

# New Method to Determine Algebraic Expression of Rijndael S-box\*

Liu Jingmei<sup>1</sup> Wei Baodian<sup>2</sup> Wang Xinmei<sup>1</sup>

1. Key Laboratory of Computer Networks and Information Security, Xidian Univ., Ministry of Education, Xi'an, 710071
2. Information Science and Technology School of Sun Yat-sen University +86-29-88201015

[jmliu@mail.xidian.edu.cn](mailto:jmliu@mail.xidian.edu.cn) [weibaodian@hotmail.com](mailto:weibaodian@hotmail.com) [xmwang@xidian.edu.cn](mailto:xmwang@xidian.edu.cn)

## ABSTRACT

By the discovered correlation between linear functions over  $GF(q^n)$  and matrices over  $GF(q)$ , a new scheme is presented to resolve the algebraic expression of Rijndael S-box in this paper. This new scheme has the advantage of predetermining in the case of a given random base over  $GF(q^n)$ . The reason why only 9 terms are involved in the algebraic expression of Rijndael S-box is presented, which corrects the available inaccurate illustration. We finally conclude all the available methods to determine the algebraic expression of Rijndael S-box.

## Categories and Subject: C.2.0 General

**Keywords:** AES; Rijndael; Sbox; q-polynomial;

## 1. INTRODUCTION

On October 2nd, 2000, the US National Institute of Standards and Technology (NIST) announced to select Rijndael [1] as the Advanced Encryption Standard (AES), and published it as FIPS 197[2] on 26 November 2001. In the past years more attention has been concentrated on the security of Rijndael. Especially we move our consideration to the algebraic structure of Rijndael S-box, which is the only nonlinear part of Rijndael, but offers the particular advantage of diffusion proposed by Shannon [3] in 1949. So we can claim that the unusual security of the algorithm almost depends on the security of the S-box, and much progress has been made on the research of Rijndael S-box, such as the latest two achievements [4,5] highlighted in [6] On 27 September, 2000.

It is well known that only 9 terms are involved in the algebraic expression of Rijndael S-box, researches [7-9] illustrated this phenomenon and people seem to be still worried about Rijndael security. In this paper we present some important properties of the linear functions over  $GF(q^n)$ , matrices of order n over  $GF(q)$ , and the q-polynomials over  $GF(q^n)$ . We discover and prove the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. InfoSecu04, November 14-16, 2004, Pudong, Shanghai, China. Copyright 2004 ACM ISBN: 1-58113-955-1

equivalence relationship among the q-polynomials, the matrices of order n and the linear functions over finite field. It is discovered that one linear function will correspond to distinct matrices under strict different basis, and the absence of generality of the algorithm in [9] is also demonstrated. As another important contribution of this work, we design a new scheme for the mutual determinations between q-polynomials over  $GF(q^n)$  and matrices of order n over  $GF(q)$  with full generality as its advantage. And its application to resolve the algebraic expression of Rijndael S-box is presented. The essential reason why only 9 terms are involved in the algebraic expression of Rijndael S-box is developed at the end. This paper is organized as follows: In Sect. 2 we describe the equivalence among linear functions, q-polynomials over  $GF(q^n)$  and matrices of order n over  $GF(q)$ ; In Sect.3 we design a new approach of mutual determination between q-polynomial over  $GF(q^n)$  and matrix over  $GF(q)$ . The extension of the scheme [9] is also proposed; In Sect.4 we illustrate the reason why only 9 terms are involved in the algebraic expression of Rijndael S-box, and apply the new method in sect.3 to resolve the algebraic expression of Rijndael S-box. Finally Sect. 5 summarizes the whole paper.

## 2 Equivalence among Linear Functions, q-polynomials and Matrices

**Definition 1.** The linear function  $L(x)$  over  $GF(q^n)$  is defined by

- (1) for  $\forall x_1, x_2 \in GF(q^n)$ , it is satisfied that  $L(x_1 + x_2) = L(x_1) + L(x_2)$ ; and
- (2) for  $\forall x \in GF(q^n)$  and  $\forall k \in GF(q)$ , it is satisfied that  $L(kx) = kL(x)$ ;

**Theorem 1.** The number of linear function over  $GF(q^n)$  is  $q^n$ .

**Proof.** Let  $L(x)$  be one linear function over  $GF(q^n)$  and  $(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$  be one base over  $GF(q^n)$ , then  $\forall x \in GF(q^n)$  can be denoted as  $x = \sum_{i=0}^{n-1} x_i \alpha_i$ ,  $x_i \in GF(q)$  under the base. So  $L(x) = L(\sum_{i=0}^{n-1} x_i \alpha_i) = \sum_{i=0}^{n-1} L(x_i \alpha_i) = \sum_{i=0}^{n-1} x_i L(\alpha_i)$  then as long as  $(L(\alpha_0), L(\alpha_1), \dots, L(\alpha_{n-1})) \in GF(q^n)^n$  is selected,  $L(x)$  will be determined exclusively. The number of  $(L(\alpha_0), L(\alpha_1), \dots, L(\alpha_{n-1})) \in GF(q^n)^n$  is  $q^{n^2}$ , so the number of linear function over  $GF(q^n)$  is  $q^{n^2}$ .

**Definition 2.** The q-polynomial over  $GF(q^n)$  is defined by  $Q(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ ,  $a_i \in GF(q^n)$ , and the affine q-polynomial over  $GF(q^n)$  is defined by  $AQ(x) = \sum_{i=0}^{n-1} a_i x^{q^i} + b$ ,  $a_i, b \in GF(q^n)$ .

Theorem 2 denotes the essence of the q-polynomial over  $GF(q^n)$ .

**Theorem 2.** The function of  $Q(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$  over  $GF(q^n)$  is linear.

It is easy to prove Theorem 2 from the definition 1, and we can derive the following theorem 3 from the combination of the two proceeding definitions:

**Theorem 3.** Any linear function  $L(x)$  over  $GF(q^n)$  has the form of q-polynomial over  $GF(q^n)$ , that is  $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ .

Based on the fact that the inverse matrix over  $GF(q)$  is linear, it is necessary to denote the relationship between the linear functions over  $GF(q^n)$  and the matrices over  $GF(q)$ . Let  $B = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$  be one base over  $GF(q^n)$ , then for example, each element  $x \in GF(q^n)$  can be denoted as  $x = (x_0, x_1, \dots, x_{n-1})_B = (f_0(x), f_1(x), \dots, f_{n-1}(x))_B$  under the base  $B$  and called  $[x]_B$  for short.  $(x_0, x_1, \dots, x_{n-1})_B = (f_0(x), f_1(x), \dots, f_{n-1}(x))_B$  denotes the coordinate functions of  $x$  under the base  $B$ . The polynomial  $L(x)$  can also be denoted as  $(l_0, l_1, \dots, l_{n-1})_B = (g_0(x), g_1(x), \dots, g_{n-1}(x))_B$  by  $B$  and  $[L(x)]_B$  for short. Then we have Theorem 4 to describe the relationship between the linear functions over  $GF(q^n)$  and the matrices over  $GF(q)$ .

**Theorem 4.** If the polynomial  $L(x)$  over  $GF(q^n)$  holds for the equation  $[L(x)]_B = [x]_B A$ , where  $A = (a_{ij})_{n \times n}$  denotes the matrix of order  $n$  over  $GF(q)$ , then  $L(x)$  is one linear function over  $GF(q^n)$ .

We can easily prove the fact from the definition 1. Now we have found that the properties of the linear functions over  $GF(q^n)$ , the q-polynomials and the matrices over  $GF(q)$ , and we can obtain the following theorem to describe their relationship.

**Theorem 5.** The linear function  $L(x)$  over  $GF(q^n)$ , q-polynomial  $Q(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$  and the matrix  $A = (a_{ij})_{n \times n}$  over  $GF(q)$  have the following equivalent relationship:

(1) The form of polynomial expression of linear function  $L(x)$  over  $GF(q^n)$  is  $Q(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ .

(2) Any base  $B$  over  $GF(q^n)$  holds for the equation  $[L(x)]_B = [x]_B A$ , in which  $A$  varies with the base  $B$ .

### 3 New Approach of Mutual Determinations between q-polynomials and Matrices

Theorem 4 denotes the nature of linear function over  $GF(q^n)$  and the Matrix  $A$  over  $GF(q)$ . Here we will resolve the problem how to resolve the other one if one of them is specified. Furthermore if one base over  $GF(q^n)$  and one linear function are given, how can we determine the matrix  $A$  to hold for the relationship in Theorem 4? In addition how can we find the linear function  $L(x)$

corresponding to the given matrix  $A$ ? Some research has been done in paper [9], and the relationship between the linear function and the matrix  $A$  has been studied. A matrix  $M_{n^2 \times n^2}$  over  $GF(q)$

is used to denote the correlation of the linear function and the matrix  $A$ . Method in paper [9] has the merit that the matrix  $M_{n^2 \times n^2}$  makes no difference no matter which linear function and the matrix  $A$  are selected. So we can predict the matrix  $M_{n^2 \times n^2}$  under the condition that the function and the matrix  $A$  are not clear. But on the other hand, it has the disadvantage that the method is only applicable to the polynomial base, so it loses the generality. Here we extend the method to determine the correlation between the linear function over  $GF(q^n)$  and the matrix  $A$  over  $GF(q)$  with full generality as its advantage.

It is well known that the number of basis over  $GF(q^n)$  is  $\prod_{i=0}^{n-1} (q^n - q^i)$ . If we define the base  $(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$  and the base  $(k\alpha_0, k\alpha_1, \dots, k\alpha_{n-1})$  ( $0 \neq k \in GF(q)$ ) as the strict same base, thus the number of the strict distinct base is  $\prod_{i=0}^{n-1} (q^n - q^i) / (q - 1)$ . In this sense we derive the Theorem 6:

**Theorem 6.** Let  $L(x)$  be one linear function over  $GF(q^n)$ , and  $B_1 = (\alpha_0^1, \alpha_1^1, \dots, \alpha_{n-1}^1)$ ,  $B_2 = (\alpha_0^2, \alpha_1^2, \dots, \alpha_{n-1}^2)$  be the two strictly distinct basis over  $GF(q^n)$ , if  $[L(x)]_{B_1} = [x]_{B_1} A_1$  and  $[L(x)]_{B_2} = [x]_{B_2} A_2$ , then  $A_1 \neq A_2$ .

**Proof.** For arbitrary basis  $B_1$  and  $B_2$ , obviously  $B_2 = (\alpha_0^2, \alpha_1^2, \dots, \alpha_{n-1}^2) = (k_0 \alpha_0^1, k_1 \alpha_1^1, \dots, k_{n-1} \alpha_{n-1}^1)$ , in which  $k_i = \alpha_i^2 \cdot (\alpha_i^1)^{-1}$ . If  $A_1 = A_2$ , that is  $a_{ij}^1 = a_{ij}^2 = a_{ij}$ ,  $i, j \in (0, 1, \dots, n-1)$ ,

$$\text{so } L(\alpha_i^2) = \sum_{j=0}^{n-1} a_{ij} \alpha_j^2 = \sum_{j=0}^{n-1} a_{ij} k_j \alpha_j^1$$

$$\text{furthermore } L(\alpha_i^2) = L(k_i \alpha_i^1) = k_i L(\alpha_i^1)$$

$$\text{thus } k_i L(\alpha_i^1) = \sum_{j=0}^{n-1} a_{ij} k_j \alpha_j^1$$

$$\text{therefore } L(\alpha_i^1) = \sum_{j=0}^{n-1} a_{ij} (k_j / k_i) \alpha_j^1$$

$$\text{but } L(\alpha_i^1) = \sum_{j=0}^{n-1} a_{ij} \alpha_j^1$$

$$\text{then } k_0 = k_1 = \dots = k_{n-1}$$

It is a contradiction to the two strictly different bases  $B_1$  and  $B_2$ , so  $A_1 \neq A_2$ .

Theorem 6 indicates that a function will lead to different matrix under the strictly distinct basis, but the algorithm method [9] is only applicable to the case of a polynomial base, and it does not work well for the other more non-polynomial basis. In the following, we present an extension to the method [9], and design a new approach to determine the mutual determinations between the q-polynomial and the matrix over  $GF(q)$ . Both the methods hold for any different basis. We suppose all of the following discussion is processed under the arbitrary base  $B = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$  over  $GF(q^n)$ .

#### 3.1 Extension Scheme

Let  $Q(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$  be the q-polynomial over  $GF(q^n)$ , where

$b_i = \sum_{j=0}^{n-1} b_{ij} \alpha_j$ , let  $A = (a_{ij})_{n \times n}$ ,  $i, j = 0, 1, \dots, n-1$  be the corresponding matrix of  $Q(x)$  under the base  $B$ , that is  $[Q(x)]_B = [x]_B A$ . If  $x$  is substituted by any element of the base, then we obtain:  $Q(\alpha_i) = \sum_{k=0}^{n-1} b_k \alpha_i^{q^k} = \sum_{k=0}^{n-1} (\sum_{j=0}^{n-1} b_{kj} \alpha_j) \alpha_i^{q^k}$ , in which  $\alpha_s \alpha_i^{q^k}$  can be calculated by  $\alpha_s \alpha_i^{q^k} = \sum_{j=0}^{n-1} c_{iksj} \alpha_j$ , thus

$$Q(\alpha_i) = \sum_{k=0}^{n-1} \sum_{s=0}^{n-1} b_{ks} (\sum_{j=0}^{n-1} c_{iksj} \alpha_j) = \sum_{j=0}^{n-1} (\sum_{k=0}^{n-1} \sum_{s=0}^{n-1} b_{ks} c_{iksj}) \alpha_j \quad (1)$$

$$\text{Then } Q(\alpha_i) = \sum_{j=0}^{n-1} a_{ij} \alpha_j, \quad i, j = 0, 1, \dots, n-1 \quad (2)$$

So from the combination of (1) and (2) we can obtain

$$Q(\alpha_i) = \sum_{j=0}^{n-1} a_{ij} \alpha_j, \quad i, j, k, s = 0, 1, \dots, n-1 \quad (3)$$

Therefore the elements  $(a_{00}, \dots, a_{0(n-1)}, \dots, a_{(n-1)0}, \dots, a_{(n-1)(n-1)})^T$  of matrix  $A$  are linearly related to the coefficients  $(b_{00}, \dots, b_{0(n-1)}, \dots, b_{(n-1)0}, \dots, b_{(n-1)(n-1)})^T$  of  $Q(x)$  by the following equation:  $(a_{00}, \dots, a_{0(n-1)}, \dots, a_{(n-1)0}, \dots, a_{(n-1)(n-1)})^T = M_{n^2 \times n^2} \times (b_{00}, \dots, b_{0(n-1)}, \dots, b_{(n-1)0}, \dots, b_{(n-1)(n-1)})^T$  (4)

In equation (4)  $M$  is one matrix of order  $n^2$  over  $GF(q)$  with  $c_{iksj}$  as its elements. On the other hand, the coefficients of  $Q(x)$  can be calculated by the following equation:

$$(b_{00}, \dots, b_{0(n-1)}, \dots, b_{(n-1)0}, \dots, b_{(n-1)(n-1)})^T = (M^{-1})_{n^2 \times n^2} \times (a_{00}, \dots, a_{0(n-1)}, \dots, a_{(n-1)0}, \dots, a_{(n-1)(n-1)})^T.$$

### 3.2 New Approach

We develop here a method how to determine the matrix  $A$  of order  $n$  over  $GF(q)$  holding for the equation  $[Q(x)]_B = [x]_B A$ . We know that the element  $x$ , q-polynomial  $Q(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$  and  $Q(\alpha_i) \in GF(q^n)$  are related to the base  $B$  by the equation:

$$x = \sum_{j=0}^{n-1} f_j(x) \alpha_j, \quad Q(x) = \sum_{j=0}^{n-1} g_j(x) \alpha_j, \quad Q(\alpha_i) = \sum_{j=0}^{n-1} \gamma_{ij} \alpha_j$$

Thus according to the linearity of  $Q(x)$ , we can obtain:

$$\begin{aligned} \sum_{j=0}^{n-1} g_j(x) \alpha_j &= Q(x) = Q(\sum_{i=0}^{n-1} f_i(x) \alpha_i) = \sum_{i=0}^{n-1} Q(f_i(x) \alpha_i) = \sum_{i=0}^{n-1} f_i(x) Q(\alpha_i) \\ &= \sum_{i=0}^{n-1} f_i(x) \sum_{j=0}^{n-1} \gamma_{ij} \alpha_j = \sum_{j=0}^{n-1} (\sum_{i=0}^{n-1} \gamma_{ij} f_i(x)) \alpha_j. \end{aligned}$$

Then we derive  $g_j(x) = \sum_{i=0}^{n-1} \gamma_{ij} f_i(x)$ , and  $A = (\gamma_{ij})_{n \times n}$ . So the elements of  $i_{th}$  row are the coordinates of  $Q(\alpha_i)$  under the base  $B$ .

In the following we will study how to determine the q-polynomial  $Q(x) = \sum_{i=0}^{n-1} b_i x^{q^i}$  over  $GF(q^n)$  according to the matrix  $A$  of order  $n$  over  $GF(q)$  which holds for  $[Q(x)]_B = [x]_B A$ . Obviously it is not difficult to calculate  $Q(\alpha_i) = \sum_{j=0}^{n-1} \gamma_{ij} \alpha_j$  under the base  $B = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ , in which  $\gamma_{ij}$  denotes the  $i_{th}$  row elements of matrix  $A$ . When we consider the q-polynomial function, we obtain

$$\begin{cases} \alpha_0^{q^0} b_0 + \dots + \alpha_0^{q^{n-1}} b_{n-1} = \beta_0 = Q(\alpha_0) \\ \alpha_1^{q^0} b_0 + \dots + \alpha_1^{q^{n-1}} b_{n-1} = \beta_1 = Q(\alpha_1) \\ \dots \\ \alpha_{n-1}^{q^0} b_0 + \dots + \alpha_{n-1}^{q^{n-1}} b_{n-1} = \beta_{n-1} = Q(\alpha_{n-1}) \end{cases} \quad (5)$$

Elements of  $(b_0, b_1, \dots, b_{n-1})$  are the  $n$  variables to be resolved,

and the matrix of coefficients of (5) is

$$\begin{bmatrix} \alpha_0^{q^0} & \alpha_0^{q^1} & \dots & \alpha_0^{q^{n-1}} \\ \alpha_1^{q^0} & \alpha_1^{q^1} & \dots & \alpha_1^{q^{n-1}} \\ \dots & \dots & \dots & \dots \\ \alpha_{n-1}^{q^0} & \alpha_{n-1}^{q^1} & \dots & \alpha_{n-1}^{q^{n-1}} \end{bmatrix}$$

which is a matrix of Vandermonde, then equation (5) has resolutions. So when the base  $B = (\alpha_0, \alpha_1, \dots, \alpha_{n-1})$  is determined, the q-polynomial function will be derived from the equation with complexity  $O(n^3)$ .

## 4 Application to AES S-box

In this section we will apply our theory in Sec.3 to AES S-box. It is referred to AES proposal for a full description of the cipher, but we only list the significant step which is named S-box here. This S-box is the only nonlinear part of AES, but it fulfills the most important function: confusion, which is one of the significant ideas in Shannon information theory. So we can consider that it determines the security of the whole block cipher to a large degree. The structure of the AES S-box is arranged as follows.

### 4.1 Basic Structure of AES S-box

The AES encrypts a 16-byte block using a 16-byte key with 10 encryption rounds. The value of each byte in the array is substituted according to a table look-up. This table look-up S-box is a combination of three transformations:

- The input  $x$  is mapped to  $x = x^{-1}$ , where  $x^{-1}$  is defined by  $x = x^{254} (x \neq 0)$ . Here we should notice the 'AES inversion' is identical to the standard field inversion in finite field for nonzero field elements but with  $0^{-1} = 0$ .
- The intermediate value  $x$  is regarded as a  $GF(2)$ -vector of dimension 8 and transformed using an  $8 \times 8$   $GF(2)$ -matrix  $L_A$ . The transformed vector  $L_A \cdot x$  is then regarded as an element of finite fields in the natural way.

$$L_A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Here the transformed vector  $L_A$  can be deduced from the polynomial module multiplication:

$$a(x)(x^7 + x^6 + x^5 + x^4 + 1) \bmod x^8 + 1$$

where  $a(x)$  denotes the polynomial expression of the value  $x$

which is regarded as a  $GF(2)$ -vector of dimension 8.

(c) Finally, the output of the AES S-box is  $L_4 \cdot x + 0x63$ , where addition is with respect to  $GF(2)$ . The constant  $0x63$  is used to eliminate the fixed point  $x \rightarrow x$  and contrary fixed point  $x \rightarrow \bar{x}$ .

The byte inversion operation over finite field  $GF(2^8)$  was chosen by its designers to resist all possibly linear and difference invariance, the basic ingredients of linear and differential cryptanalysis. However, by using simple algebraic operations with known properties, the combinations of them may possess many interesting and unexpected algebraic properties that were not known at the initial design time. The simple algebraic expression is one of the most interesting and disadvantageous properties, although no vulnerability has been found about it up to now. From the above description, we can derive the AES S-box algebraic expression:

$$\begin{aligned} y = & 05x^{254} + 09x^{253} + f9x^{251} + 29x^{247} + f4x^{239} + 01x^{223} \\ & + b5x^{191} + 8f7x^{127} + 0x63 = 05x^{-1} + 09(x^{-1})^2 + f9(x^{-1})^4 \\ & + 29(x^{-1})^8 + f4(x^{-1})^{16} + 01(x^{-1})^{32} + b5(x^{-1})^{64} \\ & + 8f7(x^{-1})^{128} + 0x63 \end{aligned} \quad (6)$$

From this equation (6), we find that it is an affine  $q$ -polynomial over  $GF(q^n)$  with respect to  $x^{-1}$ . In order to illustrate this reason, we should first reveal the nature of the structure of AES S-box.

#### 4.2 Why Fewer Terms of AES S-box Algebraic Expression

Obviously although the algebraic degree of AES S-box algebraic expression is up to utmost 254, but it is very simple, and only 9 terms are involved. For this simple algebraic expression, it is suspected to be vulnerable to the interpolation attack. But so far no accurate reason has illustrated the reason why only 9 terms are involved in AES S-box algebraic expression, so we are challenged this open problem and present a reasonable answer to it. From Sec.4.1, we know that the nature of the structure of AES S-box is that all the linear transformation of AES S-box is based on the bit-level (coordinates of elements of finite fields) operation with respect to element  $x^{-1}$ , so it is necessary first to investigate the relationship of the coordinates of elements with respect to the elements of finite fields.

For the finite field  $GF(q^n)$  generated by the irreducible polynomial  $g(x)$  with degree  $n$ , we connect the element  $x \in GF(q^n)$  to its coordinates  $x_i \in GF(q)$  with the help of the polynomial base  $B = (1, \alpha, \alpha^2, \dots, \alpha^{n-1})$  ( $\alpha$  is a root of  $g(x)$ ):  $x = (x_{n-1}, x_{n-2}, \dots, x_0)_B = \sum_{i=0}^{n-1} x_i \alpha^i$ . Then we have the following conclusion:

**Theorem 7:**  $x = (x_{n-1}, x_{n-2}, \dots, x_0)_B = \sum_{i=0}^{n-1} x_i \alpha^i, x_i \in GF(q)$ ,

then the relationship between the coordinates  $x_i$  and the element

$x$  of finite field  $GF(q^n)$  is  $x_i = \sum_{j=0}^{n-1} a_j x^{q^j}, 0 \neq a_j \in GF(q^n)$ .

**Proof:** Let  $B = (1, \alpha, \alpha^2, \dots, \alpha^{n-1})$  be one standard base over

$GF(q^n)$ , then it is derived that  $x = \sum_{i=0}^{n-1} x_i \alpha^i$ . Because of  $(x_i)^{q^k} = x_i$ , and  $q = p^m$  is the power of the character  $p$  of the finite fields, we obtain  $x^{q^k} = \sum_{i=0}^{n-1} x_i \alpha^{iq^k \bmod (q^n-1)}$ ,  $k = 0, 1, \dots, n-1$ , and we derive the following equation:

$$\begin{cases} x = \sum_{i=0}^{n-1} x_i \alpha^i \\ x^q = \sum_{i=0}^{n-1} x_i \alpha^{iq \bmod (q^n-1)} \\ \dots \\ x^{q^{n-1}} = \sum_{i=0}^{n-1} x_i \alpha^{iq^{n-1} \bmod (q^n-1)} \end{cases} \quad (7)$$

$x_i (i = 0, 1, 2, \dots, n-1)$  can be regarded as the variables, and then

equation (7) can be written as the following equation:

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^q & \alpha^{2q} & \dots & \alpha^{(n-1)q} \\ 1 & \alpha^{q^2} & \alpha^{2q^2} & \dots & \alpha^{(n-1)q^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{q^{n-1}} & \alpha^{2q^{n-1}} & \dots & \alpha^{(n-1)q^{n-1}} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{bmatrix} = \begin{bmatrix} x \\ x^q \\ x^{q^2} \\ \vdots \\ x^{q^{n-1}} \end{bmatrix} \quad (8)$$

Coordinates of (8) constitute a matrix of Vandermonde, so  $\prod_{0 \leq j < i \leq n-1} (\alpha^{q^i} - \alpha^{q^j}) \neq 0$ , and equation (8) has a resolution as  $x_i = \sum_{j=0}^{n-1} a_j x^{q^j}$ .

For  $(x_i)^q = (\sum_{j=0}^{n-1} a_j x^{q^j})^q = x_i = \sum_{j=0}^{n-1} a_j x^{q^j}$ , we derive

$a_j = a_{(j+1) \bmod n}$ . If  $\exists a_k = 0$ , then  $a_{(k+1) \bmod n} = a_{(k+2) \bmod n} = \dots = 0$ , that is for all  $a_i = 0 (i = 0, 1, 2, \dots, n-1)$ , it makes  $x_i = 0$ , which will never be a condition, so for all  $i = 0, 1, 2, \dots, n-1, a_j \neq 0$ .

From Theorem 7, we discover the relationship between  $x_i, i = (0, 1, \dots, n-1)$  and  $x$  is that  $x_i, i = (0, 1, \dots, n-1)$  is the linear combination of  $x$  with power  $q^i$ . This conclusion is very interesting and helpful to us, and it presents us a simple and direct method to resolve the reason why only 9 terms are involved in the expression of Rijndael S-box. We know in Sec.4.1 that after the inverse transformation of the elements of finite fields, all the transformation of Rijndael S-box is based on the bit-level, and all the operation is progressed over  $GF(2)$  linearly with respect to element  $x^{-1}$ , so after all the linear transformation, the expression still is a linear expression over  $GF(2)$ . It is well known that the linear expression over  $GF(2)$  has this form:  $f(x) = \sum_{j=0}^{n-1} a_j x^{2^j}$ ,  $a_j \in GF(2^n)$ , then after the affine transformation, the expression only includes  $n+1$  terms, and the algebraic expression is an affine  $q$ -polynomial with respect to  $x^{-1}$ . But we know that the inverse of elements over  $GF(2^n)$  has this form  $x^{-1} = x^{254}$ , and  $x^{255} = 1$ , thus the reason why only 9 terms are involved in the AES S-box expression is obviously resolved.

#### 4.3 Simple Method to Resolve AES S-box

According to the discussion in Sec.4.2, the conclusion of Theorem

7 is very interesting and helpful to us, and it presents us a simple and direct method to resolve the final algebraic expression of the bit-level affine transformation with a  $n$ -dimension equation classes and complexity  $O(n^3)$ . We know that all the transformation of the AES S-box is based on the bit-level expect the initial inverse transformation, so using the theory in Sec.4.2 we know that the ultimate algebraic expression will be an affine  $q$ -polynomial form. Then we constitute the following equation:

$$\begin{cases} \alpha_0^{2^0} b_0 + \dots + \alpha_0^{2^{n-1}} b_{n-1} = y(\alpha_0) - 0x63 \\ \alpha_1^{2^0} b_0 + \dots + \alpha_1^{2^{n-1}} b_{n-1} = y(\alpha_1) - 0x63 \\ \dots \\ \alpha_{n-1}^{2^0} b_0 + \dots + \alpha_{n-1}^{2^{n-1}} b_{n-1} = y(\alpha_{n-1}) - 0x63 \end{cases} \quad (9)$$

In equation (1),  $(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in GF(2^n)^n$  and  $\alpha_i \neq \alpha_j$ . So as long as  $(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in GF(2^n)^n$  is selected, the final algebraic expression of Rijndael S-box is determined quickly. This method is also applied to any structure that is based on the bit-level linear transformation. Although we do not know what the final algebraic expression of such structure is, but we have learned that affine transformation is based on the bit-level linear transformation, and then by the previous theory, we can obtain the ultimate expression quickly.

## 5 Conclusions

So far we know there are five methods to resolve the expression of Rijndael s-box:

- (1) Lagrange formula
- (2) Partition equivalence [7]
- (3) Resolve the equations [8]
- (4) Resolve the dual trace of natural base [8]
- (5) Resolve the  $q$ -polynomial [9] and in this paper

We illustrate the reason why the degree of the expression of Rijndael s-box is 254, but only 9 terms are involved in the expression, and it does not matter which irreducible polynomial as the generating polynomials, or the affine matrices and the affine constants are, so our method has the full generality.

## 6. REFERENCES

- [1]Joan Daemen, Vincent Rijmen. AES proposal: *Rijndael* [EB/OL]. <http://www.east.kuleuven.ac.be/~rijmen/rijndael>, 1999-10-05.
- [2]National Institute of Standard and Technology. *Advanced Encryption Standard FIPS197* [S]. November 26,2001.
- [3]C. E. Shannon. Communication Theory of Secrecy Systems .*The Bell system Technical Journal*, Vol. 28 No. 4, pp. 656-715
- [4]Nicolas T. Courtois, Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations[A]. *AsiaCrypt 2002*[C]. Berlin: Springer-Verlag, 2002. 267-287.

- [5]Murphy S, Robshaw M. Essential Algebraic Structure Within the AES [A]. *Advances in Cryptology: CRYPTO'02* [C]. Berlin: Springer-Verlag, 2002. 1-16.
- [6]Charles Seife. Crucial Cipher Flawed, *Cryptographers Claim*[J].*Science*,2002, 297:2193- 2193.
- [7]Wei Baodian,Liu Dongsu, Ma Wenping and Wang Xinmei, "Property of Finite Fields and Its Cryptography Application", *IEE Electronics Letters*, vol.39, no.8, pp.655-656, 2003.
- [8]Wei Baodian, Liu Jingwei, Wang Xinmei. *Trace Representations of Coordinates of Finite Field Elements and Their Cryptographic Applications*[A]. *ChinaCrypt'2004*[C]. Beijing: Science Press. pp. 42-49.
- [9] LiNa,Chen Weihong. *On the Cryptographic Properties of a class of S-boxes*. *ChinaCrypt' 2004*[C]. Beijing: Science Press. Pp. 64-73.