
7	$x^8+x^6+x^3+x^2+1$
8	$x^8+x^6+x^4+x^3+x^2+x+1$
9	$x^8+x^6+x^5+x+1$
10	$x^8+x^6+x^5+x^2+1$
11	$x^8+x^6+x^5+x^3+1$
12	$x^8+x^6+x^5+x^4+1$
13	$x^8+x^6+x^5+x^4+x^2+x+1$
14	$x^8+x^6+x^5+x^4+x^3+x+1$
15	$x^8+x^7+x^2+x+1$
16	$x^8+x^7+x^3+x+1$
17	$x^8+x^4+x^3+x^2+1$
18	$x^8+x^7+x^4+x^3+x^2+x+1$
19	$x^8+x^7+x^5+x+1$
20	$x^8+x^7+x^5+x^3+1$
21	$x^8+x^7+x^5+x^4+1$
22	$x^8+x^7+x^5+x^4+x^3+x^2+1$
23	$x^8+x^7+x^6+x+1$
24	$x^8+x^7+x^6+x^3+x^2+x+1$
25	$x^8+x^7+x^6+x^4+x^2+x+1$
26	$x^8+x^7+x^6+x^4+x^3+x^2+1$
27	$x^8+x^7+x^6+x^5+x^2+x+1$
28	$x^8+x^7+x^6+x^5+x^4+x+1$
29	$x^8+x^7+x^6+x^5+x^4+x^2+1$
30	$x^8+x^7+x^6+x^5+x^4+x^3+1$

Taking the irreducible polynomials in table 1, we construct 30 S-boxes using MATLAB. And then, we make the performance analysis of the S-boxes [6, 7]

IV. THE COMPARISON OF THE REPLACEMENTS ON S-BOX IN RIJNDAEL ALGORITHM

The 30 S-boxes take the four different tests and we find that their uniformity of differential is 4 and linear degree is 112 respectively. So their performances in differential testing and linear or correlation testing are similar. Their critical differences are the performances in avalanche testing and boolean expressions testing. The study of two tests is as follows.

A. *Avalanche testing*

Through the avalanche testing of the 30 S-box, we find that their distribution of number of bits is about 0.5 and they all can pass the t testing and x^{2} testing the main difference of which is the variance. So we determine the best performance by the value of the variance, following the rule that the smaller the better. The results of the testing are as follows:

TABLE II. THE RESULTS OF VARIANCE FOR EACH S-BOX

Order	Variance	Order	Variance	Order	Variance
1	0.0017973	11	0.0022018	21	0.001768
2	0.0021753	12	0.0019243	22	0.0020615
3	0.0020678	13	0.0022971	23	0.0021854
4	0.0014098	14	0.0020253	24	0.0024737
5	0.0019371	15	0.0018125	25	0.0014888
6	0.0015242	16	0.0021486	26	0.0019535
7	0.0025838	17	0.001847	27	0.0016923
8	0.0024854	18	0.0015496	28	0.0020312
9	0.0013541	19	0.0020774	29	0.0021968
10	0.0020996	20	0.0021135	30	0.0015127

According to table 2, it is only the result of one test. The smallest value of the variance is 0.0013541, which is from the NO.9 irreducible polynomial—x^8+ x^6+ x^5+ x+1. After several rounds of tests, we find that its average value is also the smallest. The test data are randomly generated, so the results can only be observed from the distribution of the stability of the performance of avalanche effect.

B. *Boolean expressions testing*

As The S-boxes in Rijndael algorithm are one to one mapping in GF(2^8)->GF(2^8), their average number of Boolean expression component functions is all 128. We compute their variance and also follow the rule that the smaller the better. The results are as shown in Table Ⅲ:

TABLE III. THE RESULTS OF BOOLEAN EXPRESSIONS TESTING FOR EACH S-BOX

Order	Result	Order	Result	Order	Result
1	104.5714	11	35.7143	21	65.7143
2	14	12	45.7143	22	45.4286
3	75.7143	13	100.8571	23	91.4286
4	54.2857	14	41.7143	24	44.8571
5	43.7143	15	82.2857	25	43.1429
6	68	16	26.8571	26	31.4286
7	82	17	24	27	40.5714
8	111.4286	18	10.2857	28	33.4286
9	80.8571	19	55.7143	29	81.1429
10	35.7143	20	137.1429	30	81.1429

From Table Ⅲ, the smallest value is 10.2857, which is from the NO.18 irreducible polynomial—x^8+x^7+x^4+x^3+x^2+x+1. Its distribution is stable, which indicates that it has the best performance in the resistance of the interpolation cryptanalysis and high-end differential cryptanalysis.

V. CONCLUSIONS

In this paper, according to 30 irreducible polynomials in finite field, we construct 30 different S-boxes in order to find which one has the best performance. Though four kinds of test methods as differential test, linear or correlation tests, avalanche test and boolean expressions test, we achieve the conclusion as follows:

The values of two elements of all S-boxes are the same, which is resulted from that the counterpart values in S-boxes mapping to 0 and 1 are constant. The values are 99 and 124. In this point, a single round of S-box transform has two constant points 0 and 1 which can be avoided by affine transformation and multi-round transform..

The 30 S-boxes take the four different tests and we find that their uniformity of differential is 4 and linear degree is 112 respectively. So their performances in differential testing and linear or correlation testing are similar.

Their critical differences are the performances in avalanche testing and boolean expressions testing. The No. 9 and No. 18 irreducible polynomials have the best performance in avalanche and Boolean expressions test.

REFERENCES

[1] NIST.The Rijndael Block Cipher. http://csrc.nist.gov/encryption/aes/rijndael/

[2] Jorg J. Buchholz. Matlab Implementation of the Advanced Encryption Standard.. http://buchholz.hs-bremen.de.

[3] He De-Quan, Xiao Guo-Zhen, Yang Bo. Modern cryptography. Beijing: Tsinghua University Press, 2003

[4] Yuan Chuan-Gai, Sun Wei. Modern Algebra and Its Application. Beijing: Beijing University of Posts and Telecommunications Publishing House, 2001. pp. 274-305.

[5] mathworld.wolfram.com. Finite field. http://mathworld.wolfram.com/FiniteField.htm.

[6] mathworld.wolfram.com. IrreduciblePolynomial. http://mathworld.wolfram.com/ IrreduciblePolynomial.html.

[7] Introduction to Finite Fields. http://www-math.cudenver.edu/~wcherowi/courses/finflds.html