Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2017, Article ID 9828967, 9 pages
https://doi.org/10.1155/2017/9828967

Research Article

Algebraic Cryptanalysis Scheme of AES-256 Using Gröbner Basis

Kaixin Zhao,[1] Jie Cui,[2] and Zhiqiang Xie[2]

[1]*Department of Computer Science and Technology, Henan Institute of Technology, Xinxiang 453003, China*
[2]*School of Computer Science and Technology, Anhui University, Hefei 230039, China*

Correspondence should be addressed to Jie Cui; cuijie@mail.ustc.edu.cn

Received 22 October 2016; Accepted 22 January 2017; Published 23 February 2017

Academic Editor: Jucheng Yang

The zero-dimensional Gröbner basis construction is a crucial step in Gröbner basis cryptanalysis on AES-256. In this paper, after performing an in-depth study on the linear transformation and the system of multivariate polynomial equations of AES-256, the zero-dimensional Gröbner basis construction method is proposed by choosing suitable term order and variable order. After giving a detailed construction process of the zero-dimensional Gröbner basis, the necessary theoretical proof is presented. Based on this, an algebraic cryptanalysis scheme of AES-256 using Gröbner basis is proposed. Analysis shows that the complexity of our scheme is lower than that of the exhaustive attack.

1. Introduction

On October 2, 2000, the Rijndael algorithm, which was designed by Daemen and Rijmen, was determined by the National Institute of Standards and Technology (NIST) for the Advanced Encryption Standard (AES) [1]. It has been of concern to the cryptographic community since the Rijndael algorithm was proposed, and there have been many attack methods. However, there is no successful attack on the full Rijndael algorithm up to now [2, 3].

Cryptanalysis and cryptography not only are mutually antagonistic, but also promote each other. Because of the great advantages of algebraic cryptanalysis technology, it has become a hot research topic in recent years. Algebraic attack is mainly composed of two steps: the first step is to establish a system of algebraic equations to describe the relationship among the plaintext, the ciphertext, and the key in cryptographic algorithm; the second step is to solve the system of equations to obtain the key by some of the known plaintext-ciphertext pairs. The first step has already obtained some research results, and many scholars have proposed many kinds of equation systems of AES algorithm [4, 5]. In the second step, the multivariate equation system is still a problem to be solved. Although solving the multivariate equation system is an NP-hard problem, the complexity of solving a sparse overdetermined system of equations is far lower than that of the NP-hard problem.

At present, the methods of solving the high order multivariate equation system mainly include XL, XSL, and Gröbner basis. Since the algebraic expression of AES algorithm is sparse and structured, it is inefficient to apply XL attacks directly. In 2002, Courtois et al. proposed an XSL attack method and claimed to break the key length of 256-bit AES algorithm in theory. However, the number of linear independent equations generated by XSL attacks in the academic field is disputed, and the validity of the attack is questioned [6, 7]. Gröbner basis is an effective method for solving the high order multivariate equation system, which is proposed by Buchberger. Its essence is to set up a set of arbitrary ideals in polynomial rings, describe and compute a set of generators with good properties, and then study the ideal structure and carry out the ideal computation [3].

Gröbner basis is a standard representation method of polynomial ideals, which has some useful properties [8]. Gröbner basis exists in any ideal, and the Gröbner basis of any ideal can be computed by the Buchberger algorithm or F4 or F5 algorithm [6]. Lexicographic order is a commonly used elimination order. The coefficient matrix of the basis is triangular when using lexicographical Gröbner basis in the computation, and the last row solves single-variable equations. This is the reason why lexicographical Gröbner

basis can solve the equation system. But the direct computation of lexicographic Gröbner basis will produce excessive coefficients.

Common practice is to compute the total degree order Gröbner basis of the ideal firstly and then convert the total degree order Gröbner basis to lexicographical Gröbner basis using Gröbner basis conversion algorithm. Gröbner basis conversion algorithms include the Gröbner Walk [7] and the FGLM algorithm [6]. Compared with the Gröbner Walk, FGLM algorithm is simple and efficient, but the FGLM algorithm only works for zero-dimensional ideals [9, 10]. Therefore, constructing the zero-dimensional Gröbner basis of AES algorithm is crucial to implement Gröbner basis cryptanalysis. In 2013, the zero-dimensional Gröbner basis construction method of Rijndael-192 was proposed [11]. However, how to construct the zero-dimensional Gröbner basis of AES-256 and how to apply Gröbner basis cryptanalysis to AES-256 are still open questions. In this paper, the authors perform some particular studies on the linear transformation and the system of multivariate polynomial equations of AES-256 and propose its zero-dimensional Gröbner basis construction method through choosing suitable term order and variable order. After presenting the construction method of the Gröbner basis, the authors give the necessary theoretical proof. Moreover, the authors propose an algebraic cryptanalysis of AES-256 using Gröbner basis. Analysis suggests that the complexity of our scheme is lower than the exhaustive attack. The main contributions are given as follows:

(1) The zero-dimensional Gröbner basis construction method is proposed by choosing suitable term order and variable order.

(2) The necessary theoretical proof is given, and it shows that the set of polynomials is a zero-dimensional Gröbner basis.

(3) The effective algebraic cryptanalysis scheme of AES-256 using Gröbner basis is proposed.

The rest of this paper is formed as follows. The mathematical model of AES-256 is shown in Section 2. Section 3 demonstrates the Gröbner basis theory. The equation system of AES-256 is given in Section 4. In Section 5, the Gröbner basis construction method of AES-256 and the algebraic cryptanalysis scheme of AES-256 are proposed. Finally, the paper is concluded in Section 6.

2. Mathematical Model of AES-256

The block length and key length of AES can be specified independently as 128 bits, 192 bits, or 256 bits, and the corresponding round time is 10, 12, or 14. Each round consists of 4 transformations: the S-box substitution (ByteSub), ShiftRow, MixColumn, and AddRoundKey. With AES starting from the AddRoundKey, with 13 rounds of iteration, the final round is equal to the round with the MixColumn step removed. AES is an iterated block cipher with a variable block length and a variable key length. In this paper, both the block length and the key length are specified to 256 bits.

2.1. S-Box Substitution. The S-box transformation is a nonlinear byte substitution, operating on each of the state bytes independently. The S-box is invertible and is constructed by the composition of two transformations:

(1) Seeking the inverse operation of multiplication in $\mathrm{GF}(2^8) = Z_2[x]/(x^8 + x^4 + x^3 + x + 1)$ field, that is, input $\omega \in \mathrm{GF}(2^8)$ and output $\upsilon \in \mathrm{GF}(2^8)$, to meet

$$\omega * \upsilon = 1 \bmod \left(x^8 + x^4 + x^3 + x + 1\right), \tag{1}$$

then

$$\upsilon = \omega^{-1} = \begin{cases} \omega^{254}, & \omega \neq 0, \\ 0, & \omega = 0. \end{cases} \tag{2}$$

(2) Let element components of $x = \upsilon$ in $\mathrm{GF}(2)^8$ be $(x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0)$; the affine transformations are as follows:

$$y = \mathrm{La} \times x + \text{“63”}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}. \tag{3}$$

The selection of constant “63” is to ensure the S-box is not a fixed point $S(a) = a$ and an opposite fixed point $S(a) = \bar{a}$. S-box has the ability to resist linear attacks and differential attacks [1].

2.2. ShiftRow and MixColumn Transformations. The 4×8-byte matrix is obtained by S-box substitution, where $S_{i,j}$ is the byte in the ith row and the jth column, $0 \le i \le 3$, $0 \le j \le 7$. SR (ShiftRow) shift i bytes to the left for the ith row of the matrix:

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} \end{bmatrix} \longrightarrow$$

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} & s_{1,0} \\ s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} & s_{2,0} & s_{2,1} \\ s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} & s_{3,0} & s_{3,1} & s_{3,2} \end{bmatrix}. \tag{4}$$

MC (MixColumn) transforms the independent operation of each column for the purpose of causing confusion. Each

byte in each column is mapped to the new value; this value is 4 bytes in the column with the function obtained. Transformation is as follows:

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} & s'_{0,4} & s'_{0,5} & s'_{0,6} & s'_{0,7} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} & s'_{1,4} & s'_{1,5} & s'_{1,6} & s'_{1,7} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} & s'_{2,4} & s'_{2,5} & s'_{2,6} & s'_{2,7} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} & s'_{3,4} & s'_{3,5} & s'_{3,6} & s'_{3,7} \end{bmatrix} = D \cdot \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} \end{bmatrix}, \tag{5}$$

where

$$D = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}. \tag{6}$$

For mathematical convenience, we use a column vector instead of the original matrix to represent intermediate states and keys. The mapping relationship between the elements in column vector and the elements in the original matrix is as follows:

$$\varphi : F^{4\times 8} \longrightarrow F^{32},$$

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} & s_{0,4} & s_{0,5} & s_{0,6} & s_{0,7} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} & s_{1,4} & s_{1,5} & s_{1,6} & s_{1,7} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} & s_{2,4} & s_{2,5} & s_{2,6} & s_{2,7} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} & s_{3,4} & s_{3,5} & s_{3,6} & s_{3,7} \end{pmatrix} \longmapsto \tag{7}$$

$$(s_{0,0}, s_{1,0}, \ldots, s_{0,1}, s_{1,1}, \ldots)^T.$$

The finite field GF(2^8) is denoted as F in this paper. Introducing a 32×32 0-1 transformation matrix M_{SR}, the SR transform is equivalent to left multiplication by the matrix M_{SR}. There is only one element in each column and each row of the matrix is 1 and all the others are 0. Similarly, by introducing a new transformation matrix M_{MC}, the MC transform is equivalent to left multiplication by the matrix M_{MC}. The construction principle of M_{MC} is $M_{MC} = D \otimes I_8 \in F^{32\times 32}$, where $\otimes$ denotes tensor product and I_8 denotes 8-order identity matrix. The composite transformation of the SR transform and the MC transform is denoted as M, and then $M = M_{MC} \cdot M_{SR}$. It is easy to get

$$M = M_{MC} \cdot M_{SR}$$

$$= \begin{bmatrix}
02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03\\
00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02\\
00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00&00&00&00&01&00\\
00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00&00&00&00&03&00\\
00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00&00&00&00&02&00\\
00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00&00&00&00&01&00\\
00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00&00&00&00&03&00\\
00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&02&00\\
00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00&00&00&00&01&00\\
00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00&00&00&00&01&00\\
00&03&00&00&00&00&01&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&02&00\\
00&02&00&00&00&00&03&00&00&00&00&01&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00\\
00&01&00&00&00&00&02&00&00&00&00&03&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&01&00\\
00&01&00&00&00&00&01&00&00&00&00&02&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&00&03&00
\end{bmatrix}. \tag{8}$$

Thus, the linear transformation consisting of the SR transform and the MC transform can be expressed as

$$\begin{aligned}&\left(s''_{0,0}, s''_{1,0}, \ldots, s''_{0,1}, s''_{1,1}, \ldots\right)^T \\ &\quad = M \cdot \left(s_{0,0}, s_{1,0}, \ldots, s_{0,1}, s_{1,1}, \ldots\right)^T.\end{aligned} \tag{9}$$

2.3. AddRoundKey. In this operation, a round key is applied to the state by a simple bitwise EXOR. The round key is derived from the cipher key by means of the key schedule. It can be denoted as $Y = X \oplus K$, where K is the round key.

2.4. Key Schedule Algorithm. Key schedule consists of two modules: key expansion and round key selection. The block length and key length are denoted as N_b and N_k, respectively, and the unit is a 4-byte word. That is, N_b = block length/32 and N_k = key length/32. The number of rounds is denoted by R.

For AES-256, $N_b = 8$, $N_k = 8$, and $R = 14$. The key expansion of AES-256 is to extend eight 4-byte key words into 90 4-byte words $W[\cdot]$, where $W[0], \ldots, W[7]$ is the cipher key. The expansion algorithm is as shown in Algorithm 1.

3. Gröbner Basis Theory

Let R be a ring; for a nonempty ideal $I \subset R$, its Gröbner basis is generally not unique [12, 13]. The Gröbner basis is related to the selection of term orders. Related definitions are given below.

Definition 1. Order $\leq$ on a set $T(R)$ is called term order, if and only if $\leq$ is a linear order, and satisfies two properties:

(1) For all $t \in T(R)$, $t \geq 1$.

(2) For any $s, t_1, t_2 \in T(R)$, if $t_1 \leq t_2$, then $st_1 \leq st_2$.

In a term order $\leq$, the largest element of a polynomial p is called the head term of p, denoted as $\mathrm{HT}(p)$.

The set of natural numbers is $\mathbb{N}$, and n is a given positive integer, and $x_1, x_2, \ldots, x_n$ are n variables in ring R. Let the set of terms be

$$T(R) = \left\{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{N},\ i = 1, 2, \ldots, n\right\}. \tag{10}$$

That is, $T(R)$ is the power product set of n variables. The degree of term $t = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \in T(R)$ is denoted as $\deg(t) = \sum_{i=1}^{n} \alpha_i$. Let $X = (x_1, x_2, \ldots, x_n)$; then, the definitions of three common term orders will be given below.

Definition 2. $T(R)$ $x_1 > x_2 > \cdots > x_n$ on lexicographical order, denoted as lex, is defined as follows.

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, then $X^\alpha <_{\text{lex}} X^\beta \Leftrightarrow$ let $\alpha_j = \beta_j$, $j = 0, 1, \ldots, k$, and $\alpha_{k+1} < \beta_{k+1}$ $(\alpha_0 = \beta_0)$, where $0 \leq k \leq n-1$.

Definition 3. $T(R)$ $x_1 > x_2 > \cdots > x_n$ on degree lexicographical order, denoted as deglex, is defined as follows.

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, then

$$X^\alpha <_{\text{deglex}} X^\beta \Longleftrightarrow \begin{cases} \sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i & \text{or} \\ \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i, & \text{and according to the lexicographic order.} \\ X^\alpha <_{\text{lex}} X^\beta \end{cases} \tag{11}$$

Definition 4. $T(R)$ $x_1 > x_2 > \cdots > x_n$ on degree reverse lexicographical order, denoted as degrevlex, is defined as follows.

For $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{N}^n$, then

$$\begin{aligned}&X^\alpha <_{\text{degrevlex}} X^\beta \Longleftrightarrow \\ &\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i, \\ &\text{or } \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i, \\ &\alpha_n = \beta_n, \ldots, \alpha_{i+1} = \beta_{i+1},\ \alpha_i \neq \beta_i,\ \alpha_i > \beta_i, \text{between } \alpha \text{ and } \beta, \text{the first different coords from right side}, \alpha_i > \beta_i.\end{aligned} \tag{12}$$

Definition 5. Let R be a ring and let I be one nonzero ideal in R, $G = \{g_1, \ldots, g_m\} \subset I$. G is called the Gröbner basis of ideal I if and only if

$$\langle \mathrm{HT}(g_1), \ldots, \mathrm{HT}(g_m) \rangle = \langle \{\mathrm{HT}(p) : p \in I\} \rangle. \tag{13}$$

The Gröbner basis of any nonzero ideal can be obtained by using the Buchberger algorithm [12]. In the implementation of the Buchberger algorithm, the Buchberger rule can be used to eliminate unnecessary polynomials [12, 14]. Based on the Buchberger rule, the following conclusions can be obtained.

Theorem 6. *Let G be a set of polynomials, $H = \{HT(f) : f \in G\}$; if all elements in H are pairwise prime, then G is a Gröbner basis.*

Proof. See [15]. □

A zero-dimensional ideal is an ideal that has a finite number of solutions over the closure of the field. It usually

```
(1) for (i = 8; i < 90; i + +) do
(2)   if i %8 = 0 then
(3)     W[i] = W[i − 8] ⊕ BS(RotByte(W[i − 1])) ⊕const(i/8);
(4)   else
(5)     W[i] = W[i − 8] ⊕ W[i − 1];
(6)   end if
(7) end for
(8) return W[8], W[9], . . . , W[89];
```

Algorithm 1: Key expansion algorithm of AES-256.

is advantageous to have this property for Gröbner basis computations. By using Corollary 6.56 of [16], we can determine whether an ideal I is zero-dimensional. Below we state a reduced version of this corollary.

Theorem 7. *Let G be a Gröbner basis of the ideal I; then, $\dim(I) = 0$ if and only if, for any $1 \le i \le n$, there exists a polynomial $g \in G$, so that $HT(g) = x_i^{d_i}$.*

4. Equation System of AES-256

Let $((p_0, \ldots, p_{31}), (c_0, \ldots, c_{31})) \in F^{32} \times F^{32}$ be a known pair of plaintext and ciphertext in this paper. We call $x_{i,j}$ the jth element of the output of the AddRoundKey in the ith round transformation. We denote by $k_{i,j}$ the jth element of the ith round key. It is easy to see that $k_{0,j}$ denotes the cipher key, $0 \le i \le 14, 0 \le j \le 31$. The equation system on GF(2^8) consists of the following four parts:

(1) Initial round (round 0) equations and the cipher equations:

$$\begin{aligned} x_{0,0} + k_{0,0} + p_0 &= 0 \quad & x_{14,0} + c_0 &= 0 \\ &\vdots & &\vdots \\ x_{0,31} + k_{0,31} + p_{31} &= 0 \quad & x_{14,31} + c_{31} &= 0. \end{aligned} \tag{14}$$

(2) The equations of intermediate rounds, that is, the encryption equation of the ith round, $1 \le i \le 13$:

$$\begin{pmatrix} x_{i,0} + k_{i,0} \\ x_{i,1} + k_{i,1} \\ \vdots \\ x_{i,31} + k_{i,31} \end{pmatrix} + M \cdot \begin{pmatrix} S(x_{i-1,0}) \\ S(x_{i-1,1}) \\ \vdots \\ S(x_{i-1,31}) \end{pmatrix} = 0. \tag{15}$$

(3) The equations of the final round:

$$\begin{pmatrix} x_{14,0} + k_{14,0} \\ x_{14,1} + k_{14,1} \\ \vdots \\ x_{14,31} + k_{14,31} \end{pmatrix} + M_{\mathrm{SR}} \cdot \begin{pmatrix} S(x_{13,0}) \\ S(x_{13,1}) \\ \vdots \\ S(x_{13,31}) \end{pmatrix} = 0. \tag{16}$$

(4) Key scheduling equations:

$$\begin{pmatrix} k_{i,0} \\ k_{i,1} \\ k_{i,2} \\ k_{i,3} \\ k_{i,4} \\ k_{i,5} \\ \vdots \\ k_{i,31} \end{pmatrix} = \begin{pmatrix} k_{i-1,0} + S(k_{i-1,29}) + \xi^{i-1} \\ k_{i-1,1} + S(k_{i-1,30}) \\ k_{i-1,2} + S(k_{i-1,31}) \\ k_{i-1,3} + S(k_{i-1,28}) \\ k_{i-1,4} + k_{i,0} \\ k_{i-1,5} + k_{i,1} \\ \vdots \\ k_{i-1,31} + k_{i,27} \end{pmatrix}, \tag{17}$$

where ξ^{i-1} $(1 \le i \le 14)$ is a round constant.

5. Algebraic Cryptanalysis Scheme of AES-256

Definition 8. Denote the finite domain GF(2^8) as F; the multivariate polynomial ring on F, R is defined as

$$R := F\left[x_{i,j}, k_{i,j} : \{0 \le i \le 31, 0 \le j \le 14\}\right]. \tag{18}$$

To construct AES-256 Gröbner basis, the multivariate equation system obtained in Section 4 must be improved to meet the requirements of Gröbner basis; that is, the head terms of the polynomial on the left-hand side of the equation are pairwise prime.

5.1. The Gröbner Basis Construction Method of AES-256. The Gröbner basis of AES-256 is constructed as follows.

Step 1. The purpose of this step is to construct the polynomial set of the S-box and the inverse S-box. In this step, we make use of the algebraic expression of the S-box and the inverse S-box.

AES S-box is constructed based on evident mathematical theory, so it can be written in the form of an algebraic expression. The sparse algebraic expression of the S-box in F is as follows:

$$\begin{aligned} &S : F \longrightarrow F, \\ &x \longmapsto \\ &05x^{FE} + 09x^{FD} + F9x^{FB} + 25x^{F7} + F4x^{EF} + B5x^{DF} + B9x^{BF} + 8Fx^{7F} + 63. \end{aligned} \tag{19}$$

Table 1: Coefficients of algebraic expression of AES inverse S-box (Hex).

C (mn)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	F3	7E	1E	90	BB	2C	8A	1C	85	6D	C0	B2	1B	40	23
1	F6	73	29	D9	39	21	CF	3D	9A	8A	2F	CF	7B	04	E8	C8
2	85	7B	7C	AF	86	2F	13	65	75	D3	6D	D4	89	8E	65	05
3	EA	77	50	A3	C5	01	0B	46	BF	A7	0C	C7	8E	F2	B1	CB
4	E5	E2	10	D1	05	B0	F5	86	E4	03	71	A6	56	03	9E	3E
5	19	18	52	16	B9	D3	38	D9	04	E3	72	6B	BA	E8	BF	9D
6	1D	5A	55	FF	71	E1	A8	8E	FE	A2	A7	1F	DF	B0	03	CB
7	08	53	6F	B0	7F	87	8B	02	B1	92	81	27	40	2E	1A	EE
8	10	CA	82	4F	09	AA	C7	55	24	6C	E2	58	BC	E0	26	37
9	ED	8D	2A	D5	ED	45	C3	EC	1C	3E	2A	B3	9E	B7	38	82
A	23	2D	87	EA	DA	45	24	03	E7	C9	E3	D3	4E	DD	11	4E
B	81	91	91	59	A3	80	92	7E	DB	C4	20	EC	DB	55	7F	A8
C	C1	64	AB	1B	FD	60	05	13	2C	A9	76	A5	1D	32	8E	1E
D	C0	65	CB	8B	93	E4	AE	BE	5F	2C	3B	D2	0F	9F	42	CC
E	6C	80	68	43	09	23	C5	6D	1D	18	BD	5E	1B	B4	85	49
F	BC	0D	1F	A6	6B	D8	22	01	7A	C0	55	16	B3	CF	05	00

The nonsparse algebraic expression of the inverse S-box contains 255 terms. The coefficients of the algebraic expression of AES inverse S-box are shown in Table 1. The abbreviated form of the algebraic expression of AES inverse S-box can be expressed as follows:

$$S^{-1} : F \longrightarrow F,$$
$$x \longmapsto \sum_{i=0}^{254} c_i x^i, \tag{20}$$

where c_i is the coefficient of the term with degree i.

Step 2. The purpose of this step is to construct the polynomial set of linear transformations (i.e., ShiftRow and MixColumn). In this step, we use the equation system given in Section 4.

By (14), the plaintext equations, that is, the initial round equation system, can be obtained as (21), and the ciphertext equations can be obtained as (22). Hence,

$$x_{0,i} + k_{0,i} + p_i = 0, \quad p_i \in F, 0 \le i \le 31, \tag{21}$$

$$x_{14,i} + c_i = 0, \quad c_i \in F, 0 \le i \le 31. \tag{22}$$

Since $x_{0,i}$ and $k_{0,i}$ have the same degree, the head term of polynomials in (21) is $x_{0,i}$ or $k_{0,i}$. If the selected term order is $x_{0,i} < k_{0,i}$, then the head term of polynomial is $k_{0,i}$, $0 \le i \le 31$. For (22), the head term of polynomial is $x_{14,i}$, $0 \le i \le 31$.

It is needed to improve (15) and (16) to meet the requirements of Gröbner basis. From (15), it is easy to get 24 polynomial equations of round i $(1 \le i \le 13)$ as shown in

$$\begin{pmatrix} S(x_{i-1,0}) \\ S(x_{i-1,1}) \\ \vdots \\ S(x_{i-1,31}) \end{pmatrix} + M^{-1} \cdot \begin{pmatrix} x_{i,0} + k_{i,0} \\ x_{i,1} + k_{i,1} \\ \vdots \\ x_{i,31} + k_{i,31} \end{pmatrix} = 0. \tag{23}$$

Similarly, from (16), the 32 polynomial equations of the final round can be obtained as shown in

$$\begin{pmatrix} S(x_{13,0}) \\ S(x_{13,1}) \\ \vdots \\ S(x_{13,31}) \end{pmatrix} + M_{\mathrm{SR}}^{-1} \cdot \begin{pmatrix} x_{14,0} + k_{14,0} \\ x_{14,1} + k_{14,1} \\ \vdots \\ x_{14,31} + k_{14,31} \end{pmatrix} = 0. \tag{24}$$

For degree lexicographical order, the head term of polynomial in (23) and (24) is $x_{i,j}^{254}$, $0 \le i \le 13$, $0 \le j \le 31$. It is easy to see that the head term has no nontrivial common factor; that is, the greatest common factor is 1.

Step 3. The purpose of this step is to construct the polynomial set of the key schedule algorithm. In this step, we also use the equation system given in Section 4.

In order to get the polynomial Gröbner basis of the whole encryption algorithm, the equation system of the key schedule algorithm needs to be improved. It is easy to deduce (25) from (17). Hence,

$$\begin{pmatrix} k_{i,0} \\ k_{i,1} \\ k_{i,2} \\ k_{i,3} \\ k_{i,4} \\ k_{i,5} \\ \vdots \\ k_{i,31} \end{pmatrix} = \begin{pmatrix} k_{i-1,0} \\ k_{i-1,1} \\ k_{i-1,2} \\ k_{i-1,3} \\ k_{i-1,4} \\ k_{i-1,5} \\ \vdots \\ k_{i-1,31} \end{pmatrix} + \begin{pmatrix} S(k_{i-1,29}) \\ S(k_{i-1,30}) \\ S(k_{i-1,31}) \\ S(k_{i-1,28}) \\ k_{i,0} \\ k_{i,1} \\ \vdots \\ k_{i,27} \end{pmatrix}$$

$$+\begin{pmatrix} \xi^{i-1} \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{25}$$

In order to ensure that the head terms of key schedule polynomials are pairwise prime, applying the inverse S-box transformation to (25) is needed. The transformation results are shown in

$$\begin{pmatrix} S^{-1}\left(k_{i,0}+k_{i-1,0}+\xi^{i-1}\right) \\ S^{-1}\left(k_{i,1}+k_{i-1,1}\right) \\ S^{-1}\left(k_{i,2}+k_{i-1,2}\right) \\ S^{-1}\left(k_{i,3}+k_{i-1,3}\right) \\ k_{i,4}+k_{i-1,4} \\ k_{i,5}+k_{i-1,5} \\ \vdots \\ k_{i,31}+k_{i-1,31} \end{pmatrix} + \begin{pmatrix} k_{i-1,29} \\ k_{i-1,30} \\ k_{i-1,31} \\ k_{i-1,28} \\ k_{i,0} \\ k_{i,1} \\ \vdots \\ k_{i,27} \end{pmatrix} = 0. \tag{26}$$

According to the algebraic expression of the inverse S-box, all the equations included in (26) can be obtained. If the selected term order is

$$\begin{aligned} k_{i,31} > k_{i,30} > \cdots > k_{i,0} > k_{i-1,31} > \cdots > k_{i-1,1} \\ > k_{i-1,0}, \end{aligned} \tag{27}$$

where $1 \le i \le 14$, then the set of polynomial head terms of the key schedule equation (26) is

$$\left\{k_{i,j}^{254}, k_{i,h} : 1 \le i \le 14, 0 \le j \le 3, 4 \le h \le 31\right\}. \tag{28}$$

It is easy to see that the elements of the head term set have no nontrivial common factor.

Step 4. The purpose of this step is the reasonable selection of term order and variable order. If we choose a degree lexicographical order over reasonable variable order, we can make the polynomial head terms of the whole encryption algorithm pairwise prime.

The left-hand sides of (21), (22), (23), (24), and (26) constitute a set of polynomials denoted as A, and the degree lexicographical order $<_A$ over the following variable order makes the head terms of polynomials in A pairwise prime. Hence,

$$\begin{aligned} &\underbrace{x_{0,0} < \cdots < x_{0,31}}_{\text{initial round state variables}} < \underbrace{k_{0,0} < \cdots < k_{0,31}}_{\text{initial key variable}} \\ &< \underbrace{k_{1,0} < \cdots < k_{1,31}}_{\text{first round key variables}} < \cdots \\ &< \underbrace{k_{14,0} < \cdots < k_{14,31}}_{\text{last round key variables}} \\ &< \underbrace{x_{1,0} < \cdots < x_{1,31}}_{\text{first round internal state variables}} < \cdots \\ &< \underbrace{x_{13,0} < \cdots < x_{13,31}}_{\text{11th round internal state variables}} \\ &< \underbrace{x_{14,0} < \cdots < x_{14,31}}_{\text{ciphertext variables}}. \end{aligned} \tag{29}$$

After these four steps, the polynomial set A in the term order $<_A$ is a Gröbner basis of the ideal $\langle A\rangle$ in ring R. The following will give the relevant properties and their theoretical proof.

5.2. The Properties of AES-256 Gröbner Basis. Gröbner basis is the standard notation of polynomial ideal, and there are two useful properties: (1) given a Gröbner basis of an ideal, it is effective to determine whether a polynomial belongs to the ideal; (2) for reasonable term order, the ideal type can be calculated effectively, and the polynomial equation systems deduced from these ideals can be solved. The polynomial set A contains 720 polynomials, where 384 polynomials are with the degree 254 and 336 are linear polynomials that contain 720 variables $x_{i,j}, k_{i,j}, 0 \le i \le 14, 0 \le j \le 31$. For polynomial set A, there are the following conclusions.

Theorem 9. *The set of polynomials A is a Gröbner basis relative to degree lexicographical order $<_A$.*

Proof. Relative to the term order $<_A$, the head term set of polynomials in (21) is $H_1 = \{k_{0,i} : 0 \le i \le 31\}$, the head term set of polynomials in (22) is $H_2 = \{x_{14,i} : 0 \le i \le 31\}$, the head term set of polynomials in (23) and (24) is $H_3 = \{x_{i,j}^{254} : 0 \le i \le 13, 0 \le j \le 31\}$, and the head term set of polynomials in (26) is $H_4 = \{k_{i,j}^{254}, k_{i,h} : 1 \le i \le 14, 0 \le j \le 3, 4 \le h \le 31\}$, so the head term set of polynomials A is $H = H_1 \cup H_2 \cup H_3 \cup H_4$. Since, $\forall a, b \in H, \gcd(a, b) = 1$, elements in H are pairwise prime. According to Theorem 6, it can be obtained that the set of polynomials A is a Gröbner basis relative to term order $<_A$. □

Theorem 9 indicates that the set of polynomials A is a Gröbner basis of ideal $\langle A\rangle$ in ring R. This provides the possibility of carrying out the ideal calculation of AES-256.

Theorem 10. *The ideal $\langle A\rangle$ generated by Gröbner basis A of AES-256 is zero-dimensional.*

(1) list the equation system of AES-256 algorithm;
(2) select a known plaintext and ciphertext pair, and substitute it into the equation system;
(3) construct Gröbner basis Ggrelex of the ideal relative to degree lexicographical order using the method in Section 5.1;
(4) judge the solution structure of the Gröbner basis. Because the equation system contains the field equation, the equation is finite or no solution.
(5) **if and only if** Ggrelex = (1) **then**
(6) the equation system is no solution;
(7) **if** it is no solution, **then**
(8) select another plaintext and ciphertext pair to return to Step (3);
(9) **else** continue;
(10) **end if**
(11) **end if**
(12) convert degree lexicographical Gröbner basis Ggrelex to lexicographical Gröbner basis Glex by using FGLM algorithm;
(13) solve the key variables;
(14) verify the correctness of key by applying plaintext, ciphertext and key to AES-256 algorithm;
(15) **return** the key value;

Algorithm 2: Algebraic cryptanalysis algorithm of AES-256.

Proof. The variable set of the AES-256 equation system is $V = \{x_{i,j}, k_{i,j} : 0 \le i \le 14, 0 \le j \le 31\}$, so the number of variables is $|V| = 720$. It can be seen from the proof process of Theorem 9 that the head term set of polynomials set A is H. $\forall x \in V$, there exists $1 \le d \le 254$ satisfying $x^d \in H$; that is, all variables are in the form of a certain number of times in H. Based on this, for any variable x, there exists a polynomial $g \in A$, so that $\mathrm{HT}(g) = x^d$. According to Theorem 7, it is obvious that $\dim(\langle A \rangle) = 0$; that is, the ideal $\langle A \rangle$ generated by the Gröbner basis A is zero-dimensional. □

Theorem 10 points out that the Gröbner basis A constructed by this paper is zero-dimensional. Due to the term order conversion algorithm FGLM can convert any term order Gröbner basis of zero-dimensional ideal into lexicographical Gröbner basis, so the FGLM algorithm can convert degree lexicographical Gröbner basis A into lexicographical Gröbner basis. The construction of zero-dimensional Gröbner basis is helpful to simplify Gröbner basis calculation, which makes it possible to reduce the complexity of solving multivariate equation system.

5.3. The Algebraic Cryptanalysis Scheme and Its Complexity. The algebraic cryptanalysis algorithm of AES-256 is shown in Algorithm 2.

The maximum degree when computing the Gröbner basis is no more than N, where N is the number of the unknown variables in the equation system, so the upper bound of complexity of computing Gröbner basis is $O(2^N)$. Since the upper bound of the complexity of our scheme depends on the complexity of the Gröbner basis computation, the upper bound of the complexity of our scheme is $O(2^N)$. It can be seen from [17] that the complexity of exhaustively solving the equation system is $O(N2^N)$. It is obvious that the complexity of our scheme is less than the complexity of exhaustive attack, which indicates that our scheme is a successful attack scheme. Moreover, taking into account the sparse and overdefined features of AES-256 equation system, the actual complexity will be far less than the exhaustive attack.

Not all equations are always true in the equation system. For an S-box, there is an equation whose true probability is 255/256. For the full AES-256, the true probability of this kind of equation is 1/9. It needs 9 plaintext and ciphertext pairs to conduct computation 9 times in Step 3, and the equation system will have a finite set of solutions.

6. Conclusions

Based on the characteristics of the round transformation in AES-256, the ShiftRow and MixColumn transformations are merged into left multiplication by a matrix M, making it in the form of linear transformation. In further research on AES-256, the linear transformation and multivariate equation system of AES-256 are further studied. The Gröbner basis is proposed and constructed by choosing reasonable term order and variable order. At the same time, we point out and prove that the Gröbner basis is zero-dimensional. Based on this, the Gröbner basis attack scheme is proposed, and the attack complexity is far lower than the brute force attack. Taking into account the fact that the complexity of our scheme is very high, our research results have a theoretical value. However, the discovery of the zero-dimensional Gröbner basis of AES-256 has guiding significance for further study on efficient Gröbner based attack scheme. The complexity of FGLM and the effectiveness of Gröbner basis attack still need to be further studied.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (no. 61502008), the Key Scientific Research Project of Henan Higher Education (no. 16A520084), the Natural Science Foundation of Anhui

Province (no. 1508085QF132), and the Doctoral Research Start-Up Funds Project of Anhui University.

References

[1] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer Science & Business Media, 2013.

[2] A. Hashemi and D. Lazard, "Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving," *International Journal of Algebra and Computation*, vol. 21, no. 5, pp. 703–713, 2011.

[3] M. Bardet, J.-C. Faugère, and B. Salvy, "On the complexity of the F_5 Gröbner basis algorithm," *Journal of Symbolic Computation*, vol. 70, pp. 49–70, 2015.

[4] A. Bogdanov and V. Rijmen, "Linear hulls with correlation zero and linear cryptanalysis of block ciphers," *Designs, Codes and Cryptography*, vol. 70, no. 3, pp. 369–383, 2014.

[5] Y. Sasaki, "Known-key attacks on rijndael with large blocks and strengthening shiftrow parameter," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 95, no. 1, pp. 21–28, 2012.

[6] C. Cid and G. Leurent, "An Analysis of the XSL Algorithm," in *Advances in cryptology—ASIACRYPT 2005*, vol. 3788 of *Lecture Notes in Comput. Sci.*, pp. 333–352, Springer, Berlin, Germany, 2005.

[7] S. Murphy and M. Robshaw, "Comments on the security of the AES and the XSL technique," *Electronic Letters*, vol. 39, no. 1, pp. 36–38, 2003.

[8] J. Buchmann, A. Pyshkin, and R.-P. Weinmann, "A zero-dimensional Gröbner basis for AES-128," *Lecture Notes in Computer Science*, vol. 4047, pp. 78–88, 2006.

[9] S. Ghosh and A. Das, "An improvement of linearization-based algebraic attacks," in *Security Aspects in Information Technology*, vol. 7011 of *Lecture Notes in Computer Science*, pp. 157–167, Springer, 2011.

[10] M. R. Z'Aba, K. Wong, E. Dawson, and L. Simpson, "Algebraic analysis of small scale LEX-BES," in *Proceedings of the 2nd International Cryptology Conference: Curve is an Art, Cryptology is a Science (Cryptology '10)*, pp. 77–82, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia, July 2010.

[11] J. Cui, L. Huang, H. Zhong, and W. Yang, "Algebraic attack on Rijndael-192 based on Grobner basis," *Acta Electronica Sinica*, vol. 41, no. 5, pp. 833–839, 2013.

[12] S. N. Ahmad and N. Aris, "The Gröbner package in Maple and computer algebra system for solving multivariate polynomial equations," *Academic Journal UiTM Johor*, vol. 10, pp. 156–174, 2011.

[13] M. Bardet, J. C. Faugere, and B. Salvy, "On the complexity of the F_5 Gröbner basis algorithm," *Journal of Symbolic Computation*, vol. 70, pp. 49–70, 2015.

[14] V. Gerdt and R. La Scala, "Noetherian quotients of the algebra of partial difference polynomials and Gröbner bases of symmetric ideals," *Journal of Algebra*, vol. 423, pp. 1233–1261, 2015.

[15] J. Buchmann, A. Pyshkin, and R.-P. Weinmann, "Block ciphers sensitive to Gröbner basis attacks," in *Topics in Cryptology—CT-RSA 2006*, vol. 3860 of *Lecture Notes in Comput. Sci.*, pp. 313–331, Springer, Berlin, Germany, 2006.

[16] D.-M. Li, J.-W. Liu, and W.-J. Liu, "W-Gröbner basis and monomial ideals under polynomial composition," *Applied Mathematics A*, vol. 26, no. 3, pp. 287–294, 2011.

[17] J.-C. Faugère and A. Joux, "Algebraic cryptanalysis of Hidden Field Equation (HFE) cryptosystems using Gröbner bases," in *Proceedings of the Annual International Cryptology Conference (CRYPTO '03)*, vol. 2729 of *Lecture Notes in Computer Science LNCS*, pp. 44–60, Springer, Santa Barbara, Calif, USA, 2003.