A Probabilistic Problem Related to Difference Equations for Modulo Additions

Minghao Bai

Nanjing Foreign Language School, Nanjing, 210008, China

Abstract: *Based on differential analysis in modern cryptography, this paper studies the differential probability of the modular addition operation in the cipher algorithm of ARX structure. This paper first researches characteristics of modulo addition operations through binary expansion and expresses probabilities by carry bit difference expression calculation. By using the Markov chain and state transition matrix, we determine the probability distribution of the number of solutions for a modulo addition difference equation system containing two equations with respect to the difference value, and calculate the mathematical expectation of the number of solutions. At last, this paper provides future research on related probability problems with new insights and methods.*

Keywords: *differential analysis, Markov chain, state transition matrix, modulo addition difference equations*

1. Introduction

In modern cryptography, block cipher is often used to encrypt data. The design of modern block ciphers usually adopts key alternating structure, and the specific structure of cipher algorithms includes Feistel structure, SPN structure and ARX structure [1]. Among them, the cipher algorithm of ARX structure mainly uses integer modulo addition "+", bit-wise XOR "⊕" and bit vector cyclic shift" >>> ", which is a kind of structure that has been widely concerned in the field of block cipher algorithm design in recent years [2]. Differential analysis is a basic and important method in the analysis of block ciphers [1]. The core idea of differential analysis method is to find the input differenceΔX and output differenceΔY for a given cryptographic algorithm E_k, so that the difference propagation$\Delta X \rightarrow \Delta Y$has a high probability. The differential propagation probability is defined as

$$Pr_E[\Delta X \rightarrow \Delta Y] = \frac{1}{2^n} \cdot \# \{ X \in F_2^n \mid E(x) \oplus E(X \oplus \Delta X) = \Delta Y \}.$$

Therefore, in difference analysis, the key problem is to study the distribution of the solutions of the difference equation $E(x) \oplus E(X \oplus \Delta X) = \Delta Y$ for fixed ΔX and ΔY . (See figure 1)

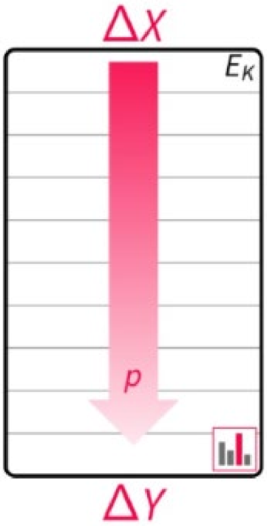

Figure 1: Transformation from ΔX to ΔY under E_k

The purpose of this paper is to analyze modulo addition difference equations that need to be dealt with in the differential analysis of ARX structured block cipher. The specific form is as follows:

$$\begin{cases} X \oplus Y = Z \\ (Y \oplus \beta) \oplus (X \oplus \alpha) = (Z \oplus \gamma). \end{cases} \tag{1}$$

where $X, Y, Z \in \mathbb{Z}/2^n\mathbb{Z}$ represents the variable to be solved, $\alpha, \beta, \gamma \in \mathbb{Z}/2^n\mathbb{Z}$ are given integers, which represent given difference values.

For equation system (1), we studies number of solutions of (1) based on given α, β, γ. Assuming that the input and output differences in the equation system (1) are known, and that the input differences are independent and uniformly distributed, we want to calculate the mathematical expectation of the number of solutions for the equation system (1).

Firstly, by studying characteristics of modulo addition operation in the equation system (1), two equations can be converted into the probability of existing solutions in a single equation. By transforming the difference expression, we find the condition of the special case with probability 0. For other cases, the expression of each conditional difference probability is obtained by transforming the characteristics of probability distribution. We conclude the condition of non-zero probability of differential propagation by using Markov chain and calculating the correlation state transition matrix. Finally, the expected expression of the correlation solution is calculated by using the obtained conclusion.

The structure of this paper is as follows: In the second part, by combing the modulo addition operation, we get recursive relation to express the binary carry of modulo addition operation, and further use each bit to express recursive expression; In the third part, through the transformation of two equations in the original problem and the carry recurrence in the second section, we get the preliminary condition that the probability is 0 for a special value on each bit α, β, γ. Based on the conditional probability formula and the characteristics of uniformly distributed binary variables in the modulo addition operation, we find the specific probability values under different conditional probabilities; In the fourth part, by using the mathematical tool of Markov chain, we transform probability calculation into matrix product, and all matrices are obtained for different values. In the fifth part, through the calculation results of the matrix in the probability in the fourth section, the specific values and conditions of the probability of the original problem are obtained, and the mathematical expectation of the number is further calculated.

2. Carry Characteristics of Modulo Addition Operations

Let $X, Y, Z \in \mathbb{Z}/2^n\mathbb{Z}$, for any such integer can be binary expansion, for example:

$$\mathrm{X} = \mathrm{X}_0 + \mathrm{X}_1 \times 2 + \ldots + \mathrm{X}_{n-1} \times 2^{n-1},$$

where $\mathrm{X}_k \in \mathbb{F}_2, \mathrm{k} = 0,1,2,\ldots,\mathrm{n}-1$.

Following this expansion, we can correspond $X \in \mathbb{Z}/2^n\mathbb{Z}$ to a vector of length *n*, that is:

$$\mathrm{X} \to (\mathrm{X}_{n-1},\ \mathrm{X}_{n-2}, \dots, \mathrm{X}_1, \mathrm{X}_0),$$

which are called a bit vector.

Considering the system equations (1) with the idea of bit vectors, we find that,

$$\begin{aligned} \mathrm{X} + \mathrm{Y} &= (\mathrm{X}_{n-1},\ \mathrm{X}_{n-2}, \dots, \mathrm{X}_1, \mathrm{X}_0) + (\mathrm{Y}_{n-1},\ \mathrm{Y}_{n-2}, \dots, \mathrm{Y}_1, \mathrm{Y}_0) \\ &= \mathrm{Z} \\ &= (\mathrm{Z}_{n-1},\ \mathrm{Z}_{n-2}, \dots, \mathrm{Z}_1, \mathrm{Z}_0). \end{aligned}$$

We use c_i to represent the bit *i* of a carry bit. Then we find carry bits of bits 0 and 1 can be represented as $\mathrm{c}_0 = 0, \mathrm{c}_1 = \mathrm{X}_0\mathrm{Y}_1$. Combine carry bits, so that the modulo of bit zero and bit i are represented as $\mathrm{Z}_0 = \mathrm{X}_0 \oplus \mathrm{Y}_0$, $\mathrm{Z}_\mathrm{i} = \mathrm{X}_\mathrm{i} \oplus \mathrm{Y}_\mathrm{i} \oplus c_\mathrm{i}$. Considering properties of $\mathrm{X}_\mathrm{i}, \mathrm{Y}_\mathrm{i}, \mathrm{c}_\mathrm{i} \in \mathbb{F}_2$, we can further construct an expression of carry bits $\mathrm{c}_{\mathrm{i}+1} = \mathrm{X}_\mathrm{i}\mathrm{Y}_\mathrm{i} \oplus \mathrm{c}_\mathrm{i}(\mathrm{X}_\mathrm{i} \oplus \mathrm{Y}_\mathrm{i})$.With the recursive carry bit expression, we get,

$$\begin{aligned} \mathrm{c}_{\mathrm{i}+1} &= \mathrm{X}_\mathrm{i}\mathrm{Y}_\mathrm{i} \oplus \mathrm{c}_\mathrm{i}(\mathrm{X}_\mathrm{i} \oplus \mathrm{Y}_\mathrm{i}) \\ &= \mathrm{f}(\mathrm{X}_0,\mathrm{X}_1,\ldots,\mathrm{X}_\mathrm{i},\mathrm{Y}_0,\mathrm{Y}_1,\ldots,\mathrm{Y}_\mathrm{i}) \end{aligned}$$

$$= \mathrm{X_iY_i} \oplus (\mathrm{X_i} \oplus \mathrm{Y_i})[\mathrm{X_{i-1}Y_{i-1}} \oplus \mathrm{c_{i-1}}(\mathrm{X_{i-1}} \oplus \mathrm{Y_{i-1}})]$$

$$= \mathrm{X_iY_i} \oplus \mathrm{X_iX_{i-1}Y_{i-1}} + \ldots$$

3. Transformation of Modulo Addition Difference Equations

This section further studies the equation system (1), converts the equation system with two equations into a single equation, brings the first line of the equation system (1) $\mathrm{X + Y}$into the Z in the second line, and obtains,

$$(Y \oplus \beta) \oplus (X \oplus \alpha) = (X + Y) \oplus \gamma.$$

For such a difference equation, the propagation probability of the solution of this difference equation can be further calculated by dividing the number of solutions $2^{2\mathrm{n}}$. The calculation process is as follows:

$$\Pr[(\alpha, \beta) \rightarrow \gamma]$$

$$= \frac{1}{2^{2\mathrm{n}}} \#\{(\mathrm{X}, \mathrm{Y}) | (\mathrm{Y} \oplus \beta) \oplus (\mathrm{X} \oplus \alpha) = (\mathrm{X} + \mathrm{Y}) \oplus \gamma\}$$

$$= \frac{1}{2^{2\mathrm{n}}} \#\{(\mathrm{X}, \mathrm{Y}) | [(\mathrm{Y} \oplus \beta) \oplus (\mathrm{X} \oplus \alpha)][\mathrm{X} + \mathrm{Y}] = \gamma\}$$

$$= \frac{1}{2^{2\mathrm{n}}} \#\{(\mathrm{X}, \mathrm{Y}) | \mathrm{X_i} \oplus \mathrm{Y_i} \oplus \mathrm{c_i}(\mathrm{X}, \mathrm{Y}) \oplus \mathrm{X_i} \oplus \alpha_\mathrm{i} \oplus \mathrm{y_i} \oplus \beta_\mathrm{i} \oplus \mathrm{c_i^*}(\mathrm{X} \oplus \alpha_\mathrm{i}, \mathrm{Y} \oplus \beta_\mathrm{i}) = \gamma_\mathrm{i}; 0 \le \mathrm{i} \le \mathrm{n} - 1\}$$

$$= \frac{1}{2^{2\mathrm{n}}} \#\{(\mathrm{X}, \mathrm{Y}) | \mathrm{c_i}(\mathrm{X}, \mathrm{Y}) \oplus \mathrm{c_i^*}(\mathrm{X} \oplus \alpha_\mathrm{i}, \mathrm{Y} \oplus \beta_\mathrm{i}) = \alpha_\mathrm{i} \oplus \beta_\mathrm{i} \oplus \gamma_\mathrm{i}; 0 \le \mathrm{i} \le \mathrm{n} - 1\}$$

$$= \frac{1}{2^{2\mathrm{n}}} \#\{(\mathrm{X}, \mathrm{Y}) | \Delta \mathrm{c} = \alpha \oplus \beta \oplus \gamma\}.$$

For the carry bit, we consider the difference of the carry bit further, i.e.,

$$\Delta \mathrm{c_{i+1}} = \mathrm{c_{i+1}}(\mathrm{X}, \mathrm{Y}) \oplus \mathrm{c_{i+1}^*}(\mathrm{X} \oplus \alpha, \mathrm{Y} \oplus \beta)$$

$$= \mathrm{c_{i+1}} \oplus \mathrm{c_{i+1}^*}$$

$$= \mathrm{X_iY_i} \oplus \mathrm{c_i}(\mathrm{X_i} \oplus \mathrm{Y_i}) \oplus (\mathrm{X_i} \oplus \alpha_\mathrm{i})(\mathrm{y_i} \oplus \beta_\mathrm{i}) \oplus \mathrm{c_i^*}(\mathrm{X_i} \oplus \alpha_\mathrm{i} \oplus \mathrm{Y_i} \oplus \beta_\mathrm{i})$$

$$= \mathrm{c_i}(\mathrm{X_i} \oplus \mathrm{Y_i}) \oplus \mathrm{X_i}\beta_\mathrm{i} \oplus \alpha_\mathrm{i}\mathrm{y_i} \oplus \alpha_\mathrm{i}\beta_\mathrm{i} \oplus \mathrm{c_i^*}(\mathrm{X_i} \oplus \alpha_\mathrm{i} \oplus \mathrm{Y_i} \oplus \beta_\mathrm{i})$$

$$= (\alpha_\mathrm{i} \oplus \gamma_\mathrm{i} \oplus \beta_\mathrm{i})(\mathrm{X_i} \oplus \mathrm{Y_i}) \oplus \mathrm{X_i}\beta_\mathrm{i} \oplus \alpha_\mathrm{i}\mathrm{y_i} \oplus \alpha_\mathrm{i}\beta_\mathrm{i} \oplus \mathrm{c_i^*}(\alpha_\mathrm{i} \oplus \beta_\mathrm{i}),$$

where $\mathrm{c_i^*} = \mathrm{X_i} \oplus \alpha_\mathrm{i} \oplus \mathrm{Y_i} \oplus \beta_\mathrm{i} \oplus \mathrm{Z_i} \oplus \gamma_\mathrm{i}$.

It is to easy to find that when

$$\alpha_\mathrm{i} \oplus \gamma_\mathrm{i} \oplus \beta_\mathrm{i} = 1, \Pr[(\alpha, \beta) \rightarrow \gamma] = 0. \tag{2}$$

Lemma 1 Let Z, Y be two independent binary variables. If they satisfy $\Pr[\mathrm{Z} = 0] = \Pr[\mathrm{Z} = 1] = 0.5$, $\Pr[\mathrm{Y} = 0] = \mathrm{p}, \Pr[\mathrm{Y} = 1] = 1 - \mathrm{p}$,then $\mathrm{Z} \oplus \mathrm{Y}$ follows a uniform distribution.

Proof:We have

$$\Pr[\mathrm{Z} \oplus \mathrm{Y} = 0] = \Pr[\mathrm{Z} = 0, \mathrm{Y} = 0] + \Pr[\mathrm{Z} = 1, \mathrm{Y} = 1]$$

$$= \Pr[\mathrm{Z} = 0 | \mathrm{Y} = 0] \times \Pr[\mathrm{Z} = 0] + \Pr[\mathrm{Z} = 1, \mathrm{Y} = 1] \times \Pr[\mathrm{Z} = 1]$$

$$= \frac{1}{2}[\Pr[\mathrm{Y} = 0] + \Pr[\mathrm{Y} = 1]]$$

$$= \frac{1}{2},$$

then the result follows.

Corollary 2 Let $\mathrm{Z}, \mathrm{Y_1}, \mathrm{Y_2}, \ldots \mathrm{Y_m}$ be independent binary variables. If they satisfy $\Pr[\mathrm{Z} = 0] = \Pr[\mathrm{Z} = 1] = 0.5$, then $\mathrm{Z} \oplus \mathrm{Y_1} \oplus \mathrm{Y_2} \oplus \ldots \oplus \mathrm{Y_m}$ is subject to uniform distribution.

Proof: Using mathematical first induction, for $\mathrm{m} = 1$, it is easy to prove by **Lemma 1**. So assume $\mathrm{m} = \mathrm{n}, \mathrm{Z} \oplus \mathrm{Y_1} \oplus \mathrm{Y_2} \oplus \ldots \oplus \mathrm{Y_n}$is a uniform distribution. What we need to prove is that for $\mathrm{m} = \mathrm{n} + 1, \mathrm{Z} \oplus \mathrm{Y_1} \oplus \mathrm{Y_2} \oplus \ldots \oplus \mathrm{Y_n} \oplus \mathrm{Y_{n+1}}$is a uniform distribution.

Let $Z \oplus Y_1 \oplus Y_2 \oplus \ldots \oplus Y_n = Z'$, we find that,

$$\Pr[Z' \oplus Y_{n+1} = 0] = \Pr[Z' = 0, Y_{n+1} = 0] + \Pr[Z' = 1, Y_{n+1} = 1]$$

$$= \Pr[Z' = 0 | Y_{n+1} = 0] \times \Pr[Z' = 0] + \Pr[Z' = 1, Y_{n+1} = 1] \times \Pr[Z' = 1]$$

$$= \frac{1}{2}[\Pr[Y_{n+1} = 0] + \Pr[Y_{n+1} = 1]]$$

$$= \frac{1}{2}.$$

As a result, $Z \oplus Y_1 \oplus Y_2 \oplus \ldots \oplus Y_n \oplus Y_{n+1}$ follows a uniform distribution.

Combining Lemma 1 and Corollary 1, we get,

$$\Pr(\Delta c_{i+1} = 0) = \Pr[\Delta c_{i+1} = 0 | \Delta c_i = 0] \times \Pr[\Delta c_i = 0] + \Pr[\Delta c_{i+1} = 0 | \Delta c_i = 1] \times \Pr[\Delta c_i = 1],$$

$$\Pr(\Delta c_{i+1} = 1) = \Pr[\Delta c_{i+1} = 1 | \Delta c_i = 1] \times \Pr[\Delta c_i = 0] + \Pr[\Delta c_{i+1} = 1 | \Delta c_i = 0] \times \Pr[\Delta c_i = 1].$$

According to formula (2), the difference of carry bits can be obtained:

$$\Delta c_{i+1} = \Delta c_i (X_i \oplus Y_i) \oplus X_i \beta_i \oplus \alpha_i y_i \oplus \alpha_i \beta_i \oplus c_i^* (\alpha_i \oplus \beta_i).$$

We can combine difference of carry bits with (2). Considering the different values of $\alpha_i, \beta_i, \gamma_i \in \mathbb{F}_2$and using the carry bit difference expression calculation, we can get the following probability,

$$\Pr[\Delta c_{i+1} = 1 | \Delta c_{i+1} = r] = T(\alpha_i, \beta_i, \gamma_i)$$

$$= \begin{cases} 0 & \alpha_i + \beta_i + \gamma_i = 0 \\ \frac{1}{2} & \alpha_i + \beta_i + \gamma_i = 1,2 \\ 1 & \alpha_i + \beta_i + \gamma_i = 3. \end{cases}$$

Let $T: (\alpha, \beta, \gamma) \leftrightarrow 4\alpha + 2\beta + \gamma = Z$, we get,

$$T(Z) = \begin{cases} 0 & Z = 0 \\ \frac{1}{2} & 1 \leq Z \leq 6 \\ 1 & Z = 7. \end{cases}$$

4. Establishment of Markov Chains and Calculation of Matrices

Returning to the original problem, the equation system (1), according to the calculation of the differential propagation probability of carry bits in part 3, this part presents a method based on Markov chain to describe the state transition rule between carries and calculate the state transition matrix of Markov chain.

For $i, j \in \mathbb{F}_2$, we get,

$$P_j(k) = \Pr[\Delta c_k = j, \Delta c_s = w_s, 0 \leq s \leq k-1]$$

$$P_i(k) = \Pr[\Delta c_{k+1} = i, \Delta c_k = w_k, \Delta c_s = w_s, 0 \leq s \leq k-1]$$

$$= \Pr[\Delta c_{k+1} = i, \Delta c_k = w_k \mid \Delta c_k = 0, \Delta c_s = w_s] \cdot \Pr[\Delta c_k = 0, \Delta c_s = w_s]$$

$$+\Pr[\Delta c_{k+1} = i, \Delta c_k = w_k \mid \Delta c_k = 1, \Delta c_s = w_s] \cdot \Pr[\Delta c_k = 1, \Delta c_s = w_s].$$

The differential propagation probability expression is further obtained,

$$\Pr[(\alpha, \beta) \to \gamma] = \Pr[\Delta c = \alpha \oplus \beta \oplus \gamma]$$

$$= \Pr[\Delta c_0 = w_0, \Delta c_1 = w_1, \ldots, \Delta c_{n-1} = w_{n-1}](w = \alpha \oplus \beta \oplus \gamma)$$

$$= \Pr[\Delta c_{n-1} = w_{n-1} \mid \Delta c_0 = w_0, \Delta c_1 = w_1, \ldots, \Delta c_{n-2} = w_{n-2}]$$

$$\cdot \Pr[\Delta c_i = w_i, 0 \leq i \leq n-2].$$

Based on Markov chain, the state transition formula is obtained [3],

$$[\begin{matrix} P_0(k+1) \\ P_1(k+1) \end{matrix}] = (A_k)_{ij} [\begin{matrix} P_0(k) \\ P_1(k) \end{matrix}],$$

where,

$$(A_k)_{ij} = \begin{cases} T(\alpha_k + \beta_k + \gamma_k) & i = 1, w_k = j \\ 1 - T(\alpha_k + \beta_k + \gamma_k) & i = 0, w_k = j \\ 0 & w_k \neq j. \end{cases}$$

Theorem 4.1: Let $w_i = 4\alpha_i + 2\beta_i + \gamma_i \in [0,7]$. Then

$$\Pr[(\alpha,\beta) \to \gamma] = \binom{1}{0} A_{w_0} \cdots A_{w_{n-1}} (1\ 1).$$

Through the established Markov chain progressive relationship, the matrix can be obtained as follows,

$$A_7 = \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, A_0 = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix},$$

$$A_3 = A_5 = A_6 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, A_1 = A_2 = A_4 = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Considering the different methods of obtaining the above four matrices in **Theorem 4.1**, the above calculation process is repeated as follows:

$$A_0\binom{1}{0} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\binom{1}{0} = \binom{1}{0}$$

$$A_1\binom{1}{0} = A_2\binom{1}{0} = A_4\binom{1}{0} = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\binom{1}{0} = \binom{0}{0}$$

$$A_3\binom{1}{0} = A_5\binom{1}{0} = A_6\binom{1}{0} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\binom{1}{0} = \frac{1}{2}\binom{1}{1}$$

$$A_7\binom{1}{0} = \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}\binom{1}{0} = \binom{0}{0}$$

$$A_0\binom{0}{1} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\binom{0}{1} = \binom{0}{0}$$

$$A_1\binom{0}{1} = A_2\binom{0}{1} = A_4\binom{0}{1} = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\binom{0}{1} = \frac{1}{2}\binom{1}{1}$$

$$A_3\binom{0}{1} = A_5\binom{0}{1} = A_6\binom{0}{1} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\binom{0}{1} = \binom{0}{0}$$

$$A_7\binom{0}{1} = \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}\binom{0}{1} = \binom{0}{1}$$

$$A_0\binom{1}{1} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\binom{1}{1} = \binom{1}{0}$$

$$A_1\binom{1}{1} = A_2\binom{1}{1} = A_4\binom{1}{1} = \frac{1}{2}\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\binom{1}{1} = \frac{1}{2}\binom{1}{1}$$

$$A_3\binom{1}{1} = A_5\binom{1}{1} = A_6\binom{1}{1} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\binom{1}{1} = \frac{1}{2}\binom{1}{1}$$

$$A_7\binom{1}{1} = \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}\binom{1}{1} = \binom{0}{1}.$$

5. Mathematical Expectation Calculation

Theorem 5.1: The sufficient and necessary conditions for $\Pr[(\alpha,\beta) \to \gamma] = \Pr[w_0, w_1, \ldots, w_{n-1}] = 0$ are,

(1)$w_0 \in \{1,2,4,7\}$,

(2)$\exists w_{i-1} = 0, w_i \in \{1,2,4,7\}$,

(3)$\exists w_{i-1} = 7, w_i \in \{0,3,5,6\}$.

(At least one or more conditions are met）

Proof:

If the zero matrix appears in the state transition matrix, by Theorem 4.1, the differential propagation probability must be 0 by calculation.

By observing the zero matrix above, it can be found that if the initial subscript $w_0 = 1,2,4,7$, the initial matrix is zero matrix.

If there is a subscript of $w_{i-1} = 0$, by observing the $w_i = 1,2,4,7$ there also appears a zero matrix.

On the other hand, if there is a subscript of $w_{i-1} = 7$, by observing the $w_i = 1,2,4,7$.There is a zero matrix.

Theorem 5.2: The sufficient and necessary conditions for $\Pr[(\alpha,\beta) \to \gamma] = \Pr[w_0, w_1, \ldots, w_{n-1}] \neq 0$ are,

(1)$w_0 \in \{0,3,5,6\}$,

(2)$\forall w_{i-1} = 7, w_i \in \{1,2,4,7\}$,

(3)$\forall w_{i-1} = 0, w_i \in \{0,3,5,6\}$.

(At least one or more conditions are met）

Proof:

Considering that **Theorem 5.1** and **Theorem 5.2** are complementary propositions, it is easy to obtain **Theorem 5.2**.

Combining **Theorem 5.1** and **Theorem 5.2**,

$$\Pr[w_0, w_1, \ldots, w_{n-1}] = 2^{-k}, k = \#\{0 \leq i \leq n-2 \mid w_i \neq 0,7\}.$$

Mathematical expectations [4] are:

$$E(X) = \sum_{k=0}^{n-1} 2^{2n-k} \cdot \frac{D_k}{2^{3n}},$$

where $D_k = \#\{w_{n-1} \ldots w_0 \mid \Pr[w_{n-1} \ldots w_0] = 2^{-k}\} = 4 \times 6^k \binom{n-1}{k}$.

6. Conclusions and Further Work

In this paper, by studying the probability of difference analysis based on two modulo addition equations and correlation probability calculation in cryptography, the mathematical expectation of the number of probability solutions in equation system (1) is obtained.

Firstly, by combing the characteristics of modulo addition operation, the recursive expression of carry is derived, and the recursive expression is expressed by bits. Through the transformation of two equations and the carry recurrence formula, the preliminary condition that the probability of zero is obtained. By using the conditional probability formula and the uniform distribution of binary variables, we find the specific probability values of the next difference under different values. By using method of Markov chain, probability is transformed into matrix product, and all possible matrices are obtained. Further, the matrix under different methods is calculated, and through the calculation results of the matrix in the probability, the specific values and conditions of the original probability are obtained, and then mathematical expectation is calculated.

By analyzing the characteristics of modular addition operation and probability distribution, we find the detailed derivation process and conclusion, which provide useful theoretical support for differential analysis in block cipher cracking. In this paper, we only study the mathematical expectation of the number of solutions in the case of two equations. In the subsequent work, we will continue to study the probability and correlation probability of the solution of the equation system when there are multiple difference equations. It is believed that the research method and the research model established in this paper can be further extended to the study of multiple difference equations, and provided a reference for the number of solutions of difference equations and related probability problems.

References

[1] Zichen Li. Cryptography - Basic theory and application (in Chinese).Publishing House of Electronics Industry, 2019.
[2] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.
[3] Wai-Ki Ching, Ximin Huang, Michael K.Ng, Tak-Kuen Siu. Markov chains: Models, algorithms, and applications.Beijing: Tsinghua University Press,2015.
[4] Zhenming Yang. Probability theory (in Chinese). Science Press, 2021.