The Study of Modulo 2^n

A General Method To Calculate The Probability Or Correlation Coefficients For The Any Property Of Modulo 2^n

Zhongfeng Niu

Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
niuzhongfeng@iie.ac.cn

Abstract. In this paper, we present a new concept named the basic function. By the study of the basic function, we find the $O(n)$-time algorithm to calculate the probability or correlation for some property of Modulo 2^n, including the difference-linear connective correlation coefficients, the linear approximation correlation coefficients, the differential probability, difference-boomerange connective probability, boomerange connective probability, boomerange-difference connective probability, etc.

Keywords: Modulo addition 2^n · basic function · difference-linear connective correlation coefficients · linear approximation correlation coefficients · difference-boomerange connective probability · boomerange connective probability · differential probability · boomerange-difference connective probability

Contents

Introduction

Since the differential analysis and the linear analysis were proposed, statistical analysis have become one of the research hotspots in the cryptanalysis of block cypher in the last 30 years. The most statistical analysis for block cypher is based on the statistical properties of nonlinear functions, namely, the probability of $\bigoplus_{z=1}^{n_j} f_j(x)_z = A_j \ 1 \le j \le m$ or the correlation coefficients of $\lambda \cdot (\bigoplus_{i=1}^{n} f(x)_i)$, where $f(x)_z,\ 1 \le j \le m,\ 1 \le z \le n_j$; $f_j(x)_i,\ 1 \le i \le n$ are composite operation of $\oplus$, the nonlinear function and its inverse. In most of block cypher, the construction of the nonlinear functions is based on the S-box that it can be regard as the nonlinear function with small scale, especially the SPN structure and the Festial structure, the calculation of the statistical properties of nonlinear functions can be completed by the calculating the statistical properties of S-box. Due to the S-box with tiny scale, the statistical properties of S-box can be got in a short time by trying all possible value. Thus, it almost has no problem to do the statistical analysis for the SPN structure and the Festial structure, such as differential analysis, linear analysis, boomrange analysis, differential-linear analysis, etc. However, because of the modular addition 2^n with large-scale adopted as the nonlinear functions in ARX structure, it is infeasible for the ARX structure to get the statistical properties of nonlinear functions by trying all possible value. Thus, compared with the SPN structure and the Festial structure, the most statistical analysis method used for ARX structure, especially the new method or improvement method proposed in the last decade, have made slow progress due to the above reason.

In order to overcome the above problem, we have to look for polynomial time algorithms to calculate the statistical properties of modular addition 2^n. In 2001, Lipmaa.etc and Johan Wallén have proposed the polynomial time algorithms to calculate the linear approximation correlation coefficients and the differential probability respectively, which is been about 10 years since the differential attack and the linear analysis were proposed. And in 2013, Schulte-Geers showed that mod 2^n is CCZ-equivalent to a quadratic vectorial Boolean function. Based on it, he proposed the explicit formula to calculate the linear approximation correlation coefficients and the differential probability, of which time complex is polynomial. Since then, the CCZ-equivalent of mod 2^n have be acknowledged as the most powerful method to look for the polynomial time algorithms to calculate the statistical properties of modular addition 2^n. In addition, a series of new statistical properties, including the difference-linear connective correlation coefficients, difference-boomerange connective probability, boomerange connective probability and boomerange-difference connective probability, etc, were proposed in order to improve the previous methods. And those methods have better performance in the SPN cipher and the Festial cipher. Unfortunately, according to the study of difference-linear connective correlation coefficients for nonlinear function, for any two permutations in the same CCZ-equivalent class, their difference-linear connective correlation coefficients are not in general invariant. Thus, the CCZ-equivalent can't be regard as the general method to look for polynomial time algorithms to calculate the statistical properties of modular addition 2^n. The following questions may be asked naturally.

1.How to find the polynomial time algorithms to calculate such statistical properties ?

2.Does there exits a general method applying to all of the current statistical properties of modular addition 2^n for finding the explicit formula?

Our contribution

Firstly, this paper can give the $O(n)$-time algorithm to calculate the probability or correlation for some property of Modulo 2^n, including the difference-linear connective correlation coefficients(DLCT), the linear approximation correlation coefficients(LAT), the differential probability(DDT), difference-boomerange connective probability(DBT), boomerange connective probability(BCT), boomerange-difference connective probability(BDT), etc.

Secondly, for all of the current statistical analysis method in block cipher, such as difference-linear connective correlation coefficients(DLCT), the linear approximation correlation coefficients(LAT), the differential probability(DDT), difference-boomerange connective probability(DBT), boomerange connective probability(BCT), boomerange-difference connective probability(BDT), etc, it can be summarized as the probability of $\bigoplus_{z=1}^{n_j} f_j(x)_z = A_j \ 1 \leq j \leq m$ or the correlation coefficients of $\lambda \cdot (\bigoplus_{i=1}^{n} f(x)_i)$, where $f(x)_z \ 1 \leq j \leq m, \ 1 \leq z \leq n_j; \ f_j(x)_i \ 1 \leq i \leq n$ are composite operation of $\oplus$, the nonlinear function and its inverse. Based the above fact, we proposed the concept of the basic function, which is a composite operation of $\oplus$ and $\boxplus$. Then, based on the regular of the basic function, we construct the Aa-set and Df-set. By the property of the Aa-set and Df-set, we can answer the question 2. The general method has been found, which is fit for all of current statistical properties of modular addition 2^n. As a result, the form of formula for all of current statistical properties of modular addition 2^n are similar with the Johan Wallén's.

1 Preliminaries

In this section, we will introduce some basic knowledge that we will use in the following.

Definition 1(Addition modulo 2^n): For $x, y \in F_2^n$, define $y \boxplus x = x \oplus y \oplus carry(x, y)$, where $carry(x, y) = [c_{n-1}, \cdots, c_0]$. The i-th bit c_i is defined as

$$c_0 = 0$$
$$c_{i+1} = (x_i \wedge y_i) \oplus (x_i \wedge c_i) \oplus (y_i \wedge c_i), 0 \le i \le n-1$$

Definition 2: Let $x, y \in F_2^n$,$e \in F_2$, define $y \boxplus x \boxplus e = y \boxplus x \boxplus (0, \cdots 0, e)$.

Let $carry_e^*(x, y) = [c_{n-1}^*, \cdots, c_0^*]$, if we define i-th bit c_i^* as

$$c_0^* = e$$
$$c_{i+1}^* = (x_i \wedge y_i) \oplus (x_i \wedge c_i^*) \oplus (y_i \wedge c_i^*), 0 \le i \le t-1$$

And the purpose of defining $carry_e^*(x, y)$ is to make $y \boxplus x \boxplus e$ have the same form as $y \boxplus x$:

Theorems 1: For $x, y \in F_2^n$,$e \in F_2$, define $y \boxplus x \boxplus e = x \oplus y \oplus carry_e^*(x, y)$.

Proof. If $e = 0$, then the theorem holds.
If $e = 1$, let $c_i = carry(x, y)[i]$, $c_i^1 = carry(x \boxplus y, (0, \cdots 0, e))[i]$, for $0 \le i \le n$; then

$$c_0^1 = 0$$
$$c_1^1 = x_0 \oplus y_0$$
$$c_{i+1}^1 = (x_i \oplus y_i \oplus c_i) \wedge c_i^1, 2 \le i \le n-1$$

Obviously, $c_0^1 \wedge c_0 = 0$, $c_1^1 \wedge c_1 = x_0 \wedge y_0 \wedge (x_0 \oplus y_0) = (x_0 \wedge y_0) \oplus (x_0 \wedge y_0) = 0$
Next, we will proof $c_i^1 \wedge c_i = 0$, $0 \le i \le n-1$ by introduction. Supposed that $c_i^1 \wedge c_i = 0$ for $1 \le i \le k$. Then, for $c_{k+1}^1 \wedge c_{k+1}$, we have

$$\begin{aligned}
&c_{k+1}^1 \wedge c_{k+1} \\
&= ((x_k \oplus y_k \oplus c_k) \wedge c_k^1) \wedge ((x_k \wedge y_k) \oplus (x_k \wedge c_k) \oplus (y_k \wedge c_k)) \\
&= ((x_k \oplus y_k) \wedge c_k^1) \wedge ((x_k \wedge y_k) \oplus ((x_k \oplus y_k) \wedge c_k)) \\
&= ((x_k \oplus y_k) \wedge (x_k \wedge y_k)) \wedge c_k^1 \\
&= ((x_k \wedge y_k) \oplus (x_k \wedge y_k)) \wedge c_k^1 = 0
\end{aligned}$$

Thus, for $2 \le i \le n-1$, we have $c_{i+1}^1 = (x_i \oplus y_i \oplus c_i) \wedge c_i^1 = (x_i \oplus y_i) \wedge c_i^1$, and

$$\begin{aligned}
&c_0^* = c_0 \oplus c_0^1 \oplus 1 = 1 \\
&c_1^* = c_1 \oplus c_1^1 \\
&c_{i+1}^* = c_{i+1}^1 \oplus c_{i+1} \\
&= (x_i \wedge y_i) \oplus \big(x_i \wedge (c_i^1 \oplus c_i)\big) \oplus \big(y_i \wedge (c_i^1 \oplus c_i)\big), 2 \le i \le n-1
\end{aligned}$$

Notice that $carry_e^*(x,y) = carry(x,y) \oplus carry(x \boxplus y, (0,\cdots 0,e)) \oplus (0,\cdots 0,e)$.
Thus, $y \boxplus x \boxplus (0,\cdots 0,e) = x \oplus y \oplus carry_e^*(x,y)$. □

From the definition of $\boxplus$, we can see that the subtraction modulo 2^n ($\boxminus$) can be converted into the addition modulo 2^n ($\boxplus$):

Theorems 2: $y \boxminus x = (x \oplus (1,\cdots 1)) \boxplus y \boxplus 1$.

Proof. Notice that $(1,\cdots 1) = -1 \ mod\ 2^n$ and $carry(x \oplus (1,\cdots 1), x) = 0$, then
$(x \oplus (1,\cdots 1)) \boxplus x = (1,\cdots 1) = -1 \ mod\ 2^n$, which is equal to
$(x \oplus (1,\cdots 1)) \boxplus 1 = -x \ mod\ 2^n$.
Thus, $y \boxminus x = y - x \ mod\ 2^n = (x \oplus (1,\cdots 1)) \boxplus y \boxplus 1$. □

Combing with the **Theorems 3**, the $y \boxminus x$ have the same form as $y \boxplus x$:

Corollary 1: $y \boxminus x = (x \oplus (1,\cdots 1)) \oplus y \oplus carry_1^*(x \oplus (1,\cdots 1), y)$.

2 The Basic Function

2.1 The motivation and property

In the cryptanalysis of block cypher, the scholar proposed many attack method based on some statistics property of the nonlinear function in the cipher, such as difference-linear connective correlation coefficients(DLCT), the linear approximation correlation coefficients(LAT), the differential probability(DDT), difference-boomerange connective probability(DBT), boomerange connective probability(BCT), boomerange-difference connective probability(BDT), etc. In a word, these statistics properties can be summarized as the probability of $\bigoplus_{z=1}^{n_j} f_j(x)_z = A_j \ 1 \le j \le m$ or the correlation coefficients of $\lambda \cdot (\bigoplus_{i=1}^{n} f(x)_i)$. For $1 \le i \le n,\ 1 \le j \le m,\ 1 \le z \le n_j,\ f(x)_z, f_j(x)_i$ is composite operation of $\oplus$, the nonlinear function and its inverse. In the ARX structure, the sole nonlinear function is the $\boxplus$ and its inverse can be converted into the composite operation of $\oplus$ and $\boxplus$. Thus, we can define the basic function as composite operation of $\oplus$ and $\boxplus$:

Definition 3(The Basic function): Supposed that $x, y \in F_2^n$, $E_k = (e_0, e_1, \cdots e_{k-1}) \in F_2^{k-1}$, $\alpha_0, \alpha_1, \cdots \alpha_{k-1} \in F_2^n$, $\beta_0, \beta_1, \cdots \beta_{k-1} \in F_2^n$. Let $A_k = (\alpha_0, \alpha_2, \cdots \alpha_{k-1})$, $B_k = (\beta_0, \beta_2, \cdots \beta_{k-1})$, $\alpha_0 = \beta_0 = 0$, where the element of A_k, B_k is n-dimension vector. Then the $f(x,y)_{E_k,A_k,B_k}$ is called basic function with k order, if $f(x,y)_{E_k,A_k,B_k}$ satisfies the follow the form:

$$
\begin{aligned}
&(x_0, y_0) = (x, y)\\
&(x_{i+1}, y_{i+1}) = (x_i \oplus \alpha_i, (x_i \oplus \alpha_i) \boxplus (y_i \oplus \beta_i) \boxplus e_i), 0 \le i \le k-1\\
&f(x,y)_{E_k,A_k,B_k} = (x_k, y_k).
\end{aligned}
$$

For $0 \le i \le k-1$, $(x_i \oplus \alpha_i, (x_i \oplus \alpha_i) \boxplus (y_i \oplus \beta_i) \boxplus e_i)$ is called the $(i+1)$-th round function, and $carry_{e_i}^*(x_i \oplus \alpha_i, y_i \oplus \beta_i)$ is called the carry function of $(i+1)$-th round function in $f(x,y)_{E_k,A_k,B_k}$.

According to the **definition 3:**, we can see the relation between the $f(x,y)_{E_{k-1},A_{k-1},B_{k-1}}$ and the $f(x,y)_{E_k,A_k,B_k}$:

Remark 3: According to the definition of $f(x,y)_{E_k,A_k,B_k}$, the $f(x,y)_{E_k,A_k,B_k}$ can be written as:

$$
\begin{aligned}
&(x_{k-1}, y_{k-1}) = f(x,y)_{E_{k-1},A_{k-1},B_{k-1}} \\
&(x_k, y_k) = (x_{k-1} \oplus \alpha_{k-1}, (x_{k-1} \oplus \alpha_{k-1}) \boxplus (y_{k-1} \oplus \beta_{k-1}) \boxplus e_{k-1}) \\
&f(x,y)_{E_k,A_k,B_k} = (x_k, y_k)
\end{aligned}
$$

where $E_{k-1} = E_k[0 : k-2], A_{k-1} = A_k[0 : k-2], B_{k-1} = B_k[0 : k-2]$.

Definition 4: For $x = X^2||X^1 \in F_2^n$, where $X^2 \in F_2^q, X^1 \in F_2^p$, $p+q = n$. Define $x = X^2||X^1 = X^2 \cdot 2^p + X^1$.

Then, according to the definition of Addition modulo 2^n, we can see that the basic function can be divided into two basic function:
Theorem 3: For $i > 0$ and any positive integer t, supposed that $X^{1,i+1}, Y^{1,i+1}, \alpha_0^{1,i+1}, \alpha_1^{1,i+1}, \cdots, \alpha_{k-1}^{1,i+1}, \beta_0^{1,i+1}, \beta_1^{1,i+1}, \cdots \beta_{k-1}^{1,i+1} \in F_2^{(i+1)\cdot t}$; $E_k = (e_0, e_1, \cdots e_{k-1}) \in F_2^{k-1}$. Let $Y^{1,i} = Y^{1,i+1}[i \cdot t - 1 : 0]$, $Y^{2,i} = Y^{1,i+1}[(i+1)\cdot t - 1 : i \cdot t]$, $X^{1,i} = X^{1,i+1}[i \cdot t - 1 : 0]$, $X^{2,i} = X^{1,i+1}[(i+1)\cdot t - 1 : i \cdot t]$, then the k order basic function $f(X^{1,i+1}, Y^{1,i+1})_{E_k,A_k^{i+1},B_k^{i+1}}$ can be written as

$$
f(X^{1,i+1}, Y^{1,i+1})_{E_k,A_k^{i+1},B_k^{i+1}} = f(X^{2,i}, Y^{2,i})_{M_k^i,C_k^i,D_k^i} \cdot 2^{i\cdot t} + f(X^{1,i}, Y^{1,i})_{E_k,A_k^i,B_k^i}
$$

where

$$
\begin{aligned}
\alpha_m^{2,i} &= \alpha_m^{1,i+1}[(i+1)\cdot t - 1 : i \cdot t], 0 \le m \le k-1 \\
\beta_m^{2,i} &= \beta_m^{1,i+1}[(i+1)\cdot t - 1 : i \cdot t], 0 \le m \le k-1 \\
\alpha_m^{1,i} &= \alpha_m^{1,i+1}[i \cdot t - 1 : 0], 0 \le m \le k-1 \\
\beta_m^{1,i} &= \beta_m^{1,i+1}[i \cdot t - 1 : 0], 0 \le m \le k-1 \\
c_m^i &= carry^*_{e_m}(X_m^{1,i} \oplus \alpha_m^{1,i}, Y_m^{1,i} \oplus \beta_m^{1,i})[i \cdot t], 0 \le m \le k-1 \\
s_m^i &= carry^*_{c_m^i}(X_m^{2,i} \oplus \alpha_m^{2,i}, Y_m^{2,i} \oplus \beta_m^{2,i})[t], 0 \le m \le k-1 \\
A_k^i &= [\alpha_0^{1,i}, \alpha_1^{1,i}, \cdots \alpha_{k-1}^{1,i}] \\
B_k^i &= [\beta_0^{1,i}, \beta_1^{1,i}, \cdots \beta_{k-1}^{1,i}] \\
C_k^i &= [\alpha_0^{2,i}, \alpha_1^{2,i}, \cdots \alpha_{k-1}^{2,i}] \\
D_k^i &= [\beta_0^{2,i}, \beta_1^{2,i}, \cdots \beta_{k-1}^{2,i}] \\
M_k^i &= [c_0^i, c_1^i, \cdots c_{k-1}^i] \\
S_k^i &= [s_0^i, s_1^i, \cdots s_{k-1}^i]
\end{aligned}
$$

Proof. Notice that when order $k = 1$, according to the definition 2, $(X^{1,i+1} \oplus \alpha_0^{1,i+1}) \boxplus (Y^{1,i+1} \oplus \beta_0^{1,i+1}) \boxplus e_0$ can be written as

$$
\begin{aligned}
&(X^{1,i+1} \oplus \alpha_0^{1,i+1}) \boxplus (Y^{1,i+1} \oplus \beta_0^{1,i+1}) \boxplus e_0 \\
=&((X^{1,i} \oplus \alpha_0^{1,i}) \boxplus (Y^{1,i} \oplus \beta_0^{1,i}) \boxplus c_0^i\ )2^{i\cdot t} + (X^{2,i} \oplus \alpha_0^{2,i}) \boxplus (Y^{2,i} \oplus \beta_0^{2,i}) \boxplus e_0
\end{aligned}
$$

Thus, when order $k = 1$, the theorem holds.
Supposed that when order $m \le k$, the theorem holds.
When order $m = k+1$, according to the definition of $carry^*_e(x,y)$, the value of the $i \cdot t - th$ bit of $carry^*_{e_k}(X_k^{1,i+1} \oplus \alpha_k^{1,i+1}, Y_k^{1,i+1} \oplus \beta_k^{1,i+1})[i \cdot t]$ is only rely on the first $i \cdot t - 1$ bits of

$X_k^{1,i+1} \oplus \alpha_k^{1,i+1}$ and $Y_k^{1,i+1} \oplus \beta_k^{1,i+1}$, namely,

$$\begin{aligned} &carry^*_{e_k}(X_k^{1,i+1} \oplus \alpha_k^{1,i+1}, Y_k^{1,i+1} \oplus \beta_k^{1,i+1}) \\ &= carry^*_{e_k}(X_k^{1,i} \oplus \alpha_k^{1,i}, Y_k^{1,i} \oplus \beta_k^{1,i}) \\ &= c_k^i \end{aligned}$$

Thus,

$$\begin{aligned} &f(X^{1,i+1}, Y^{1,i+1})_{E_{k+1}, A_{k+1}^{i+1}, B_{k+1}^{i+1}} \\ &= (X_k^{1,i+1} \oplus \alpha_k^{1,i+1}) \boxplus (Y_k^{1,i+1} \oplus \beta_k^{1,i+1}) \boxplus e_k \\ &= ((X_k^{2,i} \oplus \alpha_k^{2,i}) \boxplus (Y_k^{2,i} \oplus \beta_k^{2,i}) \boxplus c_k^i\ )2^{i \cdot t} + (X_k^{1,i} \oplus \alpha_k^{1,i}) \boxplus (Y_k^{1,i} \oplus \beta_k^{1,i}) \boxplus e_k \end{aligned}$$

On the other hand,

$$\begin{aligned} &(X_k^{1,i+1}, X_k^{1,i+1}) = (X_k^{2,i}, X_k^{2,i}) \cdot 2^{i \cdot t} + (X_k^{1,i}, X_k^{1,i}) \\ &= f(X^{2,i}, Y^{2,i})_{M_k^i, C_k^i, D_k^i} + f(X^{1,i}, Y^{1,i})_{E_k, A_k^i, B_k^i} \end{aligned}$$

Thus,

$$\begin{aligned} &f(X^{1,i+1}, Y^{1,i+1})_{E_{k+1}, A_{k+1}^{i+1}, B_{k+1}^{i+1}} = (X_k^{1,i+1} \oplus \alpha_k^{1,i+1}) \boxplus (Y_k^{1,i+1} \oplus \beta_k^{1,i+1}) \boxplus e_k \\ &= ((X_k^{2,i} \oplus \alpha_k^{2,i}) \boxplus (Y_k^{2,i} \oplus \beta_k^{2,i}) \boxplus c_k^i\ ) \cdot 2^{i \cdot t} + (X_k^{1,i} \oplus \alpha_k^{1,i}) \boxplus (Y_k^{1,i} \oplus \beta_k^{1,i}) \boxplus e_k \\ &= f(X^{2,i}, Y^{2,i})_{M_{k+1}^i, C_{k+1}^i, D_{k+1}^i} \cdot 2^{i \cdot t} + f(X^{1,i}, Y^{1,i})_{E_{k+1}, A_{k+1}^i, B_{k+1}^i} \end{aligned}$$

When $m = k + 1$, the theorem holds. □

Remark 4: Meanwhile for $i > 0$, $k > 0$, according to the definition of $carry^*_e(x, y)$ and Theorems 1, we have: $S_k^i = M_k^{i+1}$.

Remark 5: Obviously, for any $E_k, A_k^{i+1}, B_k^{i+1}$, where $i > 0$, $k > 0$, when $X^{1,i+1}, Y^{1,i+1}$are given, then $M_k^{i+1}$are uniquely identified.

Definition 5: For $X, Y \in F_2^n$, given $\{f(X,Y)_{E_{k_{m,j}}, A_{k_{m,j}}^{i+1}, B_{k_{m,j}}^{i+1}};\ 1 \le m \le r_j\}_j$ as a basic function set with code number j, which contains r_j basic functions, where $k_{1,j} \le \cdots \le k_{r_j,j}$. If $E_{k_{m,j}} = E_{k_{m+1,j}}[0 : k_{m,j}]$, $A_{k_{m,j}}^{i+1} = A_{k_{m+1,j}}^{i+1}[0 : k_{m,j}]$, $B_{k_{m,j}}^{i+1} = B_{k_{m+1,j}}^{i+1}[0 : k_{m,j}]$ holds for $f(X,Y)_{E_{k_{m,j}}, A_{k_{m,j}}^{i+1}, B_{k_{m,j}}^{i+1}}$, where $1 \le m \le r_j - 1$. Then, we called the $\{f(X,Y)_{E_{k_{m,j}}, A_{k_{m,j}}^{i+1}, B_{k_{m,j}}^{i+1}};\ 1 \le m \le r_j\}_j$ is basic function series with code number j. In addition, $k_{r_j,j}$ is called the depth of the basic function series $\{f(X,Y)_{E_{k_{m,j}}, A_{k_{m,j}}^{i+1}, B_{k_{m,j}}^{i+1}};\ 1 \le m \le r_j\}_j$.

Besides this, for convenience to express the combination of the basic function in $\bigoplus$, for $a \in F_2$, we define the operation $*$ as

$$\begin{aligned} &a * f(x,y)_{E_k, A_k, B_k} = 0,\ when\ a = 0 \\ &a * f(x,y)_{E_k, A_k, B_k} = f(x,y)_{E_k, A_k, B_k},\ when\ a = 1 \\ &a * x = 0,\ a * y = 0,\ when\ a = 0 \\ &a * x = x,\ a * y = y,\ when\ a = 1 \end{aligned}$$

2.2 Notion Description About The Basic Function Series

In order to reduce the redundancy of the article, we will introduce some notion description about the basic function series $\{f(X^{1,i}, Y^{1,i})_{E_{k_{m,j}}, A_{k_{m,j}}^i, B_{k_{m,j}}^i}; 1 \le m \le r_j\}_j$, which we

will frequently adopt in the following proof.
For any positive integer q, t, n, supposed that $X, Y \in F_2^{q\cdot t}$, $C = (J, N) \in (F_2^{n\times q\cdot t}, F_2^{n\times q\cdot t})$, $\gamma, \lambda, v, w \in F_2^{q\cdot t}$, $\alpha^{1,q}_{0,k_{r_j,j}}, \alpha^{1,q}_{1,k_{r_j,j}}, \cdots, \alpha^{1,q}_{k_{r_j,j}-1,k_{r_j,j}}$, $\beta^{1,q}_{0,k_{r_j,j}}, \beta^{1,q}_{1,k_{r_j,j}}, \cdots, \beta^{1,q}_{k_{r_j,j}-1,k_{r_j,j}} \in F_2^{q\cdot t}$, $E_{k_{r_j,j}} = (e_{0,k_{r_j,j}}, e_{1,k_{r_j,j}}, \cdots e_{k_{r_j,j}-1,k_{r_j,j}}) \in F_2^{k_{r_j,j}}$. Let

$$\begin{aligned}
&X^{1,q} = X\\
&Y^{1,q} = Y\\
&A^q_{k_{r_j,j}} = [\alpha^{1,q}_{0,k_{r_j,j}}, \alpha^{1,q}_{1,k_{r_j,j}}, \cdots \alpha^{1,q}_{k_{r_j,j}-1,k_{r_j,j}}],\\
&B^q_{k_{r_j,j}} = [\beta^{1,q}_{0,k_{r_j,j}}, \beta^{1,q}_{1,k_{r_j,j}}, \cdots \beta^{1,q}_{k_{r_j,j}-1,k_{r_j,j}}];\\
&C = (J, N) = C^1_q = (J^1_q, N^1_q),\ \lambda^1_q = \lambda, \gamma^1_q = \gamma, V^1_q = v, w^1_q = w.
\end{aligned}$$

Then, define the basic function series with code number j as $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A^q_{k_{m,j}}, B^q_{k_{m,j}}};\ 1 \le m \le r_j - 1\}_j$. Due to the property of the basic function series, the follow relation holds.

$$\begin{aligned}
E_{k_{m,j}} &= E_{k_{r_j,j}}[0 : k_{m,j}], 1 \le m \le r_j\\
A^{i+1}_{k_{m,j}} &= A^{i+1}_{k_{r_j,j}}[0 : k_{m,j}], 1 \le m \le r_j\\
B^{i+1}_{k_{m,j}} &= B^{i+1}_{k_{r_j,j}}[0 : k_{m,j}], 1 \le m \le r_j
\end{aligned}$$

Then, for any basic function series $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A^q_{k_{m,j}}, B^q_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, define:

$$\begin{aligned}
&Y^{1,i} = Y^{1,i+1}[i\cdot t - 1 : 0] = Y^{1,q}[i\cdot t - 1 : 0]\\
&Y^{2,i} = Y^{1,i+1}[(i+1)\cdot t - 1 : i\cdot t] = Y^{1,q}[(i+1)\cdot t - 1 : i\cdot t]\\
&X^{1,i} = X^{1,i+1}[i\cdot t - 1 : 0] = X^{1,q}[i\cdot t - 1 : 0]\\
&X^{2,i} = X^{1,i+1}[(i+1)\cdot t - 1 : i\cdot t] = X^{1,q}[(i+1)\cdot t - 1 : i\cdot t]\\
&\alpha^{2,i}_{z,k_{m,j}} = \alpha^{1,i+1}_{z,k_{m,j}}[(i+1)\cdot t - 1 : i\cdot t] = \alpha^{1,q}_{z,k_{r_j,j}}[(i+1)\cdot t - 1 : i\cdot t], 0 \le z \le k_{r_j,j} - 1,\ 1 \le m \le r_j\\
&\beta^{2,i}_{z,k_{m,j}} = \beta^{1,i+1}_{z,k_{m,j}}[(i+1)\cdot t - 1 : i\cdot t] = \beta^{1,q}_{z,k_{r_j,j}}[(i+1)\cdot t - 1 : i\cdot t], 0 \le z \le k_{r_j,j} - 1,\ 1 \le m \le r_j\\
&\alpha^{1,i}_{z,k_{m,j}} = \alpha^{1,i+1}_{z,k_{m,j}}[i\cdot t - 1 : 0] = \alpha^{1,q}_{z,k_{r_j,j}}[i\cdot t - 1 : 0], 0 \le z \le k_{r_j,j} - 1,\ 1 \le m \le r_j\\
&\beta^{1,i}_{z,k_{m,j}} = \beta^{1,i+1}_{z,k_{m,j}}[i\cdot t - 1 : 0] = \beta^{1,q}_{z,k_{r_j,j}}[i\cdot t - 1 : 0], 0 \le z \le k_{r_j,j} - 1,\ 1 \le m \le r_j
\end{aligned}$$

where, $1 \le i \le q - 1$.
Obviously, for $1 < i \le q - 1$, $0 \le z \le k_{m,j} - 1$, $1 \le m \le r_j$, let

$$\begin{aligned}
\alpha^{1,i+1}_{z,k_{m,j}} &= [\alpha^{2,i}_{z,k_{r_j,j}}, \alpha^{2,i-1}_{z,k_{r_j,j}} \cdots, \alpha^{2,1}_{z,k_{r_j,j}} \alpha^{1,1}_{z,k_{r_j,j}}]\\
\beta^{1,i+1}_{z,k_{m,j}} &= [\beta^{2,i}_{z,k_{r_j,j}}, \beta^{2,i-1}_{z,k_{r_j,j}} \cdots, \beta^{2,1}_{z,k_{r_j,j}} \beta^{1,1}_{z,k_{r_j,j}}]\\
X^{1,i+1} &= [X^{2,i}, X^{2,i-1} \cdots, X^{2,1} X^{1,1}]\\
Y^{1,i+1} &= [Y^{2,i}, Y^{2,i-1} \cdots, Y^{2,1}, Y^{1,1}]
\end{aligned}$$

Beside this, for $1 \le i \le q$, $1 \le m \le r_j$ define

$$\begin{aligned}
&(X^{1,i}_0, y^{1,i}_0) = (X^{1,i}, Y^{1,i})\\
&(X^{1,i}_{z+1}, Y^{1,i}_{z+1}) = (X^{1,i}_z \oplus \alpha^{1,i}_{z,k_{r_j,j}}, (X^{1,i}_z \oplus \alpha^{1,i}_{z,k_{r_j,j}}) \boxplus (Y^{1,i}_z \oplus \beta^{1,i}_{z,k_{r_j,j}}) \boxplus e_{z,k_{r_j,j}}),\ 0 \le z \le k_{m,j} - 1
\end{aligned}$$

and for $1 \le i \le q$, let

$$A^i_{k_{m,j}} = [\alpha^{1,i}_{0,k_{r_j,j}}, \alpha^{1,i}_{1,k_{r_j,j}}, \cdots \alpha^{1,i}_{k_{m,j}-1,k_{r_j,j}}], 1 \le m \le r_j$$
$$B^i_{k_{m,j}} = [\beta^{1,i}_{0,k_{r_j,j}}, \beta^{1,i}_{1,k_{r_j,j}}, \cdots \beta^{1,i}_{k_{m,j}-1,k_{r_j,j}}], 1 \le m \le r_j$$

then we have $(X^{1,i}_{k_{m,j}}, Y^{1,i}_{k_{m,j}}) = f(X^{1,i}, Y^{1,i})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}}$ $1 \le m \le r_j$

From the above, we get a series of basic function series from $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A^q_{k_{m,j}}, B^q_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, namely $\{f(X^{1,i}, Y^{1,i})_{E_{k_{m,j}}, A^i_{k_{m,j}}, B^i_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, $1 \le i \le q$.

Secondly, let $M^i_{k_{m,j}}[z]$ denote the $i{\cdot}t$-th value of the carry function of $f(X^{1,i}, Y^{1,i})_{E_{k_{z,j}}, A^i_{k_{m,j}}, B^i_{k_{m,j}}}$ in round $z+1$, where $1 \le i \le q$, $0 \le z \le k_{m,j} - 1$, $1 \le m \le r_j$.

Property 2: Due to for any positive integer q, t, $1 \le i \le q$, when $E_{k_{r_j,j}}, A^i_{k_{r_j,j}}, B^i_{k_{r_j,j}}$, $X^{1,i}, X^{1,i}$ are given, then $M^i_{k_{m,j}}$ are uniquely identified, where $1 \le m \le r_j - 1$. Thus, for $\{f(X^{1,i}, Y^{1,i})_{E_{k_{m,j}}, A^i_{k_{m,j}}, B^i_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, satisfied $M^i_{k_{m,j}} = M^i_{k_{r_j,j}}[0 : k_{m,j}]$, $1 \le m \le r_j$.

Thus ,we can define

$$c^i_{z,k_{m,j}} = carry^*_{e_{z,k_{r_j,j}}}(X^{1,i}_z \oplus \alpha^{1,i}_{z,k_{r_j,j}}, Y^{1,i}_z \oplus \beta^{1,i}_{z,k_{r_j,j}})[i \cdot t],\ 0 \le z \le k_{m,j} - 1,\ 1 \le m \le r_j$$
$$M^i_{k_{m,j}} = [c^i_{0,k_{r_j,j}}, c^i_{1,k_{r_j,j}}, \cdots c^i_{k_{m,j}-1,k_{r_j,j}}],\ 1 \le m \le r_j$$

where $1 \le i \le q$.

$$s^i_{z,k_{m,j}} = carry^*_{c^i_{z,k_{r_j,j}}}(X^{2,i}_z \oplus \alpha^{2,i}_{z,k_{r_j,j}}, Y^{2,i}_z \oplus \beta^{2,i}_{z,k_{r_j,j}})[t],\ 0 \le z \le k_{m,j} - 1,\ 1 \le m \le r_j$$
$$S^i_{k_{m,j}} = [s^i_{0,k_{r_j,j}}, s^i_{1,k_{r_j,j}}, \cdots s^i_{k_{m,j}-1,k_{r_j,j}}],\ 1 \le m \le r_j.$$

where $1 \le i \le q - 1$.
According to the **Remark 4:**, we have

Remark 6: $M^{i+1}_{k_{m,j}} = S^i_{k_{m,j}}$, for $1 \le m \le r_j$, $1 \le i \le q - 1$.

For convenience to the follow following discussion, for $1 \le i \le q - 1$, let

$$T^0_{k_{m,j}} = A^1_{k_{m,j}}, 1 \le m \le r_j - 1$$
$$D^0_{k_{m,j}} = B^1_{k_{m,j}}, 1 \le m \le r_j - 1$$
$$T^i_{k_{m,j}} = [\alpha^{2,i}_{0,k_{r_j,j}}, \alpha^{2,i}_{1,k_{r_j,j}}, \cdots \alpha^{2,i}_{k_{m,j}-1,k_{r_j,j}}], 1 \le m \le r_j$$
$$D^i_{k_{m,j}} = [\beta^{r_j,i}_{0,k_{z,j}}, \beta^{r_j,i}_{1,k_{z,j}}, \cdots \beta^{2,i}_{k_{m,j}-1,k_{r_j,j}}], 1 \le m \le r_j$$

$J_i^1[s] = J_{i+1}^1[s, 0 : i \cdot t - 1] = J_q^1[s, 0 : i \cdot t - 1],\ 1 \le s \le n.$
$J_i^2[s] = J_{i+1}^1[s, (i+1) \cdot t - 1 : i \cdot t] = J_q^1[s, (i+1) \cdot t - 1 : i \cdot t],\ 1 \le s \le n.$
$N_i^1[s] = N_{i+1}^1[s, 0 : i \cdot t - 1] = N_q^1[s, 0 : i \cdot t - 1],\ 1 \le s \le n.$
$N_i^2[s] = N_{i+1}^1[s, (i+1) \cdot t - 1 : i \cdot t] = N_q^1[s, (i+1) \cdot t - 1 : i \cdot t],\ 1 \le s \le n.$
$C_i^1[s] = (J_i^1[s], N_i^1[s]),\ 1 \le s \le n.$
$C_i^2[s] = (J_i^2[s], N_i^2[s]),\ 1 \le s \le n.$
$C_0^2[s] = (J_1^1[s], N_1^2[s]),\ 1 \le s \le n.$
$\lambda_i^1 = \lambda_{i+1}^1[0 : i \cdot t - 1] = \lambda_q^1[0 : i \cdot t - 1],$
$\lambda_i^2 = \lambda_{i+1}^1[(i+1) \cdot t - 1 : i \cdot t] = \lambda_q^1[(i+1) \cdot t - 1 : i \cdot t],$
$\gamma_i^1 = \gamma_{i+1}^1[0 : i \cdot t - 1] = \gamma_q^1[0 : i \cdot t - 1],$
$\gamma_i^2 = \gamma_{i+1}^1[(i+1) \cdot t - 1 : i \cdot t] = \gamma_q^1[(i+1) \cdot t - 1 : i \cdot t],$
$V_i^1 = V_{i+1}^1[0 : i \cdot t - 1] = V_q^1[0 : i \cdot t - 1],$
$V_i^2 = V_{i+1}^1[(i+1) \cdot t - 1 : i \cdot t] = V_q^1[(i+1) \cdot t - 1 : i \cdot t],$
$W_i^1 = W_{i+1}^1[0 : i \cdot t - 1] = W_q^1[0 : i \cdot t - 1],$
$W_i^2 = W_{i+1}^1[(i+1) \cdot t - 1 : i \cdot t] = W_q^1[(i+1) \cdot t - 1 : i \cdot t],$
$\lambda_0^2 = \lambda_1^1,\ \gamma_0^2 = \gamma_1^1,\ V_0^2 = V_1^1,\ W_0^2 = W_1^1$

3 The Aa-set

Definition 6: For any positive integer q, t, z, i, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A_{k_{m,j}}^{i+1}, B_{k_{m,j}}^{i+1}};\ 1 \le m \le r_j\}_j,\ 1 \le j \le z$. We define the Aa-set with $Out,\ In$ as

$$Aa_{Out,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z)$$
$$= \{(X^{1,i+1},\ Y^{1,i+1}) | X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}, Out = (M_{k_{r_1},1}^{i+1}, \cdots M_{k_{r_z},z}^{i+1}), In = (E_{k_{r_1},1}, \cdots E_{k_{r_z},z})\}$$

where $Out, In \in F_2^d$, $d = \sum_{i=0}^{z} k_{r_i}$.
Let $d = \sum_{i=0}^{z} k_{r_i}$, then there are 2^d possible results for $(M_{k_{r_1},1}^{i+1}, \cdots M_{k_{r_z},z}^{i+1})$, thus

Property 3: For any positive integer q, t, z, i, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A_{k_{m,j}}^{i+1}, B_{k_{m,j}}^{i+1}};\ 1 \le m \le r_j\}_j,\ 1 \le j \le z$. Then

$$\bigcup_{Out \in F_2^d} Aa_{Out,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) = \left\{(X_{1,i+1}, Y_{1,i+1}) \,\middle|\, X_{1,i+1}, Y_{1,i+1} \in F_2^{(i+1)t}\right\}$$

where $In \in F_2^d$.

According to the **Property 2:**, we have:

Property 4: For any positive integer q, t, z, i, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A_{k_{m,j}}^{i+1}, B_{k_{m,j}}^{i+1}};\ 1 \le m \le r_j\}_j,\ 1 \le j \le z$. To any $Out_1, Out_2 \in F_2^d$, satisfied $Out_1 \ne Out_2$, then

$$Aa_{Out_1,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \cap Aa_{Out_2,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) = \varnothing$$

holds, where $In \in F_2^d$.

From **Theorem 3:**, we can that the Aa-set with Out, In can be divided into many disjoint subset , and each subset has the recursive structure:

Lemma 1: For any positive integer q, t, z, i, where i satisfy $0 \le i \le q-1$, given any z basic function series$\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, $1 \le j \le z$. We define the Aa-set with Out, $Middle$, In as

$$\begin{aligned} &Aa^{i+1}_{Out,Middle,In}(A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z) \\ &= \left\{ (X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i}) \middle| \begin{array}{c} X^{1,i}, Y^{1,i} \in Aa^i_{Middle,In}(A^i_{k_{r_j},j}, B^i_{k_{r_j},j},\ 1 \le j \le z); \\ Middle = (M^i_{k_{r_1,1}}, \cdots M^i_{k_{r_z,z}}); \\ X^{2,i}, Y^{2,i} \in Aa^1_{Out,Middle}(T^i_{k_{r_j},j}, D^i_{k_{r_j},j},\ 1 \le j \le z). \end{array} \right\}. \end{aligned}$$

where $Middle, Out, In \in F_2^d$, $d = \sum_{i=0}^{z} k_{r_i}$. Then,

$$Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z) = \bigcup_{Middle \in F_2^d} Aa^{i+1}_{Out,Middle,In}(Aa^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z)$$

holds, and for $Middle_1 \ne Middle_2$, $Middle_1, Middle_2 \in F_2^d$, satisfy

$$Aa^{i+1}_{Out,Middle_1,In}(A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z) \cap Aa^{i+1}_{Out,Middle_2,In}(A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z) = \varnothing$$

Proof. Firstly, due to $A^i_{k_{r_j},j}, B^i_{k_{r_j},j}$ can be decided according to the definition from the $A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j}$. From the **Property 4**, we know that for $Middle_1 \ne Middle_2$,

$$Aa^i_{Middle_1,In}(A^i_{k_{r_j},j}, B^i_{k_{r_j},j},\ 1 \le j \le z) \cap Aa^i_{Middle_2,In}(A^i_{k_{r_j},j}, B^i_{k_{r_j},j},\ 1 \le j \le z) = \varnothing$$

Thus,

$$Aa^{i+1}_{Out,Middle_1,In}(A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z) \cap Aa^{i+1}_{Out,Middle_2,In}(A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z) = \varnothing$$

Secondly, from **Theorem 3**, for $1 \le j \le z$, we have

$$f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}} = f(X^{2,i}, Y^{2,i})_{M^i_{k_{r_j},j}, T^i_{k_{r_j},j}, D^i_{k_{r_j},j}} \cdot 2^{i \cdot t} + f(X^{1,i}, Y^{1,i})_{E_{k_{m,j}}, A^i_{k_{m,j}}, B^i_{k_{m,j}}}.$$

For $1 \le j \le z$, let

$$\begin{aligned} M^{i+1}_{k_{r_j},j} &= [c^{2,i+1}_{0,k_{r_j},j}, c^{2,i+1}_{1,k_{r_j},j}, \cdots c^{2,i+1}_{k_{r_j},j-1,k_{r_j},j}] \\ S^i_{k_{r_j},j} &= [s^i_{0,k_{r_j},j}, s^i_{1,k_{r_j},j}, \cdots s^i_{k_{r_j},j-1}] \end{aligned}$$

According to the **Remark 6**,

$$c^{i+1}_{m,k_{r_j},j} = s^i_{m,k_{r_j},j} = carry^*_{c^i_{m,k_{r_j},j}}(X^{2,i}_m \oplus \alpha^{2,i}_{m,k_{r_j},j}, Y^{2,i}_m \oplus \beta^{2,i}_{k_{r_j},j})[t],\ 0 \le m \le k_{r_j},j - 1$$

hold. Thus,

$$
\begin{aligned}
&Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1\le j\le z)\\
=&\{(X^{1,i+1},\ Y^{1,i+1})|\ X^{1,i+1}, Y^{1,i+1}\in F_2^{(i+1)\cdot t}, Out=(M^{i+1}_{k_{r_1,1}},\cdots M^{i+1}_{k_{r_z,z}}), In=(E_{k_{r_1,1}},\cdots E_{k_{r_z,z}})\}\\
=&\left\{(X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{array}{c}X^{1,i}, Y^{1,i}\in F_2^{i\cdot t}, X^{2,i}, Y^{2,i}\in F_2^t, Middle\in F_2^d, In=(E_{k_{r_1,1}},\cdots E_{k_{r_z,z}}),\\ Middle=(M^i_{k_{r_1,1}},\cdots M^i_{k_{r_z,z}}),\ Out=(S^i_{k_{r_1,1}},\cdots S^i_{k_{r_z,z}}).\end{array}\right\}\\
=&\bigcup_{Middle\in F_2^d}\left\{X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{array}{c}X^{1,i}, Y^{1,i}\in F_2^{i\cdot t}; X^{2,i}, Y^{2,i}\in F_2^t; In=(E_{k_{r_1,1}},\cdots E_{k_{r_z,z}});\\ Middle=(M^i_{k_{r_1,1}},\cdots M^i_{k_{r_z,z}}); Out=(S^i_{k_{r_1,1}},\cdots S^i_{k_{r_z,z}}).\end{array}\right\}\\
=&\bigcup_{Middle\in F_2^d}\left\{(X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{array}{c}X^{1,i}, Y^{1,i}\in Aa^i_{Middle,In}(A^i_{k_{r_j,j}}, B^i_{k_{r_j,j}},\ 1\le j\le z),\\ X^{2,i}, Y^{2,i}\in Aa^1_{Out,Middle}(T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}},\ 1\le j\le z).\end{array}\right\}\\
=&\bigcup_{Middle\in F_2^d} Aa^{i+1}_{Out,Middle,In}(A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1\le j\le z)\}
\end{aligned}
$$

□

Definition 7: For any positive integer q, t, z, i, where i satisfy $0\le i\le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}};\ 1\le m\le r_j\}_j,\ 1\le j\le z$. Supposed that $G_j\in F_2^{r_j}$, $1\le j\le z$, $\gamma^1_{i+1}, \lambda^1_{i+1}, V^1_{i+1}, W^1_{i+1}\in F_2^{(i+1)\cdot t}$, $Out, In, Middle\in F_2^d$, where $d=\sum_{i=0}^{z} k_{r_i}$. Define the correlation coefficients of $h(X^{1,i+1}, Y^{1,i+1})$ as

$$
\begin{aligned}
&Cor^{i+1}_{In}\begin{pmatrix}\gamma^1_{i+1}, \lambda^1_{i+1}, V^1_{i+1}, W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}}, G_j,\ 1\le j\le z\end{pmatrix}\\
=&\sum_{\substack{X_{1,i+1}\in F_2^{(i+1)t},\\ Y_{1,i+1}\in F_2^{(i+1)t}}}(-1)^{(\gamma^1_{i+1},\lambda^1_{i+1})\cdot h(X^{1,i+1},Y^{1,i+1})\oplus V^1_{i+1}\cdot X^{1,i+1}\oplus W^1_{i+1}\cdot Y^{1,i+1}}\\
&where\ In=(E_{k_{r_1,1}},\cdots E_{k_{r_z,z}}).
\end{aligned}
$$

In addition, we also define the correlation coefficients of $h(X^{1,i+1}, Y^{1,i+1})$ over the Aa-set with $Out,\ In$ and the correlation coefficients of $h(X^{1,i+1}, Y^{1,i+1})$ over the Aa-set with $Out,\ Middle,\ In$ respectively as

$$
\begin{aligned}
&Cor^{i+1}_{Out,In}\begin{pmatrix}\gamma^1_{i+1}, \lambda^1_{i+1}, V^1_{i+1}, W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}}, G_j,\ 1\le j\le z\end{pmatrix}\\
=&\sum\nolimits_{(X_{1,i+1},Y_{1,i+1})\in Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},\ 1\le j\le z)}(-1)^{(\gamma^1_{i+1},\lambda^1_{i+1})\cdot h(X^{1,i+1},Y^{1,i+1})\oplus V^1_{i+1}\cdot X^{1,i+1}\oplus W^1_{i+1}\cdot Y^{1,i+1}}
\end{aligned}
$$

$$
\begin{aligned}
&Cor^{i+1}_{Out,Middile,In}\begin{pmatrix}\gamma^1_{i+1}, \lambda^1_{i+1}, V^1_{i+1}, W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}}, G_j,\ 1\le j\le z\end{pmatrix}\\
=&\sum\nolimits_{(X_{1,i+1},Y_{1,i+1})\in Aa^{i+1}_{Out,Middile,In}(A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},\ 1\le j\le z)}(-1)^{(\gamma^1_{i+1},\lambda^1_{i+1})\cdot h(X^{1,i+1},Y^{1,i+1})\oplus V^1_{i+1}\cdot X^{1,i+1}\oplus W^1_{i+1}\cdot Y^{1,i+1}}
\end{aligned}
$$

where

$$
h(X^{1,i+1}, Y^{1,i+1})=\bigoplus_{j=1}^{z}\bigoplus_{m=1}^{r_j} G_j[m]*f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}}
$$

From the property of the above defined set, we can see that the correlation coefficients of $h(X^{1,i+1},Y^{1,i+1})$ is equal to the sum of the correlation coefficients of $h(X^{1,i+1},Y^{1,i+1})$ over the Aa-set with $Out,\ In$, for all $Out \in F_2^d$. And the correlation coefficients of $h(X^{1,i+1},Y^{1,i+1})$ over the Aa-set with $Out,\ In$, have the recursive structure :

Theorem 4: For any positive integer q,t,z,i, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1},Y^{1,i+1})_{E_{k_{m,j}},A^{i+1}_{k_{m,j}},B^{i+1}_{k_{m,j}}};\ 1 \le m \le r_j\}_j,\ 1 \le j \le z$. Supposed that $G_j \in F_2^{r_j},\ 1 \le j \le z$, $\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1} \in F_2^{(i+1)\cdot t}$, $Out, In, Middle \in F_2^d$, where $d=\sum_{i=0}^{z} k_{r_i}$. Then

$$Cor^{i+1}_{In}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix} = \sum_{Out\in F_2^d} Cor^{i+1}_{Out,In}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix}$$

$$\begin{aligned}&Cor^{i+1}_{Out,In}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix}\\ &= \sum_{Middle\in F_2^d} Cor^{i+1}_{Out,Middle,In}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix}\\ &= \sum_{Middile\in F_2^d} Cor^{1}_{Out,Middle}\begin{pmatrix}\gamma^2_{i},\lambda^2_{i},V^2_{i},W^2_{i},\\ T^{i}_{k_{r_j,j}},D^{i}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix} \times Cor^{i}_{Middle,In}\begin{pmatrix}\gamma^1_{i},\lambda^1_{i},V^1_{i},W^1_{i},\\ A^{i}_{k_{r_j,j}},B^{i}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix}\end{aligned}$$

Proof. According to the **Property 3** and **Property 4**, we know that

$$\bigcup_{Out\in F_2^d} Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z) = \left\{(X_{1,i+1},Y_{1,i+1})\,\middle|\,X_{1,i+1},Y_{1,i+1} \in F_2^{(i+1)t}\right\}$$

and for different $Out \in F_2^d$, $Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)$ are disjoint. Thus

$$\begin{aligned}&Cor^{i+1}_{In}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix}\\ &= \sum_{(X_{1,i+1},Y_{1,i+1})\in F_2^{(i+1)t}} (-1)^{(\gamma^1_{i+1},\lambda^1_{i+1})\cdot h(X^{1,i+1},Y^{1,i+1})\oplus V^1_{i+1}\cdot X^{1,i+1}\oplus W^1_{i+1}\cdot Y^{1,i+1}}\\ &= \sum_{(X_{1,i+1},Y_{1,i+1})\in \bigcup_{Out\in F_2^d} Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},\ 1\le j\le z)} (-1)^{(\gamma^1_{i+1},\lambda^1_{i+1})\cdot h(X^{1,i+1},Y^{1,i+1})\oplus V^1_{i+1}\cdot X^{1,i+1}\oplus W^1_{i+1}\cdot Y^{1,i+1}}\\ &= \sum_{Out\in F_2^d}\sum_{(X_{1,i+1},Y_{1,i+1})\in Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},\ 1\le j\le z)} (-1)^{(\gamma^1_{i+1},\lambda^1_{i+1})\cdot h(X^{1,i+1},Y^{1,i+1})\oplus V^1_{i+1}\cdot X^{1,i+1}\oplus W^1_{i+1}\cdot Y^{1,i+1}}\\ &= \sum_{Out\in F_2^d} Cor^{i+1}_{In,Out}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix}\end{aligned}$$

Likely, from **Lemma 1**, we can also get

$$Cor^{i+1}_{In,Out}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix} = \sum_{Middle\in F_2^d} Cor^{i+1}_{In,Middle,Out}\begin{pmatrix}\gamma^1_{i+1},\lambda^1_{i+1},V^1_{i+1},W^1_{i+1},\\ A^{i+1}_{k_{r_j,j}},B^{i+1}_{k_{r_j,j}},G_j,\ 1 \le j \le z\end{pmatrix}$$

Secondly, from **Theorem 3**, for $1 \le j \le z$, we have

$$f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}} = f(X^{2,i}, Y^{2,i})_{M^i_{k_{r_j,j}}, T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}}} \cdot 2^{i \cdot t} + f(X^{1,i}, Y^{1,i})_{E_{k_{m,j}}, A^i_{k_{m,j}}, B^i_{k_{m,j}}}.$$

Then

$$\begin{aligned}
h(X^{1,i+1}, Y^{1,i+1}) &= \bigoplus_{j=1}^{z} \bigoplus_{m=1}^{r_j} G_j[m] * f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}} \\
&= \bigoplus_{j=1}^{z} \bigoplus_{m=1}^{r_j} G_j[m] * f(X^{2,i}, Y^{2,i})_{M^i_{k_{r_j,j}}, T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}}} \cdot 2^{i \cdot t} + \bigoplus_{j=1}^{z} \bigoplus_{m=1}^{r_j} G_j[m] * f(X^{1,i}, Y^{1,i})_{E_{k_{m,j}}, A^i_{k_{m,j}}, B^i_{k_{m,j}}}. \\
&= h(X^{1,i}, Y^{1,i}) \cdot 2^{i \cdot t} + h(X^{2,i}, Y^{2,i})
\end{aligned}$$

It can be concluded that:

$$Cor^{i+1}_{In,Middile,Out}\begin{pmatrix} \gamma^1_{i+1}, \lambda^1_{i+1}, V^1_{i+1}, W^1_{i+1}, \\ A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}}, G_j,\ 1 \le j \le z \end{pmatrix}$$

$$= \sum_{\substack{(X_{1,i+1}, Y_{1,i+1}) \in \\ Aa^{i+1}_{Out,Middile,In}(A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)}} (-1)^{\left[(\gamma^1_i, \lambda^1_i) \cdot h(X^{1,i}, Y^{1,i}) \oplus V^1_i \cdot X^{1,i} \oplus W^1_i \cdot Y^{1,i}\right] \oplus \left[(\gamma^2_i, \lambda^2_i) \cdot h(X^{2,i}, Y^{2,i}) \oplus V^2_i \cdot X^{2,i} \oplus W^2_i \cdot Y^{2,i}\right]}$$

$$\begin{aligned}
&= \sum\nolimits_{(X^{1,i}, Y^{1,i}) \in Aa^i_{Middle,In}(A^i_{k_{r_j,j}}, B^i_{k_{r_j,j}}\ 1 \le j \le z)} (-1)^{(\gamma^1_i, \lambda^1_i) \cdot h(X^{1,i}, Y^{1,i}) \oplus V^1_i \cdot X^{1,i} \oplus W^1_i \cdot Y^{1,i}} \\
&\times \sum\nolimits_{(X^{2,i}, Y^{2,i}) \in Aa^1_{Out,Middle}(T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}},\ 1 \le j \le z)} (-1)^{(\gamma^2_i, \lambda^2_i) \cdot h(X^{2,i}, Y^{2,i}) \oplus V^2_i \cdot X^{2,i} \oplus W^2_i \cdot Y^{2,i}} \\
&= Cor^1_{Middle,Out}\begin{pmatrix} \gamma^2_i, \lambda^2_i, V^2_i, W^2_i, \\ T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}}, G_j,\ 1 \le j \le z \end{pmatrix} \times Cor^i_{In,Middle}\begin{pmatrix} \gamma^1_i, \lambda^1_i, V^1_i, W^1_i, \\ A^i_{k_{r_j,j}}, B^i_{k_{r_j,j}}, G_j,\ 1 \le j \le z \end{pmatrix}
\end{aligned}$$

Thus,

$$\begin{aligned}
&Cor^{i+1}_{In,Out}\begin{pmatrix} \gamma^1_{i+1}, \lambda^1_{i+1}, V^1_{i+1}, W^1_{i+1}, \\ A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}}, G_j,\ 1 \le j \le z \end{pmatrix} \\
&= \sum_{Middile \in F_2^d} Cor^1_{Out,Middle}\begin{pmatrix} \gamma^2_i, \lambda^2_i, V^2_i, W^2_i, \\ T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}}, G_j,\ 1 \le j \le z \end{pmatrix} \times Cor^i_{Middle,In}\begin{pmatrix} \gamma^1_i, \lambda^1_i, V^1_i, W^1_i, \\ A^i_{k_{r_j,j}}, B^i_{k_{r_j,j}}, G_j,\ 1 \le j \le z \end{pmatrix}
\end{aligned}$$

□

4 The Df-set

Recall the law of total probability, given a series of subset $\{A_i,\ 1 \le i \le n\}$ of the total space, where $\bigcup_{i=1}^{n} A_i$ is the total space and each two subset of the $\{A_i,\ 1 \le i \le n\}$ are disjoint, then any probability $P(B)$ is equal to $\sum_{i=0}^{n} P(B \cap A_i)$. Notice that the the Aa-set with Out, In satisfy the above property, thus the same idea can be adopted to do the following study.

Definition 8: For any positive integer q, t, z, i, n, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, $1 \le j \le z$. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$, $C^1_{i+1} = (J^1_{i+1}, N^1_{i+1}) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$. We define the Df-set with In and the Df-set with Out, In respectively:

$$
\begin{aligned}
&Df^{i+1,n}_{In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)\\
=&\left\{ (X^{1,i+1},\ Y^{1,i+1}) \middle| \begin{array}{c} X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}, In = (E_{k_{r_1,1}}, \cdots E_{k_{r_z,z}}) \\ (G_0[s,0] * X^{1,i+1}, G_0[s,1] * Y^{1,i+1}) \bigoplus h_s(X^{1,i+1}, Y^{1,i+1}) = C^1_{i+1}[s], 1 \le s \le n. \end{array} \right\}\\
&Df^{i+1,n}_{Out,In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)\\
=&Df^{i+1,n}_{In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z) \bigcap Aa^{i+1}_{Out,In}(A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)\\
=&\left\{ (X^{1,i+1},\ Y^{1,i+1}) \middle| \begin{array}{c} X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}, Out = (M^{i+1}_{k_{r_1,1}}, \cdots M^{i+1}_{k_{r_z,z}}), In = (E_{k_{r_1,1}}, \cdots E_{k_{r_z,z}}), \\ (G_0[s,0] * X^{1,i+1}, G_0[s,1] * Y^{1,i+1}) \bigoplus h_s(X^{1,i+1}, Y^{1,i+1}) = C^1_{i+1}[s],\ 1 \le s \le n. \end{array} \right\}
\end{aligned}
$$

where

$$
h_s(X^{1,i+1}, Y^{1,i+1}) = \bigoplus_{j=1}^{z} \bigoplus_{m=1}^{r_j} G_j[s,m] * f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}},\ 1 \le s \le n.
$$

According to the **Property 3:** and **Property 4:** we have:
Property 5: For any positive integer q, t, z, i, n, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, $1 \le j \le z$. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$, $C^1_{i+1} = (J^1_{i+1}, N^1_{i+1}) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$. Then

$$
\bigcup_{Out \in F_2^d} Df^{i+1,n}_{Out,In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z) = Df^{i+1,n}_{In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)
$$

According to the **Property 2:**, we have:
Property 6: For any positive integer q, t, z, i, n, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, $1 \le j \le z$. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$, $C^1_{i+1} = (J^1_{i+1}, N^1_{i+1}) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, where $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$. If any two $Out_1, Out_2 \in F_2^d$ satisfy $Out_1 \ne Out_2$, then

$$
Df^{i+1,n}_{Out_1,In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z) \bigcap Df^{i+1,n}_{Out_2,In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z) = \varnothing
$$

As same as the law of total probability, we can get the relation between the Df-set with In and the Df-set with Out, In :
Theorem 5: For any positive integer q, t, z, i, n, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_{m,j}}, A^{i+1}_{k_{m,j}}, B^{i+1}_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, $1 \le j \le z$. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$, $C^1_{i+1} = (J^1_{i+1}, N^1_{i+1}) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, where $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$. Then

$$
\begin{aligned}
&\sum_{Out \in F_2^d} \# Df^{i+1,n}_{Out,In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)\\
=&\# Df^{i+1,n}_{In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j,j}}, B^{i+1}_{k_{r_j,j}},\ 1 \le j \le z)
\end{aligned}
$$

According to the **Lemma 1** and **Theorem 3**, it can be concluded that the Df-set with $Out,\ In$ have the recursive structure:

Lemma 2: For any positive integer q,t,z,i,n, where i satisfy $0 \le i \le q-1$, given any z basic function series $\{f(X^{1,i+1},Y^{1,i+1})_{E_{k_{m,j}},A^{i+1}_{k_{m,j}},B^{i+1}_{k_{m,j}}};\ 1 \le m \le r_j\}_j$, $1 \le j \le z$. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$, $C^1_{i+1} = (J^1_{i+1}, N^1_{i+1}) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, where $Out, In, Mi \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$. Define

$$Df^{i+1,n}_{Out,Mi,In}(C^1_{i+1},G_0,G_j,A^{i+1}_{k_{r_j},j},B^{i+1}_{k_{r_j},j},\ 1\le j\le z)$$
$$=\left\{(X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{matrix} X^{1,i},Y^{1,i} \in Df^{i,n}_{Mi,In}(C^1_i,G_0,G_j,A^i_{k_{r_j},j},B^i_{k_{r_j},j},\ 1\le j\le z) \\ X^{2,i},Y^{2,i} \in Df^{1,n}_{Out,Mi}(C^2_i,G_0,G_j,T^i_{k_{r_j},j},D^i_{k_{r_j},j},\ 1\le j\le z)\end{matrix}\right\}$$

Then,

$$Df^{i+1,n}_{Out,In}(C^1_{i+1},G_0,G_j,A^{i+1}_{k_{r_j},j},B^{i+1}_{k_{r_j},j},\ 1\le j\le z) = \bigcup_{Mi\in F_2^d} Df^{i+1,n}_{Out,Mi,In}(C^1_{i+1},G_0,G_j,A^{i+1}_{k_{r_j},j},B^{i+1}_{k_{r_j},j},\ 1\le j\le z)$$

holds. And for any two $Mi_1, Mi_2 \in F_2^d$, where $Mi_1 \ne Mi_2$, satisfy

$$Df^{i+1,n}_{Out,Mi_1,In}(C^1_{i+1},G_0,G_j,A^{i+1}_{k_{r_j},j},B^{i+1}_{k_{r_j},j},\ 1\le j\le z)\bigcap Df^{i+1,n}_{Out,Mi_2,In}(C^1_{i+1},G_0,G_j,A^{i+1}_{k_{r_j},j},B^{i+1}_{k_{r_j},j},\ 1\le j\le z)=\varnothing$$

Proof. According to the **Theorem 3**, we have

$$f(X^{1,i+1},Y^{1,i+1})_{E_{k_{m,j}},A^{i+1}_{k_{m,j}},B^{i+1}_{k_{m,j}}} = f(X^{2,i},Y^{2,i})_{M^i_{k_{r_j},j},T^i_{k_{r_j},j},D^i_{k_{r_j},j}}\cdot 2^{i\cdot t} + f(X^{1,i},Y^{1,i})_{E_{k_{m,j}},A^i_{k_{m,j}},B^i_{k_{m,j}}}.$$

$$h_s(X^{1,i+1},Y^{1,i+1}) = \bigoplus_{j=1}^{z}\bigoplus_{m=1}^{r_j} G_j[s,m]*f(X^{1,i+1},Y^{1,i+1})_{E_{k_{m,j}},A^{i+1}_{k_{m,j}},B^{i+1}_{k_{m,j}}},\ 1\le s\le n.$$

Thus, for $1 \le s \le n$:

$$h_s(X^{1,i+1},Y^{1,i+1}) = \bigoplus_{j=1}^{z}\bigoplus_{m=1}^{r_j} G_j[s,m]*f(X^{1,i+1},Y^{1,i+1})_{E_{k_{m,j}},A^{i+1}_{k_{m,j}},B^{i+1}_{k_{m,j}}}$$
$$=\bigoplus_{j=1}^{z}\bigoplus_{m=1}^{r_j} G_j[s,m]*f(X^{2,i},Y^{2,i})_{M^i_{k_{r_j},j},T^i_{k_{r_j},j},D^i_{k_{r_j},j}}\cdot 2^{i\cdot t} + \bigoplus_{j=1}^{z}\bigoplus_{m=1}^{r_j} G_j[s,m]*f(X^{1,i},Y^{1,i})_{E_{k_{m,j}},A^i_{k_{m,j}},B^i_{k_{m,j}}}.$$
$$= h_s(X^{1,i},Y^{1,i})\cdot 2^{i\cdot t} + h_s(X^{2,i},Y^{2,i})$$

It means that:

$$Df^{i+1,n}_{In}(C^1_{i+1},G_0,G_j,A^{i+1}_{k_{r_j},j},B^{i+1}_{k_{r_j},j},\ 1\le j\le z)$$
$$=\left\{(X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{matrix} X^{1,i},Y^{1,i}\in F_2^{i\cdot t}, X^{2,i},Y^{2,i}\in F_2^t, Mi\in F_2^d, \\ In=(E_{k_{r_1,1}},\cdots E_{k_{r_z,z}}), Mi=(M^{i+1}_{k_{r_1,1}},\cdots M^{i+1}_{k_{r_z,z}}), \\ h_s(X^{1,i},Y^{1,i})\bigoplus(G_0[s,0]*X^{1,i},G_0[s,1]*Y^{1,i}) = C^1_i[s], \\ h_s(X^{2,i},Y^{2,i})\bigoplus(G_0[s,0]*X^{2,i},G_0[s,1]*Y^{2,i}) = C^2_i[s],\ 1\le s\le n.\end{matrix}\right\}$$
$$=\left\{(X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{matrix} X^{1,i},Y^{1,i}\in Df^{i,n}_{Mi}(C^1_i,G_0,G_j,A^i_{k_{r_j},j},B^i_{k_{r_j},j},\ 1\le j\le z) \\ Mi\in F_2^d, Mi=(M^{i+1}_{k_{r_1,1}},\cdots M^{i+1}_{k_{r_z,z}}); \\ X^{2,i},Y^{2,i}\in Df^{1,n}_{In}(C^2_i,G_0,G_j,T^i_{k_{r_j},j},D^i_{k_{r_j},j},\ 1\le j\le z)\end{matrix}\right\}$$

Then,

$$
\begin{aligned}
&Df_{In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \bigcap A_{Out,Mi,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \\
&= \left\{ \begin{pmatrix} X^{2,i} || X^{1,i}, \\ Y^{2,i} || Y^{1,i} \end{pmatrix} \middle| \begin{array}{c} Mi = (M_{k_{r_1},1}^{i}, \cdots M_{k_{r_z},z}^{i}), \\ X^{1,i}, Y^{1,i} \in A_{Mi,In}^{i}(A_{k_{r_j},j}^{i}, B_{k_{r_j},j}^{i},\ 1 \le j \le z) \bigcap Df_{Mi}^{i,n}(C_i^1, G_0, G_j, A_{k_{r_j},j}^{i}, B_{k_{r_j},j}^{i},\ 1 \le j \le z) \\ X^{2,i}, Y^{2,i} \in A_{Out,Mi}^{1}(T_{k_{r_j},j}^{i}, D_{k_{r_j},j}^{i},\ 1 \le j \le z) \bigcap Df_{In}^{1,n}(C_i^2, G_0, G_j, T_{k_{r_j},j}^{i}, D_{k_{r_j},j}^{i},\ 1 \le j \le z) \end{array} \right\}
\end{aligned}
$$

It can be concluded that

$$
\begin{aligned}
&Df_{In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \bigcap A_{Out,Mi,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \\
=&Df_{Out,Mi,In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z)
\end{aligned}
$$

From Lemma 1, for any two $Mi_1, Mi_2 \in F_2^d$, where $Mi_1 \neq Mi_2$, satisfy

$$
A_{Out,Mi_1,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \bigcap A_{Out,Mi_2,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) = \varnothing
$$

Thus,

$$
Df_{Out,Mi_1,In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \bigcap Df_{Out,Mi_2,In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) = \varnothing
$$

Secondly, due to

$$
A_{Out,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) = \bigcup_{Mi \in F_2^d} A_{Out,Mi,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z)
$$

holds in Lemma 1, we can get:

$$
\begin{aligned}
&Df_{Out,In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \\
=&Df_{In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \bigcap A_{Out,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \\
=&Df_{In}^{i+1,n}(C_{i+1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \bigcap \bigcup_{Mi \in F_2^d} A_{Out,Mi,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \\
=& \bigcup_{Mi \in F_2^d} Df_{In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \bigcap A_{Out,Mi,In}^{i+1}(A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \\
=& \bigcup_{Mi \in F_2^d} Df_{Out,Mi,In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z)
\end{aligned}
$$

□

According to the above recursive structure, we can calculate the order of the Df-set with *Out*, *In* based on the following recurrence relation: **Corollary 2:** For any positive integer q, t, z, i, n, where i satisfy $0 \le i \le q-1$, then

$$
\begin{aligned}
&\#Df_{Out,In}^{i+1,n}(C_{i+1}^{1}, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z) \\
=& \sum_{Mi \in F_2^d} \#Df_{Out,Mi}^{1,n}(C_i^2, G_0, G_j, T_{k_{r_j},j}^{i}, D_{k_{r_j},j}^{i},\ 1 \le j \le z) \\
&\times \#Df_{Mi,In}^{i,n}(C_i^1, G_0, G_j, A_{k_{r_j},j}^{i}, B_{k_{r_j},j}^{i},\ 1 \le j \le z).
\end{aligned}
$$

holds.

5 The effective-time computer method

5.1 General method

From the **Theorem 4** and the **Corollary 2**, when In are given, if we define a vector D^{i+1}, of which component is taken from the $\#Df_{Out,In}^{i+1,n}(C_{i+1}^1, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \leq j \leq z)$(the correlation coefficients of $h(X^{1,i+1}, Y^{1,i+1})$ over the Aa-set with $Out,\ In$) for all possible Out, then D^{i+1} can be got by D^i premultiplying a matrix. And the coefficients of the matrix can be decided by the t-bit basic function. In addition, the recurrence relation is holds for any positive integer i, t. Let $t = 1$, we can generate all possible matrix in a short time. Then, combing with the **Theorem 4** and the **Corollary 2**, we can get the 1 bit regular:

Theorem 6: For any positive integer q, t, z, n, given any z basic function series $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A_{k_{m,j}}^q, B_{k_{m,j}}^q};\ 1 \leq m \leq r_j\}_j (X^{1,q}, Y^{1,q} \in F_2^{q \cdot t})$, $1 \leq j \leq z$; then we can get $T_{k_{r_j},j}^i, D_{k_{r_j},j}^i \in (F_2^t)^{r_j}$ from $A_{k_{m,j}}^q, B_{k_{m,j}}^q$, where $1 \leq j \leq z,\ 0 \leq j \leq q-1$. Supposed that $G_j \in F_2^{r_j}$, $1 \leq j \leq z$; $\gamma, \lambda, v, w \in F_2^{q \cdot t}$, $In, Out, In_1 \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$, Let $\lambda_q^1 = \lambda, \gamma_q^1 = \gamma, V_q^1 = v, w_q^1 = w$. Then,

$$Cor_{In}^q \begin{pmatrix} \gamma_q^1, \lambda_q^1, V_q^1, W_q^1, \\ A_{k_{r_j},j}^q, B_{k_{r_j},j}^q, G_j\ 1 \leq j \leq z \end{pmatrix} = L \prod_{i=0}^{q-1} Ma^i\ Q^T$$

where $L = (1, 1, \cdots, 1) \in F_2^d$, $Q_{In} \in F_2^d$, satisfy only $Q[In] = 1$, other component are 0; $Ma^i \in R^{d \times d}$, $Ma^i[Out, In_1] = Cor_{Out,In_1}^1 \begin{pmatrix} \gamma_i^2, \lambda_i^2, V_i^2, W_i^2, \\ T_{k_{r_j},j}^i, D_{k_{r_j},j}^i, G_j\ 1 \leq j \leq z \end{pmatrix}$, $0 \leq i \leq q-1$, $0 \leq Out, In_1 \leq 2^d - 1$.

Proof. Define vector $Base_{In}^i \in F_2^d$, $1 \leq i \leq q$, as follow:

$$Base_{In}^i[Out] = Cor_{Out,In}^i \begin{pmatrix} \gamma_i^1, \lambda_i^1, V_i^1, W_i^1, \\ A_{k_{r_j},j}^i, B_{k_{r_j},j}^i, G_j\ 1 \leq j \leq z \end{pmatrix}$$

where $0 \leq Out \leq 2^d - 1$.
According to the **Lemma 1**, we have:

$$Cor_{In}^q \begin{pmatrix} \gamma_q^1, \lambda_q^1, V_q^1, W_q^1, \\ A_{k_{r_j},j}^q, B_{k_{r_j},j}^q, G_j\ 1 \leq j \leq z \end{pmatrix} = L \cdot Base_{In}^q$$

By the definition, we see that $Base^1 = Ma^0 \cdot Q^T$.
According to the **Lemma 1**, for $1 \leq i \leq q-1$, $0 \leq Out \leq 2^d - 1$, we have

$$Base_{In}^{i+1}[Out] = \sum_{Out_1 \in F_2^d} Ma^i[Out, Out_1] \cdot Base_{In}^i[Out_1]$$

Namely,

$$Base_{In}^{i+1} = Ma^i \cdot Base_{In}^i$$

Thus, the theorem holds. □

Theorem 7: For any positive integer q, t, z, n, given any z basic function series $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A_{k_{m,j}}^q, B_{k_{m,j}}^q};\ 1 \leq m \leq r_j\}_j (X^{1,q}, Y^{1,q} \in F_2^{q \cdot t})$, $1 \leq j \leq z$; then we can get $T^i_{k_{r_j},j}, D^i_{k_{r_j},j} \in (F_2^t)^{r_j}$ from $A^q_{k_{m,j}}, B^q_{k_{m,j}}$, where $1 \le j \le z,\ 0 \le j \le q-1$. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$; $C = (J, N) \in (F_2^{n\times q\cdot t}, F_2^{n\times q\cdot t})$, $In, Out, In_1 \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$, Let $C = (J, N) = C_q^1 = (J_q^1, N_q^1)\ In$. Then,

$$Df^{q,n}_{In}(C, G_0, G_j, A^q_{k_{r_j},j}, B^q_{k_{r_j},j},\ 1 \le j \le z) = L \prod_{i=0}^{q-1} Md^i\ Q^T_{In} = || \prod_{i=0}^{q-1} Md^i\ Q^T_{In}||_1$$

where $L = (1, 1, \cdots, 1) \in F_2^d$, $Q_{In} \in F_2^d$, satisfy only $Q[In] = 1$, other component are 0; $Md^i \in R^{d\times d}$, $Md^i[Out, In_1] = \#Df^{1,n}_{Out,In_1}(C_i^2, G_0, G_j, T^i_{k_{r_j},j}, D^i_{k_{r_j},j},\ 1 \le j \le z)$, $0 \le i \le q-1$, $0 \le Out, In_1 \le 2^d - 1$.

Proof. Define vector $Num^i_{In} \in F_2^d$, $1 \le i \le q$, as follow:

$$Num^i_{In}[Out] = Df^{i,n}_{Out,In}(C_i^1, G_0, G_j, A^i_{k_{r_j},j}, B^i_{k_{r_j},j},\ 1 \le j \le z)$$

where $0 \le Out \le 2^d - 1$.
According to the **Theorem 5** we have:

$$Df^{q,n}_{In}(C_q^1, G_0, G_j, A^q_{k_{r_j},j}, B^q_{k_{r_j},j},\ 1 \le j \le z) = L \cdot Num^q_{In} = ||Num^q_{In}||_1$$

By the definition, we see that $Num^1_{In} = Md^0 \cdot Q^T_{In}$.
According to the **Corollary 2**, for $1 \le i \le q-1$, $0 \le Out \le 2^d - 1$, we have

$$Num^{i+1}_{In}[Out] = \sum_{Out_1 \in F_2^d} Md^i[Out, Out_1] \cdot Num^i_{In}[Out_1]$$

Namely,

$$Num^{i+1}_{In} = Md^i \cdot Num^i_{In}$$

Thus, the theorem holds. □

Remark 7: Supposed that $m = q$ and $t = 1$, in **Theorem 6** and **Theorem 7**, if $2^m \gg 2^d$ and $m \gg 2^{d^2}$, then the time complex of calculating the $Cor^q_{In}\begin{pmatrix} \gamma^1_q, \lambda^1_q, V^1_q, W^1_q, \\ A^q_{k_{r_j},j}, B^q_{k_{r_j},j}, G_j\ 1 \le j \le z \end{pmatrix}$ and $Df^{m,n}_{In}(C, G_j, A^q_{k_{r_j},j}, B^q_{k_{r_j},j},\ 1 \le j \le z)$ is about $O(m)$.

5.2 Instance

For $F : (x, y) \xrightarrow{F} (x, x \boxplus y)$, it can be treated as 1-order basic function. Besides this, its inverse function F^{-1} is $(x, y) \xrightarrow{F^{-1}} (x, x \boxminus y)$. According to the **Corollary 1**, it can be conversed into $(x, y) \xrightarrow{F^{-1}} (x, (x \oplus (1, 1, \cdots, 1)) \boxplus y \boxplus 1)$. For $\alpha, \beta, \gamma, \lambda \in F_2^n$, let $E = [1, 0]$, $B_1 = [0, \lambda]$, $A_1 = [0, \gamma]$, $B_2 = [\beta, \lambda]$, $A_2 = [\alpha, \gamma]$. Then, for 2-order basic function $f(x, y)_{E,A_1,B_1}$ and $f(x, y)_{E,A_2,B_2}$.

$$\begin{aligned} f(x, y)_{E,A_1,B_1} &= F^{-1}(F(x,\ y) \oplus (\gamma, \lambda)) \\ f(x, y)_{E,A_2,B_2} &= F^{-1}(F(x \oplus \alpha,\ y \oplus \beta) \oplus (\gamma, \lambda)) \end{aligned}$$

Thus, according to the **Theorem 6** and the **Theorem 7**, we have:
1. The formula for calculating the boomerange connective probability and its variant :
Corollary 3(BCT): Let F be $(x, y) \xrightarrow{F} (x, x \boxplus y)$, an element of BCT defined by

$$BCT(\alpha, \beta, \gamma, \lambda) = \#\{(x, y) \mid x, y \in F_2^n, F^{-1}(F(x,\ y) \oplus (\gamma, \lambda)) \oplus F^{-1}(F(x \oplus \alpha,\ y \oplus \beta) \oplus (\gamma, \lambda)) = (\alpha, \beta)\} \cdot 2^{-2n}$$

where $\alpha,\beta,\gamma,\lambda \in F_2^{2n}$. Then, for $0 \le i \le n-1$, let $Out = (o_1,o_2,o_3,o_4) \in F_2^4$, $In = (e_1,e_2,e_3,e_4) \in F_2^4, d[i] = (\alpha[i],\beta[i],\gamma[i],\lambda[i]), L = (1,1,\cdots,1) \in F_2^{16}$, $Q = (0,0,0,0,0,1,0,\cdots,0) \in F_2^{16}$.

And the elements of $M_{d[i]} \in F_2^{16\times 16}$ is defined as

$$M_{d[i]}[Out,In] = Df^{1,1}_{Out,In}((\alpha[i],\beta[i]),(0,0),\{(0,1),(0,\overline{\gamma[i]}),(0,\overline{\lambda[i]})\},\{(0,1),(\alpha[i],\overline{\gamma[i]}),(\beta[i],\overline{\lambda[i]})\})$$
$$=\#\left\{(x,y)\left|\begin{array}{c} e_4\oplus e_3\oplus e_1\oplus e_2=0,\ carry_{e_1}(y,x)[1]=o_1,\\ carry_{e_2}(y\oplus x\oplus e_1\oplus\lambda[i],x\oplus 1\oplus\gamma[i])[1]=o_2,\\ carry_{e_3}(y\oplus\beta[i],x\oplus\alpha[i])[1]=o_3,\\ carry_{e_4}(y\oplus\beta[i]\oplus x\oplus\alpha[i]\oplus e_3\oplus\lambda[i],x\oplus 1\oplus\alpha[i]\oplus\gamma[i])[1]=o_4;\\ where\ carry_e(x,y)[1]=(x\wedge y)\oplus(x\wedge e)\oplus(e\wedge y);\ x,y,\in F^2.\end{array}\right.\right\}$$

where $0 \le Out, In \le 15$. *Thus,*

$$BCT(\alpha,\beta,\gamma,\lambda) = 2^{-2n}\cdot L\prod_{i=0}^{n-1} M_{d[i]}\,Q^T = 2^{-2n}\cdot||\prod_{i=0}^{q-1} M_{d[i]}\,Q^T||_1$$

Corollary 4: (BCT^1) Let F be $(x,y)\xrightarrow{F}(x,x\boxplus y)$, an element of BCT^1 defined by

$$BCT^1(\alpha,\beta,\gamma,\lambda,\theta,\zeta) = \#\{(x,y)\mid x,y\in F_2^n, F^{-1}(F(x,\ y)\oplus(\gamma,\lambda))\oplus F^{-1}(F(x\oplus\alpha,\ y\oplus\beta)\oplus(\gamma,\lambda)) = (\theta,\zeta)\}\cdot 2^{-2n}$$

where $\alpha,\beta,\gamma,\lambda,\theta,\zeta \in F_2^{2n}$. Then, for $0 \le i \le n-1$, let $Out = (o_1,o_2,o_3,o_4) \in F_2^4$, $In = (e_1,e_2,e_3,e_4) \in F_2^4, L = (1,1,\cdots,1) \in F_2^{16}$, $Q = (0,0,0,0,0,1,0,\cdots,0) \in F_2^{16}$, $d[i] = (\alpha[i],\beta[i],\gamma[i],\lambda[i],\theta[i],\zeta[i]) \in F_2^6$.

And the elements of $M_{d[i]} \in F_2^{16\times 16}$ is defined as

$$M_{d[i]}[Out,In] = Df^{1,1}_{Out,In}((\theta[i],\zeta[i]),(0,0),\{(0,1),(0,\overline{\gamma[i]}),(0,\overline{\lambda[i]})\},\{(0,1),(\alpha[i],\overline{\gamma[i]}),(\beta[i],\overline{\lambda[i]})\})$$
$$=\#\left\{(x,y)\left|\begin{array}{c} \alpha[i]=\theta[i],\ \zeta[i]\oplus\beta[i]\oplus e_4\oplus e_3\oplus e_1\oplus e_2=0,\ carry_{e_1}(y,x)[1]=o_1,\\ carry_{e_2}(y\oplus x\oplus e_1\oplus\lambda[i],x\oplus 1\oplus\gamma[i])[1]=o_2,\\ carry_{e_3}(y\oplus\beta[i],x\oplus\alpha[i])[1]=o_3,\\ carry_{e_4}(y\oplus\beta[i]\oplus x\oplus\alpha[i]\oplus e_3\oplus\lambda[i],x\oplus 1\oplus\alpha[i]\oplus\gamma[i])[1]=o_4;\\ where\ carry_e(x,y)[1]=(x\wedge y)\oplus(x\wedge e)\oplus(e\wedge y);\ x,y,\in F^2.\end{array}\right.\right\}$$

where $0 \le Out, In \le 15$. *Thus,*

$$BCT^1(\alpha,\beta,\gamma,\lambda,\theta,\zeta) = 2^{-2n}\cdot L\prod_{i=0}^{n-1} M_{d[i]}\,Q^T = 2^{-2n}\cdot||\prod_{i=0}^{q-1} M_{d[i]}\,Q^T||_1$$

Corollary 5:(BCT^2) Let F be $(x,y)\xrightarrow{F}(x,x\boxplus y)$, an element of BCT^2 defined by

$$BCT^2(\alpha,\beta,\gamma,\lambda,\theta,\zeta) = \#\{(x,y)\mid x,y\in F_2^n, F^{-1}(F(x,\ y)\oplus(\theta,\zeta))\oplus F^{-1}(F(x\oplus\alpha,\ y\oplus\beta)\oplus(\gamma,\lambda)) = (\alpha,\beta)\}\cdot 2^{-2n}$$

where $\alpha,\beta,\gamma,\lambda,\theta,\zeta \in F_2^{2n}$. Then, for $0 \le i \le n-1$, let $Out = (o_1,o_2,o_3,o_4) \in F_2^4$, $In = (e_1,e_2,e_3,e_4) \in F_2^4, L = (1,1,\cdots,1) \in F_2^{16}$, $Q = (0,0,0,0,0,1,0,\cdots,0) \in F_2^{16}$, $d[i] = (\alpha[i],\beta[i],\gamma[i],\lambda[i],\theta[i],\zeta[i]) \in F_2^6$.

And the elements of $M_{d[i]} \in F_2^{16\times 16}$ is defined as

$$M_{d[i]}[Out,In] = Df^{1,1}_{Out,In}((\alpha[i],\beta[i]),(0,0),\{(0,1),(0,\overline{\theta[i]}),(0,\overline{\zeta[i]})\},\{(0,1),(\alpha[i],\overline{\gamma[i]}),(\beta[i],\overline{\lambda[i]})\})$$
$$=\#\left\{(x,y)\left|\begin{array}{c} \theta[i]\oplus\gamma[i]\oplus\zeta[i]\oplus e_4\oplus e_3\oplus e_1\oplus e_2=0,\\ \theta[i]\oplus\gamma[i]=0,\ carry_{e_1}(y,x)[1]=o_1,\\ carry_{e_2}(y\oplus x\oplus e_1\oplus\zeta[i],x\oplus 1\oplus\theta[i])[1]=o_2,\\ carry_{e_3}(y\oplus\beta[i],x\oplus\alpha[i])[1]=o_3,\\ carry_{e_4}(y\oplus\beta[i]\oplus x\oplus\alpha[i]\oplus e_3\oplus\lambda[i],x\oplus 1\oplus\alpha[i]\oplus\gamma[i])[1]=o_4;\\ where\ carry_e(x,y)[1]=(x\wedge y)\oplus(x\wedge e)\oplus(e\wedge y);\ x,y,\in F^2.\end{array}\right.\right\}$$

where $0 \le Out, In \le 15$. *Thus,*

$$BCT^1(\alpha,\beta,\gamma,\lambda,\theta,\zeta) = 2^{-2n}\cdot L\prod_{i=0}^{n-1} M_{d[i]}\, Q^T = 2^{-2n}\cdot ||\prod_{i=0}^{q-1} M_{d[i]}\, Q^T||_1$$

3. The formula for calculating the difference-boomerange connective probability and the inverse difference-boomrange probability, respectively:

Corollary 6-1:(DBT) Let F be $(x,y)\xrightarrow{F}(x,x\boxplus y)$, an element of DBT defined by

$$DBT(\alpha,\beta,\gamma,\lambda,\theta,\zeta) = \#\left\{(x,y)\middle|\begin{array}{c} x,y\in F_2^n, F\left(x,\ y\right)\oplus F\left(x\oplus\alpha,\ y\oplus\beta\right)=(\theta,\zeta),\\ F^{-1}\left(F\left(x,\ y\right)\oplus(\gamma,\lambda)\right)\oplus F^{-1}\left(F\left(x\oplus\alpha,\ y\oplus\beta\right)\oplus(\gamma,\lambda)\right)=(\alpha,\beta).\end{array}\right\}\cdot 2^{-2n}$$

where $\alpha,\beta,\gamma,\lambda,\theta,\zeta\in F_2^n$. Then, for $0\le i\le n-1$, let $Out=(o_1,o_2,o_3,o_4)\in F_2^4$, $In=(e_1,e_2,e_3,e_4)\in F_2^4, L=(1,1,\cdots,1)\in F_2^{16}$, $Q=(0,0,0,0,0,1,0,\cdots,0)\in F_2^{16}$, $d[i]=(\alpha[i],\beta[i],\gamma[i],\lambda[i],\theta[i],\zeta[i])\in F_2^6$.

And the elements of $M_{d[i]}\in F_2^{16\times 16}$ is defined as

$$\begin{aligned} & M_{d[i]}[Out,In]\\ =& Df_{Out,In}^{1,1}(\begin{pmatrix}\alpha[i], & \beta[i]\\ \theta[i], & \zeta[i]\end{pmatrix},\begin{pmatrix}0, & 0\\ 0, & 0\end{pmatrix},\{\begin{pmatrix}0,1\\1,0\end{pmatrix},(0,\overline{\gamma[i]}),(0,\overline{\lambda[i]})\},\{\begin{pmatrix}0,1\\1,0\end{pmatrix},(\alpha[i],\overline{\gamma[i]}),(\beta[i],\overline{\lambda[i]})\})\\ =&\#\left\{(x,y)\middle|\begin{array}{c}\alpha[i]=\theta[i],\ \alpha[i]\oplus\beta[i]\oplus\zeta[i]\oplus e_1\oplus e_3=0,\\ e_4\oplus e_3\oplus e_1\oplus e_2=0,\ carry_{e_1}\left(y,x\right)[1]=o_1,\\ carry_{e_2}\left(y\oplus x\oplus e_1\oplus\lambda[i],x\oplus 1\oplus\gamma\left[i\right]\right)[1]=o_2,\\ carry_{e_3}\left(y\oplus\beta\left[i\right],x\oplus\alpha\left[i\right]\right)[1]=o_3,\\ carry_{e_4}\left(y\oplus\beta\left[i\right]\oplus x\oplus\alpha\left[i\right]\oplus e_3\oplus\lambda[i],x\oplus 1\oplus\alpha\left[i\right]\oplus\gamma\left[i\right]\right)[1]=o_4;\\ where\ carry_e(x,y)[1]=\left(x\wedge y\right)\oplus\left(x\wedge e\right)\oplus\left(e\wedge y\right);\ x,y,\in F^2.\end{array}\right\}\end{aligned}$$

$where\ 0\le Out,In\le 15.\ Thus,$

$$DBT(\alpha,\beta,\gamma,\lambda,\theta,\zeta) = 2^{-2n}\cdot L\prod_{i=0}^{n-1} M_{d[i]}\, Q^T = 2^{-2n}\cdot ||\prod_{i=0}^{q-1} M_{d[i]}\, Q^T||_1$$

Corollary 6-2:(IDBT) Let F be $(x,y)\xrightarrow{F}(x,x\boxplus y)$, an element of DBT defined by

$$DBT(\alpha,\beta,\gamma,\lambda,\theta,\zeta) = \#\left\{(x,y)\middle|\begin{array}{c} x,y\in F_2^n, F^{-1}\left(x,\ y\right)\oplus F^{-1}\left(x\oplus\alpha,\ y\oplus\beta\right)=(\theta,\zeta),\\ F\left(F^{-1}\left(x,\ y\right)\oplus(\gamma,\lambda)\right)\oplus F\left(F^{-1}\left(x\oplus\alpha,\ y\oplus\beta\right)\oplus(\gamma,\lambda)\right)=(\alpha,\beta).\end{array}\right\}\cdot 2^{-2n}$$

where $\alpha,\beta,\gamma,\lambda,\theta,\zeta\in F_2^n$. Then, for $0\le i\le n-1$, let $Out=(o_1,o_2,o_3,o_4)\in F_2^4$, $In=(e_1,e_2,e_3,e_4)\in F_2^4, L=(1,1,\cdots,1)\in F_2^{16}$, $Q=(0,0,0,0,0,0,0,0,0,0,1,0,\cdots,0)\in F_2^{16}$, $d[i]=(\alpha[i],\beta[i],\gamma[i],\lambda[i],\theta[i],\zeta[i])\in F_2^6$.

And the elements of $M_{d[i]}\in F_2^{16\times 16}$ is defined as

$$\begin{aligned} & M_{d[i]}[Out,In]\\ =& Df_{Out,In}^{1,1}(\begin{pmatrix}\alpha[i], & \beta[i]\\ \theta[i], & \zeta[i]\end{pmatrix},\begin{pmatrix}0, & 0\\ 0, & 0\end{pmatrix},\{\begin{pmatrix}0,1\\1,0\end{pmatrix},(1,\gamma[i]),(1,\lambda[i])\},\{\begin{pmatrix}0,1\\1,0\end{pmatrix},(\overline{\alpha[i]},\gamma[i]),(\overline{\beta[i]},\lambda[i])\})\\ =&\#\left\{(x,y)\middle|\begin{array}{c}\alpha[i]=\theta[i],\ \alpha[i]\oplus\beta[i]\oplus\zeta[i]\oplus e_1\oplus e_3=0,\\ e_4\oplus e_3\oplus e_1\oplus e_2=0,\ carry_{e_1}\left(y,x\right)[1]=o_1,\\ carry_{e_2}\left(y\oplus x\oplus e_1\oplus\lambda[i],x\oplus 1\oplus\gamma\left[i\right]\right)[1]=o_2,\\ carry_{e_3}\left(y\oplus\beta\left[i\right],x\oplus\alpha\left[i\right]\right)[1]=o_3,\\ carry_{e_4}\left(y\oplus\beta\left[i\right]\oplus x\oplus\alpha\left[i\right]\oplus e_3\oplus\lambda[i],x\oplus 1\oplus\alpha\left[i\right]\oplus\gamma\left[i\right]\right)[1]=o_4;\\ where\ carry_e(x,y)[1]=\left(x\wedge y\right)\oplus\left(x\wedge e\right)\oplus\left(e\wedge y\right);\ x,y,\in F^2.\end{array}\right\}\end{aligned}$$

$where\ 0\le Out,In\le 15.\ Thus,$

$$DBT(\alpha,\beta,\gamma,\lambda,\theta,\zeta)=2^{-2n}\cdot L\prod_{i=0}^{n-1}M_{d[i]}\ Q^T=2^{-2n}\cdot||\prod_{i=0}^{q-1}M_{d[i]}\ Q^T||_1$$

3. The formula for calculating the difference probability :
Corollary 7:(DDT) Let S be $S(x,y)=x\boxplus y$, an element of DDT defined by

$$DDT(\alpha,\beta,\Delta)=\#\{(x,y)\mid x,y\in F_2^n, S\,(x\oplus\alpha,y\oplus\beta)\oplus S(x,y)=\Delta\}\cdot 2^{-2n}$$

where $\alpha,\beta,\Delta\in F_2^n$.Then, for $0\le i\le n-1$, let $Out=(o_1,o_3)\in F_2^2$, $In=(e_1,e_3), L=(1,1,1,1), Q=(1,0,0,0)\in F_2^4$,$d[i]=(\alpha[i],\beta[i],\Delta[i])\in F_2^3$.

And the elements of $M_{d[i]}\in F_2^{4\times4}$ is defined as

$$M_{d[i]}[Out,In]=Df^{1,1}_{Out,In}((\alpha[i],\Delta[i]),(0,0),\{(1),(0),(0)\},\{(1),(\alpha[i]),(\beta[i])\})$$
$$=\#\left\{(x,y)\left|\begin{array}{c}\alpha[i]\oplus\beta[i]\oplus\Delta[i]\oplus e_1\oplus e_3=0,\\ carry_{e_1}\,(y,x)\,[1]=o_1,\\ carry_{e_3}\,(y\oplus\beta\,[i]\,,x\oplus\alpha\,[i])\,[1]=o_3,\\ where\ carry_e(x,y)[1]=(x\wedge y)\oplus(x\wedge e)\oplus(e\wedge y)\,;\ x,y,\in F^2.\end{array}\right.\right\}$$

$where\ 0\le Out,In\le 3.\ Thus,$

$$DBT(\alpha,\beta,\gamma,\lambda,\theta,\zeta)=2^{-2n}\cdot L\prod_{i=0}^{n-1}M_{d[i]}\ Q^T=2^{-2n}\cdot||\prod_{i=0}^{q-1}M_{d[i]}\ Q^T||_1$$

4. The formula for calculating difference-linear connective correlation coefficients:
Corollary 8:(DLCT) Let S be a $S(x,y)=x\boxplus y$, an element of DLCT defined by

$$DLCT(\alpha,\beta,\lambda)=\sum_{x,y\in F_2^n}(-1)^{\lambda\cdot(S(x\oplus\alpha,y\oplus\beta)\oplus S(x,y))}$$

where $\alpha,\beta,\lambda\in F_2^n$.Then, for $0\le i\le n-1$, let $Out=(o_1,o_3)\in F_2^2$, $In=(e_1,e_3), L=(1,1,1,1), Q=(1,0,0,0)\in F_2^4$,$a[i]=(\alpha[i],\beta[i],\lambda[i])\in F_2^3$.

And the elements of $M_{a[i]}\in F_2^{4\times4}$ is defined as

$$M_{a[i]}[Out,In]=Cor^1_{Out,In}\left(\begin{array}{c}0,\lambda[i],0,0,\\ \{(1),(0),(0)\},\{(1),(\alpha[i]),(\beta[i])\}\end{array}\right)$$
$$=\sum_{x,y\in Set_{a[i],Out,In}}(-1)^{\lambda[i]\cdot(S(x\oplus\alpha[i],y\oplus\beta[i])\oplus S(x,y))}$$

where $Set_{a[i],Out,In}=\left\{(x,y)\left|\begin{array}{c}carry_{e_1}\,(y,x)\,[1]=o_1,\\ carry_{e_3}\,(y\oplus\beta\,[i]\,,x\oplus\alpha\,[i])\,[1]=o_3,\\ where\ carry_e(x,y)[1]=(x\wedge y)\oplus(x\wedge e)\oplus(e\wedge y)\,;\ x,y,\in F^2.\end{array}\right.\right\}$,

$0\le Out,In\le 3.\ Thus,$

$$DBT(\alpha,\beta,\gamma,\lambda,\theta,\zeta)=L\prod_{i=0}^{n-1}M_{a[i]}\ Q^T$$

5. The formula for calculating the linear approximation correlation coefficients(LAT):
Corollary 9:(LAT) Let S be $S(x,y)=x\boxplus y$, an element of LAT defined by

$$LAT(\mu,\omega,\lambda)=\sum_{x,y\in F_2^n}(-1)^{\mu\cdot x\oplus\omega\cdot y\oplus\lambda\cdot S(x)}$$

where $\mu, \omega, \lambda \in F_2^n$.Then, for $0 \le i \le n-1$, let $Out \in F_2$, $In \in F_2, L = (1,1)$, $Q = (1,0)$, $a[i] = (\mu[i], \omega[i], \lambda[i]) \in F_2^3$.

And the elements of $M_{a[i]} \in F_2^{2\times 2}$ is defined as

$$M_{a[i]}[Out, In] = Cor^1_{Out,In}\begin{pmatrix}0, \lambda[i], \mu[i], \omega[i], \\ \{(1), (0), (0)\},\end{pmatrix}$$
$$= \sum_{x,y \in Set_{a[i],Out,In}} (-1)^{\mu[i]\cdot x \oplus \omega[i]\cdot y \oplus \lambda[i]\cdot S(x)}$$

where $Set_{a[i],Out,In} = \left\{ (x,y) \middle| \begin{array}{c} carry_{In}(y,x)[1] = Out, \\ where\ carry_e(x,y)[1] = (x \wedge y) \oplus (x \wedge e) \oplus (e \wedge y)\,;\ x, y, \in F^2. \end{array} \right\}$,

$0 \le Out, In \le 1.\ Thus,$

$$DBT(\alpha, \beta, \gamma, \lambda, \theta, \zeta) = L \prod_{i=0}^{n-1} M_{a[i]}\ Q^T$$

Then, according to the **Theorem 8** in Appendix-A, after reducing the redundancy of matrix, we have the formulas for the calculating the boomerange-difference connective probability and the variant of difference-boomerange connective probability, respectively:

Corollary 10:(BDT**)** Let F be $(x,y) \xrightarrow{F} (x, x \boxplus y)$, an element of BDT defined by

$$BDT(\alpha, \beta, \gamma, \lambda, \theta, \zeta) = \#\left\{ (x,y) \middle| \begin{array}{c} x, y \in F_2^n, (x,y) \oplus F^{-1}(F(x \oplus \alpha,\ y \oplus \beta)) = (\theta, \zeta) \\ F^{-1}(F(x,\ y) \oplus (\gamma, \lambda)) \oplus F^{-1}(F(x \oplus \alpha,\ y \oplus \beta) \oplus (\gamma, \lambda)) = (\alpha, \beta). \end{array} \right\} \cdot 2^{-2n}$$

where $\alpha, \beta, \gamma, \lambda, \theta, \zeta \in F_2^n$. Then, for $0 \le i \le n-1$, let $Out = (o_1, o_2, o_3, o_4, o_5) \in F_2^5$, $In = (e_1, e_2, e_3, e_4, e_5) \in F_2^5$, $L = (1, 1, \cdots, 1) \in F_2^{32}$, $d[i] = (\alpha[i], \beta[i], \gamma[i], \lambda[i], \theta[i], \zeta[i]) \in F_2^6$, $Q = (0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,\cdots,0) \in F_2^{32}$.

And the elements of $M_{d[i]} \in F_2^{32\times 32}$ is defined as

$$M_{d[i]}[Out, In] = \#\left\{ (x,y) \middle| \begin{array}{c} \alpha[i] = \theta[i],\ 1 \oplus \beta[i] \oplus \zeta[i] \oplus e_5 \oplus e_3 = 0, \\ e_4 \oplus e_3 \oplus e_1 \oplus e_2 = 0,\ carry_{e_1}(y,x)[1] = o_1, \\ carry_{e_2}(y \oplus x \oplus e_1 \oplus \lambda[i], x \oplus 1 \oplus \gamma[i])[1] = o_2, \\ carry_{e_3}(y \oplus \beta[i], x \oplus \alpha[i])[1] = o_3, \\ carry_{e_4}(y \oplus \beta[i] \oplus x \oplus \alpha[i] \oplus e_3 \oplus \lambda[i], x \oplus 1 \oplus \alpha[i] \oplus \gamma[i])[1] = o_4; \\ carry_{e_5}(y \oplus \beta[i] \oplus x \oplus \alpha[i] \oplus e_3, x \oplus 1 \oplus \alpha[i] \oplus)[1] = o_5; \\ where\ carry_e(x,y)[1] = (x \wedge y) \oplus (x \wedge e) \oplus (e \wedge y)\,;\ x, y, \in F^2. \end{array} \right\}$$

$where\ 0 \le Out, In \le 31.\ Thus,$

$$BDT(\alpha, \beta, \gamma, \lambda, \theta, \zeta) = 2^{-2n} \cdot L \prod_{i=0}^{n-1} M_{d[i]}\ Q^T = 2^{-2n} \cdot ||\prod_{i=0}^{q-1} M_{d[i]}\ Q^T||_1$$

Corollary 11:(DBT^1**)** Let F be $(x,y) \xrightarrow{F} (x, x \boxplus y)$, an element of DBT^1 defined by

$$DBT^1(\alpha, \beta, \gamma, \lambda, \theta, \zeta, \eta, \psi) = \#\left\{ (x,y) \middle| \begin{array}{c} x, y \in F_2^n, F(x,\ y) \oplus F(x \oplus \alpha,\ y \oplus \beta) = (\theta, \zeta), \\ F^{-1}(F(x,\ y) \oplus (\gamma, \lambda)) \oplus F^{-1}(F(x,\ y) \oplus (\gamma, \lambda) \oplus (\theta, \zeta)) = (\eta, \psi). \end{array} \right\} \cdot 2^{-2n}$$

where $\alpha, \beta, \gamma, \lambda, \theta, \zeta, \eta, \psi \in F_2^n$.Then, for $0 \le i \le n-1$, let $Out = (o_1, o_2, o_3, o_4) \in F_2^4$, $In = (e_1, e_2, e_3, e_4) \in F_2^4, L = (1, 1, \cdots, 1) \in F_2^{16}$, $Q = (0,0,0,0,0,1,0,\cdots,0) \in F_2^{16}$, $d[i] = (\alpha[i], \beta[i], \gamma[i], \lambda[i], \theta[i], \zeta[i], \eta[i], \psi[i]) \in F_2^8$.

And the elements of $M_{d[i]} \in F_2^{16\times 16}$ is defined as

$$M_{d[i]}[Out, In] = \#\left\{ (x,y) \middle| \begin{array}{c} \alpha[i] = \theta[i],\ \alpha[i] \oplus \beta[i] \oplus \zeta[i] \oplus e_1 \oplus e_3 = 0, \\ \eta[i] = \theta[i],\ \theta[i] \oplus \zeta[i] \oplus e_4 \oplus e_1 \oplus e_2 = 0,\ carry_{e_1}(y,x)[1] = o_1, \\ carry_{e_2}(y \oplus x \oplus e_1 \oplus \lambda[i], x \oplus 1 \oplus \gamma[i])[1] = o_2, \\ carry_{e_3}(y \oplus \beta[i], x \oplus \alpha[i])[1] = o_3, \\ carry_{e_4}(y \oplus x \oplus e_1 \oplus \lambda[i] \oplus \zeta[i], x \oplus 1 \oplus \gamma[i] \oplus \theta[i])[1] = o_4; \\ where\ carry_e(x,y)[1] = (x \wedge y) \oplus (x \wedge e) \oplus (e \wedge y);\ x, y, \in F^2. \end{array} \right\}$$

$where\ 0 \le Out, In \le 15.\ Thus,$

$$DBT(\alpha, \beta, \gamma, \lambda, \theta, \zeta, \eta, \psi) = 2^{-2n} \cdot L \prod_{i=0}^{n-1} M_{d[i]}\ Q^T = 2^{-2n} \cdot || \prod_{i=0}^{q-1} M_{d[i]}\ Q^T ||_1$$

6 Appendix

6.1 Appendix A-reduce the redundancy of matrix

Definition 9: For any 2 basic function series $\{f(X,Y)_{E_{k_{m,1}}, A^{i+1}_{k_{m,1}}, B^{i+1}_{k_{m,1}}};\ 1 \le m \le r_1\}_1$ and $\{f(X,Y)_{E_{k_{m,2}}, A^{i+1}_{k_{m,2}}, B^{i+1}_{k_{m,2}}};\ 1 \le m \le r_2\}_2$, if there exist a k_1, such that $k_1 \ge 0$, $E_{k_{r_1,1}}[0:k_1] = E_{k_{r_2,2}}[0:k_1]$, $A^{i+1}_{k_{r_1,1}}[0:k_1] = A^{i+1}_{k_{r_2,2}}[0:k_1]$,$B^{i+1}_{k_{r_1,1}}[0:k_1] = B^{i+1}_{k_{r_2,2}}[0:k_1]$; then we called that the two basic function series are similar. And the degree of similarity deg for the two basic function series is defined as

$$deg = max\ \{k+1 | k \ge 0, E_{k_{m,1}}[0:k] = E_{k_{m,2}}[0:k], A^{i+1}_{k_{m,1}}[0:k] = A^{i+1}_{k_{m,2}}[0:k], B^{i+1}_{k_{m,1}}[0:k] = B^{i+1}_{k_{m,2}}\}.$$

Beside this, if two basic function series are not similar, we define $deg = 0$.
Definition 10: Given any z number $r_1, \cdot, r_z$, supposed that $1 \le j_1 \le j_2 \le z$, $deg \le r_{j_1}, r_{j_2}$, $d = \sum_{i=1}^{z} r_i$, then we can define

$$Sim^{j_1,j_2}_{deg} = \{V \in F_2^d\ | V = (V_1, V_2, \cdots V_z), V_{r_{j_1}}[0:d] = V_{r_{j_2}}[0:d], V_i \in F_2^{r_i}, 1 \le i \le z\}$$

Define the bijection $F : Sim^{j_1,j_2}_{deg} \xrightarrow{F} F_2^{d-deg}$ as:
$F(V_1, V_2, \cdots, V_{j_1}, \cdots, V_{j_2}, \cdots, V_z) = (V_1, V_2, \cdots, V_{j_1}, \cdots, V_{j_2}[deg : r_{j_2} - 1], \cdots, V_z)$.

Theorem 8: For any positive integer q, t, z, n, given any z basic function series $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A^q_{k_{m,j}}, B^q_{k_{m,j}}};\ 1 \le m \le r_j\}_j (X^{1,q}, Y^{1,q} \in F_2^{q\cdot t})$, $1 \le j \le z$; then we can get $T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}} \in (F_2^t)^{r_j}$ from $A^q_{k_{m,j}}, B^q_{k_{m,j}}$, where $1 \le j \le z$, $0 \le j \le q-1$. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$; $C = (J,N) \in (F_2^{n\times q\cdot t}, F_2^{n\times q\cdot t})$, $Out, In_1 \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$. If some of two basic function series are similar, of which code are j_1, j_2 respectively, then we define the degree of similarity for the two basic function series isdeg. Let $C = (J,N) = C_q^1 = (J_q^1, N_q^1)$, $In \in Sim^{j_1,j_2}_{deg}$. We can get:

$$Df^{q,n}_{In}(C, G_0, G_j, A^q_{k_{r_j,j}}, B^q_{k_{r_j,j}},\ 1 \le j \le z) = L \prod_{i=0}^{q-1} Md^i\ Q^T = || \prod_{i=0}^{q-1} Md^i\ Q^T ||_1$$

where $L = (1, 1, \cdots, 1) \in F_2^{d-deg}$, $Q \in F_2^{d-deg}$, satisfy only $Q[F(In)] = 1$, other component are 0; $Md^i[out, in] = \#Df^{1,n}_{F^{-1}(out), F^{-1}(in)}(C_i^2, G_0, G_j, T^i_{k_{r_j,j}}, D^i_{k_{r_j,j}},\ 1 \le j \le z)$, $0 \le i \le q-1$, $0 \le out, in \le 2^{d-deg} - 1$, $Md^i \in R^{(d-deg)\times(d-deg)}$.

Proof. According to the **Remark 5**, for $1 \le i \le q$, we have :
$Df^{i,n}_{Out,In}(C^1_i, G_0, G_j, A^i_{k_{r_j},j}, B^i_{k_{r_j},j},\ 1 \le j \le z) = 0$, when $in \notin Sim^{j_1,j_2}_{deg}$ and $out \in Sim^{j_1,j_2}_{deg}$.
$Df^{i,n}_{Out,In}(C^1_i, G_0, G_j, A^i_{k_{r_j},j}, B^i_{k_{r_j},j},\ 1 \le j \le z) = 0$, when $in \in Sim^{j_1,j_2}_{deg}$ and $out \notin Sim^{j_1,j_2}_{deg}$.
Thus, for $1 \le i \le q$, when $In \in Sim^{j_1,j_2}_{deg}$

$$\begin{aligned}&\sum_{Out \in Sim^{j_1,j_2}_{deg}} \#Df^{i,n}_{Out,In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z)\\ =&\#Df^{i,n}_{In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z)\end{aligned}$$

And for $1 \le i \le q-1$, when $In \in Sim^{j_1,j_2}_{deg}$,

$$\begin{aligned}&\#Df^{i+1,n}_{Out,In}(C^1_{i+1}, G_0, G_j, A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j},\ 1 \le j \le z)\\ =&\sum_{Mi \in Sim^{j_1,j_2}_{deg}} \#Df^{1,n}_{Out,Mi}(C^2_i, G_0, G_j, T^i_{k_{r_j},j}, D^i_{k_{r_j},j},\ 1 \le j \le z)\\ &\times \#Df^{i,n}_{Mi,In}(C^1_i, G_0, G_j, A^i_{k_{r_j},j}, B^i_{k_{r_j},j},\ 1 \le j \le z).\end{aligned}$$

Next, use the bijection F to transform Sim^{j_1,j_2}_{deg} into F_2^{d-deg} and do the similar way like the **Theorem 7**. Then, the theorem holds. □

Theorem 9: For any positive integer q, t, z, n, given any z basic function series $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A^q_{k_{m,j}}, B^q_{k_{m,j}}};\ 1 \le m \le r_j\}_j(X^{1,q}, Y^{1,q} \in F_2^{q\cdot t}),\ 1 \le j \le z$; then we can get $T^i_{k_{r_j},j}, D^i_{k_{r_j},j} \in (F_2^t)^{r_j}$ from $A^q_{k_{m,j}}, B^q_{k_{m,j}}$, where $1 \le j \le z$, $0 \le j \le q-1$. Supposed that $G_j \in F_2^{r_j}$, $1 \le j \le z$; $\gamma, \lambda, v, w \in F_2^{q\cdot t}$, $Out, In_1 \in F_2^d$, where $d = \sum_{i=0}^{z} k_{r_i}$. If some of two basic function series are similar, of which code are j_1, j_2 respectively, then we define the degree of similarity for the two basic function series isdeg. Let $\lambda^1_q = \lambda, \gamma^1_q = \gamma, V^1_q = v, W^1_q = w$, $In \in Sim^{j_1,j_2}_{deg}$. We can get:

$$Df^{q,n}_{In}(C, G_0, G_j, A^q_{k_{r_j},j}, B^q_{k_{r_j},j},\ 1 \le j \le z) = L \prod_{i=0}^{q-1} Md^i_1\ Q^T_{In} = ||\prod_{i=0}^{q-1} Md^i\ Q^T_{In}||_1$$

where $L = (1, 1, \cdots, 1) \in F_2^{d-deg}$, $Q \in F_2^{d-deg}$, satisfy only $Q[F(In)] = 1$, other component are 0; $Md^i[out, in] = \#Df^{1,n}_{F^{-1}(out),F^{-1}(in)}(C^2_i, G_0, G_j, T^i_{k_{r_j},j}, D^i_{k_{r_j},j},\ 1 \le j \le z)$, $0 \le i \le q-1$, $0 \le out, in \le 2^{d-deg} - 1$, $Md^i \in R^{(d-deg)\times(d-deg)}$.

$$Cor^q_{In}\begin{pmatrix} \gamma^1_q, \lambda^1_q, V^1_q, W^1_q, \\ A^q_{k_{r_j},j}, B^q_{k_{r_j},j}, G_j\ 1 \le j \le z\end{pmatrix} = L \prod_{i=0}^{q-1} Ma^i\ Q^T$$

where $L = (1, 1, \cdots, 1) \in F_2^{d-deg}$, $Q_{In} \in F_2^{d-deg}$, satisfy only $Q[F(In)] = 1$, other component are 0; $Ma^i[out, in] = Cor^1_{F^{-1}(out),F^{-1}(in)}\begin{pmatrix} \gamma^2_i, \lambda^2_i, V^2_i, W^2_i, \\ T^i_{k_{r_j},j}, D^i_{k_{r_j},j}, G_j\ 1 \le j \le z\end{pmatrix}$, $0 \le i \le q-1$, $0 \le out, in \le 2^{d-deg} - 1$, $Ma^i \in R^{(d-deg)\times(d-deg)}$.

Proof. According to the **Remark 5**, for $1 \le i \le q$, we have :
$Cor^i_{Out,In}\begin{pmatrix} \gamma^1_i, \lambda^1_i, V^1_i, W^1_i, \\ A^i_{k_{r_j},j}, B^i_{k_{r_j},j}, G_j,\ 1 \le j \le z\end{pmatrix} = 0$, when $in \notin Sim^{j_1,j_2}_{deg}$ and $out \in Sim^{j_1,j_2}_{deg}$.

$Cor^i_{Out,In}\begin{pmatrix} \gamma_i^1, \lambda_i^1, V_i^1, W_i^1, \\ A^i_{k_{r_j},j}, B^i_{k_{r_j},j}, G_j,\ 1 \le j \le z \end{pmatrix} = 0$, when $in \in Sim^{j_1,j_2}_{deg}$ and $out \notin Sim^{j_1,j_2}_{deg}$.

Thus, for $1 \le i \le q$, when $In \in Sim^{j_1,j_2}_{deg}$,

$$Cor^i_{In}\begin{pmatrix} \gamma_i^1, \lambda_i^1, V_i^1, W_i^1, \\ A^i_{k_{r_j},j}, B^i_{k_{r_j},j}, G_j,\ 1 \le j \le z \end{pmatrix} = \sum_{Out \in Sim^{j_1,j_2}_{deg}} Cor^i_{Out,In}\begin{pmatrix} \gamma_i^1, \lambda_i^1, V_i^1, W_{i+1}^1, \\ A^i_{k_{r_j},j}, B^i_{k_{r_j},j}, G_j,\ 1 \le j \le z \end{pmatrix}$$

And for $1 \le i \le q-1$, when $In \in Sim^{j_1,j_2}_{deg}$,

$$\begin{aligned} &Cor^{i+1}_{Out,In}\begin{pmatrix} \gamma_{i+1}^1, \lambda_{i+1}^1, V_{i+1}^1, W_{i+1}^1, \\ A^{i+1}_{k_{r_j},j}, B^{i+1}_{k_{r_j},j}, G_j,\ 1 \le j \le z \end{pmatrix} \\ = &\sum_{Mi \in Sim^{j_1,j_2}_{deg}} Cor^1_{Out,Mi}\begin{pmatrix} \gamma_i^2, \lambda_i^2, V_i^2, W_i^2, \\ T^i_{k_{r_j},j}, D^i_{k_{r_j},j}, G_j,\ 1 \le j \le z \end{pmatrix} \times Cor^i_{Mi,In}\begin{pmatrix} \gamma_i^1, \lambda_i^1, V_i^1, W_i^1, \\ A^i_{k_{r_j},j}, B^i_{k_{r_j},j}, G_j,\ 1 \le j \le z \end{pmatrix} \end{aligned}$$

Next, use the bijection F to transform Sim^{j_1,j_2}_{deg} into F_2^{d-deg} and do the similar way like the **Theorem 6**. Then, the theorem holds. □