The Study of Modulo 2^n

A General Method To Calculate The Probability Or Correlation Coefficients For Most Statistical 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-boomerang connective probability, boomerang connective probability, boomerang-difference connective probability, etc.

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

Contents

Introduction

Since the differential analysis and the linear analysis were proposed [1,2], statistical analysis, which makes use of some significant probability for the block cipher to distinguish from the random permutation, have become one of the research hotspots in the cryptanalysis of block cypher in the last 30 years. And most statistical analysis for block cypher is based on the statistical properties of nonlinear functions [1–5]. Specifically, most statistical properties of nonlinear functions is the probability that a series of boolean vector function with the form $\bigoplus_{i=1}^{n} f(x)_i$, where each $f(x)_i$ in the $\bigoplus_{i=1}^{n} f(x)_i$ is constituted by the composite operation of $\oplus$, the nonlinear function and its inverse, are equal to some given values or the correlation coefficients of a single boolean vector function $\bigoplus_{i=1}^{n} f(x)_i$. In most of block cypher, the construction of nonlinear functions is based on the S-box that it can be regard as the nonlinear function with small scale, especially in the SPN structure and Festial structure, the calculation of statistical properties of nonlinear functions can be completed by 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 values. Thus, for the SPN cipher and the Festial cipher, it almost has no problem to do the statistical analysis, such as differential analysis, linear analysis, boomerang 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 cipher to get the statistical properties of nonlinear functions by trying all possible value. In a word, compared with the SPN structure and the Festial structure, most studies of the utilize of statistical analysis method for the ARX cipher, 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 the polynomial time algorithms to calculate the statistical properties of modular addition 2^n. In 2001, Lipmaa.etc [6] and Johan Wallén [7] proposed the polynomial time algorithms to calculate the differential probability and the linear approximation correlation coefficients respectively, which was been about 10 years since the differential attack and the linear analysis were proposed. And in 2013, Schulte-Geers [8]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 are polynomial. Since then, the CCZ-equivalent relation of mod 2^n had been 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-boomerang connective probability, boomerang connective probability and boomerang-difference connective probability, etc [1–5], were proposed in order to improve the previous methods. And those methods had better performance in the SPN cipher and the Festial cipher. Unfortunately, according to the study of difference-linear connective correlation coefficients for nonlinear function [9], for any two permutations in the same CCZ-equivalent class, their difference-linear connective correlation coefficients are not in general invariant. It means that the CCZ-equivalent relation can't be regard as the general method to look for polynomial time algorithms to calculate the statistical properties of modular addition 2^n. Then, the following questions may be asked naturally:

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

2.Does there exits a general method that the explicit formula with polynomial time complex can be got for all of the current statistical properties of modular addition 2^n or even the properties that may come up in the future?

Our contribution

Firstly, this paper give the $O(n)$-time algorithm to calculate the probability or correlation for newly proposed property of Modulo 2^n, including the difference-linear connective correlation coefficients, the linear approximation correlation coefficients, the differential probability, difference-boomerang connective probability, boomerang connective probability, boomerang-difference connective probability, etc.

Secondly, for all of the current statistical property used for statistical analysis in block cipher, such as difference-linear connective correlation coefficients, the linear approximation correlation coefficients, the differential probability, difference-boomerang connective probability, boomerang connective probability, boomerang-difference connective probability, etc, it can be summarized as the probability of $\bigoplus_{z=1}^{n_j} f(x)_{z,j} = A_j,\ 1 \leq j \leq m$ or the correlation coefficients of $\lambda \cdot (\bigoplus_{i=1}^{n} f(x)_i)$, where $f(x)_{z,j},\ 1 \leq j \leq m,\ 1 \leq z \leq n_j$; $f(x)_i,\ 1 \leq i \leq n$ are composite operation of $\oplus$, the nonlinear function and its inverse. Based the above fact, we propose 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. According to 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 work.

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

$$\begin{aligned}
&c_0 = 0 \\
&c_{i+1} = (x_i \wedge y_i) \oplus (x_i \wedge c_i) \oplus (y_i \wedge c_i), 0 \leq i \leq n-1
\end{aligned}$$

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

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

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 $0 \leq i \leq n$; then

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

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 $c_i^1 \wedge c_i = 0$, for $0 \leq i \leq n-1$, by introduction. Supposed that $c_i^1 \wedge c_i = 0$ for $1 \leq i \leq k$. 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

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

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 $carry(x \oplus (1, \cdots 1), x) = 0^n$, 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 analysis method based on some statistics property of the nonlinear function in the cipher. And these statistics properties can be summarized as the probability of $\bigoplus_{z=1}^{n_j} f(x)_{z,j} = A_j,\ 1 \le j \le m$ or the correlation coefficients of $\lambda \cdot (\bigoplus_{i=1}^{n} f(x)_i)$, where $f(x)_{z,j},\ 1 \le j \le m,\ 1 \le z \le n_j$; $f(x)_i,\ 1 \le i \le n$ are composite operation of $\oplus$, the nonlinear function and its inverse. In the ARX cipher, 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 $x, y \in F_2^n$, $E_k = (e_0, e_1, \cdots e_{k-1}) \in F_2^k$, $\alpha_0, \alpha_1, \cdots \alpha_{k-1} \in F_2^n$, $\beta_0, \beta_1, \cdots \beta_{k-1} \in F_2^n$. Let $A_k = (\alpha_0, \alpha_2, \cdots \alpha_{k-1})$, $B_k = (\beta_0, \beta_2, \cdots \beta_{k-1})$, 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:

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

Then, 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 that 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 $E_{k-1}=E_k[0:k-2]=(e_0,e_1,\cdots e_{k-2}),A_{k-1}=A_k[0:k-2]=(\alpha_0,\alpha_2,\cdots\alpha_{k-2}),B_{k-1}=B_k[0:k-2]=(\beta_0,\beta_2,\cdots\beta_{k-2})$.

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 any $X^{1,i+1},Y^{1,i+1},\alpha_0^{1,i+1},\alpha_1^{1,i+1},\cdots,\alpha_{k-1}^{1,i+1},\beta_0^{1,i+1},\beta_1^{1,i+1},\cdots\beta_{k-1}^{1,i+1}\in F_2^{(i+1)\cdot t}$ and $E_k=(e_0,e_1,\cdots,e_{k-1})\in F_2^k$. 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

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

Moreover, $S_k^i=M_k^{i+1}$.

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,

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

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, due to the assumption of induction, we have:

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

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

3 Notion Description About The Basic Function Series

In order to reduce the redundancy of the article, we will introduce some notion description about the given z basic function series $\{f(X^{1,i}, Y^{1,i})_{E_{k_m}, A_{k_m}^i, B_{k_m}^i}; 1 \leq m \leq z\}$, which will be frequently adopted in the following proof.
Supposed that $X, Y \in F_2^{q \cdot t}$. For $1 \leq m \leq z$, let $\alpha_{0,m}^{1,q}, \alpha_{1,m}^{1,q}, \cdots, \alpha_{k_m-1,m}^{1,q}, \beta_{0,m}^{1,q}, \beta_{1,m}^{1,q}, \cdots,$ $\beta_{k_m-1,m}^{1,q} \in F_2^{q \cdot t}$, $E_m = (e_0, e_1, \cdots, e_{k_m-1}) \in F_2^{k_m}$.
In addition, let

$$\begin{aligned}
&X^{1,q} = X \\
&Y^{1,q} = Y \\
&A_m^q = [\alpha_{0,m}^{1,q}, \alpha_{1,m}^{1,q}, \cdots \alpha_{k_m-1,m}^{1,q}], \\
&B_m^q = [\beta_{0,m}^{1,q}, \beta_{1,m}^{1,q}, \cdots \beta_{k_m-1,m}^{1,q}];
\end{aligned}$$

And for $1 \le i \le q-1$, define:

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

Beside this, by the ,for $1 \le i \le q$, $1 \le m \le z$, let

$(X^{1,i}_{0,m}, y^{1,i}_{0,m}) = (X^{1,i}, Y^{1,i})$
$(X^{1,i}_{j+1,m}, Y^{1,i}_{j+1,m}) = (X^{1,i}_{j,m} \oplus \alpha^{1,i}_{j,m}, (X^{1,i}_{j,m} \oplus \alpha^{1,i}_{j,m}) \boxplus (Y^{1,i}_{j,m} \oplus \beta^{1,i}_{j,m}) \boxplus e_{j,m}),\ 0 \le j \le k_m - 1$

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

$$A^i_m = [\alpha^{1,i}_{0,m}, \alpha^{1,i}_{1,m}, \cdots \alpha^{1,i}_{k_m-1,m}], 1 \le m \le z$$
$$B^i_m = [\beta^{1,i}_{0,m}, \beta^{1,i}_{1,m}, \cdots \beta^{1,i}_{k_m-1,m}], 1 \le m \le z$$

then we have $(X^{1,i}_{k_{m,j}}, Y^{1,i}_{k_{m,j}}) = f(X^{1,i}, Y^{1,i})_{E_m, A^{i+1}_m, B^{i+1}_m}$, for $1 \le m \le z$.

Secondly, we can define:

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

where $1 \le i \le q$.

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

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

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

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

$$T^0_m = A^1_m, 1 \le m \le z$$
$$D^0_m = B^1_m, 1 \le m \le z$$
$$T^i_m = [\alpha^{2,i}_{0,m}, \alpha^{2,i}_{1,m}, \cdots \alpha^{2,i}_{k_m-1,m}], 1 \le m \le z$$
$$D^i_m = [\beta^{2,i}_{0,m}, \beta^{2,i}_{1,m}, \cdots \beta^{2,i}_{k_m-1,m}], 1 \le m \le z$$

4 The Aa-set

Definition 6: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A^{i+1}_{k_m}, B^{i+1}_{k_m}};\ 1 \le m \le z\}$. We define the Aa-set with $Out,\ In$

as

$$
\begin{aligned}
&Aa^{i+1}_{Out,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z)\\
&= \{(X^{1,i+1},\ Y^{1,i+1}) | X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}, Out = (M^{i+1}_1, \cdots M^{i+1}_z)\}
\end{aligned}
$$

where $Out, In \in F_2^d$, $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$.
Let $d = \sum_{i=0}^{z} k_{r_i}$, then there are 2^d possible results for $(M^{i+1}_1, \cdots M^{i+1}_z)$, thus
Property 3: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A^{i+1}_{k_m}, B^{i+1}_{k_m}};\ 1 \le m \le z\}$. Then, for all $Out \in F_2^d$, the Aa-set with $Out,\ In$ satisfies:

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

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

Property 4: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A^{i+1}_{k_m}, B^{i+1}_{k_m}};\ 1 \le m \le z\}$. For any $Out_1, Out_2 \in F_2^d$ satisfied $Out_1 \ne Out_2$, then

$$
Aa^{i+1}_{Out_1,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) \cap Aa^{i+1}_{Out_2,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) = \varnothing
$$

holds.

From **theorem 3**, we can see that the Aa-set with $Out,\ In$ can be divided into many subset, and each disjoint subset has the following recursive structure:
Lemma 1: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A^{i+1}_{k_m}, B^{i+1}_{k_m}};\ 1 \le m \le z\}$. We define the Aa-set with $Out,\ Mi,\ In$ as

$$
\begin{aligned}
&Aa^{i+1}_{Out,Mi,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z)\\
&= \left\{ (X^{2,i} || X^{1,i},\ Y^{2,i} || Y^{1,i}) \,\middle|\, \begin{array}{c} X^{1,i}, Y^{1,i} \in Aa^{i}_{Mi,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z); \\ Mi = (M^i_1, \cdots M^i_z); \\ X^{2,i}, Y^{2,i} \in Aa^{1}_{Out,Mi}(T^i_j, D^i_j,\ 1 \le j \le z). \end{array} \right\}.
\end{aligned}
$$

where $Mi, Out, In \in F_2^d$, $d = \sum_{i=0}^{z} k_{r_i}$, $In = (E_1, \cdots E_z)$. Then,

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

holds, and for $Mi_1 \ne Mi_2$, $Mi_1, Mi_2 \in F_2^d$, satisfy

$$
Aa^{i+1}_{Out,Mi_1,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) \cap Aa^{i+1}_{Out,Mi_2,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) = \varnothing
$$

Proof. Firstly, due to A^i_j, B^i_j can be decided according to the definition from the A^{i+1}_j, B^{i+1}_j. And from the **property 4**, we know that for $Mi_1 \ne Mi_2$,

$$
Aa^{i}_{Mi_1,In}(A^{i}_j, B^{i}_j,\ 1 \le j \le z) \cap Aa^{i}_{Mi_2,In}(A^{i}_j, B^{i}_j,\ 1 \le j \le z) = \varnothing
$$

Thus,

$$
Aa^{i+1}_{Out,Mi_1,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) \cap Aa^{i+1}_{Out,Mi_2,In}(A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) = \varnothing
$$

Secondly, from **theorem 3**, for $1 \leq j \leq z$, we have:

$$f(X^{1,i+1}, Y^{1,i+1})_{E_j, A_j^{i+1}, B_j^{i+1}} = f(X^{2,i}, Y^{2,i})_{M_j^i, T_j^i, D_j^i} \cdot 2^{i \cdot t} + f(X^{1,i}, Y^{1,i})_{E_j, A_j^i, B_j^i}.$$

Thus,

$$\begin{aligned}
& Aa_{Out,In}^{i+1}(A_j^{i+1}, B_j^{i+1},\ 1 \leq j \leq z) \\
=& \{(X^{1,i+1},\ Y^{1,i+1}) |\ X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}, Out = (M_1^{i+1}, \cdots M_z^{i+1})\} \\
=& \left\{ (X^{2,i} || X^{1,i},\ Y^{2,i} || Y^{1,i}) \left| \begin{array}{c} X^{1,i}, Y^{1,i} \in F_2^{i\cdot t}, X^{2,i}, Y^{2,i} \in F_2^t, Mi \in F_2^d, \\ Mi = (M_1^i, \cdots M_z^i),\ Out = (S_1^i, \cdots S_z^i). \end{array} \right. \right\} \\
=& \bigcup_{Mi \in F_2^d} \left\{ (X^{2,i} || X^{1,i},\ Y^{2,i} || Y^{1,i}) \left| \begin{array}{c} X^{1,i}, Y^{1,i} \in F_2^{i\cdot t}; Mi = (M_1^i, \cdots M_z^i); \\ X^{2,i}, Y^{2,i} \in F_2^t; Out = (S_1^i, \cdots S_z^i). \end{array} \right. \right\} \\
=& \bigcup_{Mi \in F_2^d} \left\{ (X^{2,i} || X^{1,i},\ Y^{2,i} || Y^{1,i}) \left| \begin{array}{c} X^{1,i}, Y^{1,i} \in Aa_{Mi,In}^i(A_j^i, B_j^i,\ 1 \leq j \leq z), \\ Mi = (M_1^i, \cdots M_z^i); \\ X^{2,i}, Y^{2,i} \in Aa_{Out,Mi}^1(T_j^i, D_j^i,\ 1 \leq j \leq z). \end{array} \right. \right\} \\
=& \bigcup_{Mi \in F_2^d} Aa_{Out,Mi,In}^{i+1}(A_j^{i+1}, B_j^{i+1},\ 1 \leq j \leq z)\}
\end{aligned}$$

□

Definition 7: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \leq j \leq z$, $1 \leq i \leq q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}};\ 1 \leq m \leq z\}$. Supposed that $\gamma, \lambda, V, W \in F_2^{(i+1)\cdot t}$, $Out, In, Middle \in F_2^d$, where $d = \sum_{i=0}^z k_i$, $In = (E_1, \cdots E_z)$. Define the correlation coefficients of $h(X^{1,i+1}, Y^{1,i+1})$ as

$$\begin{aligned}
& Cor_{In}^{i+1} \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^{i+1}, B_j^{i+1}\ 1 \leq j \leq z \end{pmatrix} \\
=& \sum_{\substack{X_{1,i+1} \in F_2^{(i+1)t}, \\ Y_{1,i+1} \in F_2^{(i+1)t}}} (-1)^{(\gamma,\lambda)\cdot h(X^{1,i+1}, Y^{1,i+1}) \oplus V \cdot X^{1,i+1} \oplus W \cdot Y^{1,i+1}}
\end{aligned}$$

where $h(X^{1,i+1}, Y^{1,i+1}) = \bigoplus_{m=1}^z f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}}$.
Additionally 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, Mi, In respectively as

$$\begin{aligned}
& Cor_{Out,In}^{i+1} \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^{i+1}, B_j^{i+1}\ 1 \leq j \leq z \end{pmatrix} \\
=& \sum\nolimits_{(X_{1,i+1}, Y_{1,i+1}) \in Aa_{Out,In}^{i+1}(A_j^{i+1}, B_j^{i+1})} (-1)^{(\gamma,\lambda)\cdot h(X^{1,i+1}, Y^{1,i+1}) \oplus V \cdot X^{1,i+1} \oplus W \cdot Y^{1,i+1}}
\end{aligned}$$

$$\begin{aligned}
& Cor_{Out,Mi,In}^{i+1} \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^{i+1}, B_j^{i+1}\ 1 \leq j \leq z \end{pmatrix} \\
=& \sum\nolimits_{(X_{1,i+1}, Y_{1,i+1}) \in Aa_{Out,Mi,In}^{i+1}(A_j^{i+1}, B_j^{i+1})} (-1)^{(\gamma,\lambda)\cdot h(X^{1,i+1}, Y^{1,i+1}) \oplus V \cdot X^{1,i+1} \oplus W \cdot Y^{1,i+1}}
\end{aligned}$$

From the property of the Aa-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 $h(X^{1,i+1}, Y^{1,i+1})$'s correlation coefficients 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 following recursive structure :

Theorem 4: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A^{i+1}_{k_m}, B^{i+1}_{k_m}};\ 1 \le m \le z\}$. Supposed that $\gamma, \lambda, V, W \in F_2^{(i+1)\cdot t}$, $Out, In, Middle \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$. Then

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

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

where

$$
\begin{aligned}
&\gamma^1 = \gamma[0 : i \cdot t - 1],\ \lambda^1 = \lambda[0 : i \cdot t - 1],\ V^1 = V[0 : i \cdot t - 1],\ W^1 = W[0 : i \cdot t - 1], \\
&\gamma^2 = \gamma[i \cdot t : (i+1) \cdot t - 1],\ \lambda^2 = \lambda[i \cdot t : (i+1) \cdot t - 1],\ V^2 = V[i \cdot t : (i+1) \cdot t - 1], \\
&W^2 = W[i \cdot t : (i+1) \cdot t - 1].
\end{aligned}
$$

Proof. According to the **property 3** and **property 4**, we have:

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

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

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

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

$$f(X^{1,i+1}, Y^{1,i+1})_{E_j, A_j^{i+1}, B_j^{i+1}} = f(X^{2,i}, Y^{2,i})_{M_j^i, T_j^i, D_j^i} \cdot 2^{i \cdot t} + f(X^{1,i}, Y^{1,i})_{E_j, A_j^i, B_j^i}.$$

Then

$$\begin{aligned} h(X^{1,i+1}, Y^{1,i+1}) &= \bigoplus_{j=1}^{z} h(X^{1,i+1}, Y^{1,i+1})_{E_j, A_j^{i+1}, B_j^{i+1}} \\ &= \bigoplus_{j=1}^{z} f(X^{2,i}, Y^{2,i})_{M_j^i, T_j^i, D_j^i} \cdot 2^{i \cdot t} + \bigoplus_{j=1}^{z} f(X^{1,i}, Y^{1,i})_{E_j, A_j^i, B_j^i}. \\ &= h(X^{1,i}, Y^{1,i}) \cdot 2^{i \cdot t} + h(X^{2,i}, Y^{2,i}) \end{aligned}$$

It can be concluded that:

$$\begin{aligned} & Cor_{In,Mi,Out}^{i+1} \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z \end{pmatrix} \\ =& \sum\nolimits_{(X^{1,i}, Y^{1,i}) \in Aa_{Mi,In}^{i}(A_j^i, B_j^i\ 1 \le j \le z)} (-1)^{(\gamma^1, \lambda^1) \cdot h(X^{1,i}, Y^{1,i}) \oplus V^1 \cdot X^{1,i} \oplus W^1 \cdot Y^{1,i}} \\ \times & \sum\nolimits_{(X^{2,i}, Y^{2,i}) \in Aa_{Out,Mi}^{1}(T_j^i, D_j^i,\ 1 \le j \le z)} (-1)^{(\gamma^2, \lambda^2) \cdot h(X^{2,i}, Y^{2,i}) \oplus V^2 \cdot X^{2,i} \oplus W^2 \cdot Y^{2,i}} \\ =& Cor_{Out,Mi}^{1} \begin{pmatrix} \gamma^2, \lambda^2, V^2, W^2, \\ T_j^i, D_j^i, G_j,\ 1 \le j \le z \end{pmatrix} \times Cor_{Mi,In}^{i} \begin{pmatrix} \gamma^1, \lambda^1, V^1, W^1, \\ A_j^{i+1}, B_j^{i+1}\ 1 \le j \le z \end{pmatrix} \end{aligned}$$

Thus,

$$\begin{aligned} & Cor_{Out,In}^{i+1} \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^{i+1}, B_j^{i+1}\ 1 \le j \le z \end{pmatrix} \\ =& \sum_{Mi \in F_2^d} Cor_{Out,Mi,In}^{i+1} \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^{i+1}, B_j^{i+1}\ 1 \le j \le z \end{pmatrix} \\ =& \sum_{Mi \in F_2^d} Cor_{Out,Mi}^{1} \begin{pmatrix} \gamma^2, \lambda^2, V^2, W^2, \\ T_j^i, D_j^i, G_j,\ 1 \le j \le z \end{pmatrix} \times Cor_{Mi,In}^{i} \begin{pmatrix} \gamma^1, \lambda^1, V^1, W^1, \\ A_j^{i+1}, B_j^{i+1}\ 1 \le j \le z \end{pmatrix} \end{aligned}$$

□

Theorem 6: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1) \cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}};\ 1 \le m \le z\}$. Supposed that $\gamma, \lambda, V, W \in F_2^{(i+1) \cdot t}$, $Out, In, Middle \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$. Then,

$$Cor_{In}^{q} \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^q, B_j^q, G_j\ 1 \le j \le z \end{pmatrix} = L \prod_{i=0}^{q-1} Ma^i\ Q^T$$

where $L = (1, 1, \cdots, 1) \in F_2^d$, $Q_{In} \in F_2^d$, of which the sole nonzero component satisfies $Q[In] = 1$, and $Ma^i \in R^{d \times d}$ satisfying $Ma^i[Out, In_1] = Cor_{Out,In_1}^{1} \begin{pmatrix} \gamma_i^2, \lambda_i^2, V_i^2, W_i^2, \\ T_j^i, D_j^i\ 1 \le j \le z \end{pmatrix}$, $0 \le i \le q-1$, $0 \le Out, In_1 \le 2^d - 1$, $\gamma_i^2 = \gamma[i \cdot t : (i+1) \cdot t - 1]$,$\lambda_i^2 = \lambda[i \cdot t : (i+1) \cdot t - 1]$,$V_i^2 = V[i \cdot t : (i+1) \cdot t - 1]$,$W_i^2 = W[i \cdot t : (i+1) \cdot t - 1]$.

Proof. For $1 \le i \le q$, define the vector $Base_{In}^{i} \in F_2^d$ as follow:

$$Base_{In}^{i}[Out] = Cor_{Out,In}^{i}\begin{pmatrix} \gamma_i^1, \lambda_i^1, V_i^1, W_i^1, \\ A_j^i, B_j^i\ 1 \le j \le z \end{pmatrix}$$

where $0 \le Out \le 2^d - 1$,$\gamma^1 = \gamma[0 : i \cdot t - 1]$,$\lambda^1 = \lambda[0 : i \cdot t - 1]$,$V^1 = V[0 : i \cdot t - 1]$,$W^1 = W[0 : i \cdot t - 1]$.

According to the **lemma 1**, we have:

$$Cor_{In}^{q}\begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^q, B_j^q,\ 1 \le j \le z \end{pmatrix} = L \cdot Base_{In}^{q}$$

And by the definition, we see that $Base^1 = Ma^0 \cdot Q^T$.
In addition, according to the **lemma 1**, for $1 \le i \le q-1$, $0 \le Out \le 2^d - 1$, 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. □

5 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 to equal the total space and each A_i are disjoint with each other, then for any event B, its 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 $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}};\ 1 \le m \le z\}$. Supposed that $G \in F_2^{n\times z}$, $C = (J, N) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$. We define the Df-set with In and the Df-set with Out, In respectively:

$$Df_{In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)$$
$$= \left\{ (X^{1,i+1},\ Y^{1,i+1}) \middle| \begin{array}{c} X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}, \\ h_s(X^{1,i+1}, Y^{1,i+1}) = C[s], 1 \le s \le n. \end{array} \right\}$$
$$Df_{Out,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)$$
$$= Df_{In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z) \bigcap Aa_{Out,In}^{i+1}(A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)$$
$$= \left\{ (X^{1,i+1},\ Y^{1,i+1}) \middle| \begin{array}{c} X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}, Out = (M_1^{i+1}, \cdots M_z^{i+1}), \\ h_s(X^{1,i+1}, Y^{1,i+1}) = C[s], 1 \le s \le n. \end{array} \right\}$$
$$Df_{Out,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)^*$$
$$= (\{F_2^{(i+1)\cdot t} \times F_2^{(i+1)\cdot t}\} - Df_{In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)) \bigcap Aa_{Out,In}^{i+1}(A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)$$

where

$$h_s(X^{1,i+1}, Y^{1,i+1}) = \bigoplus_{m=1}^{z} G[s, m] * f(X^{1,i+1}, Y^{1,i+1})_{E_m, A_m^{i+1}, B_m^{i+1}},\ 1 \le s \le n.$$

According to the **property 3** and **property 4** we have:
Property 5: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}};\ 1 \le m \le z\}$. Supposed that $G \in F_2^{n\times z}$, $C = (J, N) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$. Then

$$\bigcup_{Out\in F_2^d} Df_{Out,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z) = Df_{In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)$$

According to the **Property 2:**, we have:
Property 6: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}};\ 1 \le m \le z\}$. Supposed that $G \in F_2^{n\times z}$, $C = (J, N) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$. If any two $Out_1, Out_2 \in F_2^d$ satisfy $Out_1 \ne Out_2$, then

$$Df_{Out_1,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z) \bigcap Df_{Out_2,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z) = \varnothing$$

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 $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}};\ 1 \le m \le z\}$. Supposed that $G \in F_2^{n\times z}$, $C = (J, N) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$. Then

$$\begin{aligned}&\sum_{Out\in F_2^d} \#Df_{Out,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)\\ =&\#Df_{In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)\end{aligned}$$

5.1 direct method

According to the **lemma 1** and **theorem 3**, it can be concluded that the Df-set with $Out,\ In$ have the flowing recursive structure:
Lemma 2: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A_{k_m}^{i+1}, B_{k_m}^{i+1}};\ 1 \le m \le z\}$. Supposed that $G \in F_2^{n\times z}$, $C = (J, N) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$, $J^1 = J[0 : i\cdot t-1]$, $J^2 = J[i\cdot t : (i+1)\cdot t-1]$, $N^1 = N[0 : i\cdot t-1]$, $N^2 = N[i\cdot t : (i+1)\cdot t-1]$, $C^1 = (J^1, N^1), C^2 = (J^2, N^2)$. Define

$$\begin{aligned}&Df_{Out,Mi,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)\\ =&\left\{ (X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i}) \,\middle|\, \begin{array}{l} X^{1,i}, Y^{1,i} \in Df_{Mi,In}^{i,n}(C^1, G, A_j^i, B_j^i,\ 1 \le j \le z) \\ X^{2,i}, Y^{2,i} \in Df_{Out,Mi}^{1,n}(C^2, G, T_j^i, D_j^i,\ 1 \le j \le z) \end{array} \right\}\end{aligned}$$

Then,

$$Df_{Out,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z) = \bigcup_{Mi\in F_2^d} Df_{Out,Mi,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z)$$

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

$$Df_{Out,Mi_1,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z) \bigcap Df_{Out,Mi_2,In}^{i+1,n}(C, G, A_j^{i+1}, B_j^{i+1},\ 1 \le j \le z) = \varnothing$$

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

$$f(X^{1,i+1},Y^{1,i+1})_{E_j,A_j^{i+1},B_j^{i+1}} = f(X^{2,i},Y^{2,i})_{M_j^i,T_j^i,D_j^i}\cdot 2^{i\cdot t} + f(X^{1,i},Y^{1,i})_{E_j,A_j^i,B_j^i}.$$

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

$$\begin{aligned}
&h_s(X^{1,i+1},Y^{1,i+1}) = \bigoplus_{m=1}^{z} G[s,m]*f(X^{1,i+1},Y^{1,i+1})_{E_m,A_m^{i+1},B_m^{i+1}}\\
&= \bigoplus_{M=1}^{z} G[s,m]*f(X^{2,i},Y^{2,i})_{M_m^i,T_m^i,D_m^i}\cdot 2^{i\cdot t} + \bigoplus_{m=1}^{z} G_j[s,m]*f(X^{1,i},Y^{1,i})_{E_m,A_m^i,B_m^i}.\\
&= h_s(X^{1,i},Y^{1,i})\cdot 2^{i\cdot t} + h_s(X^{2,i},Y^{2,i})
\end{aligned}$$

It means that:

$$\begin{aligned}
&Df_{In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
&=\left\{(X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{matrix} X^{1,i},Y^{1,i}\in F_2^{i\cdot t}, X^{2,i},Y^{2,i}\in F_2^t, Mi\in F_2^d, Mi=(M_1^{i+1},\cdots M_z^{i+1}),\\ h_s(X^{1,i},Y^{1,i})=C_i^1[s],\\ h_s(X^{2,i},Y^{2,i})=C_i^2[s],\ 1\le s\le n.\end{matrix}\right\}\\
&=\left\{(X^{2,i}||X^{1,i},\ Y^{2,i}||Y^{1,i})\ \middle|\ \begin{matrix} X^{1,i},Y^{1,i}\in Df_{Mi}^{i,n}(C^1,G,A_j^i,B_j^i,\ 1\le j\le z)\\ Mi\in F_2^d, Mi=(M_1^{i+1},\cdots M_z^{i+1});\\ X^{2,i},Y^{2,i}\in Df_{In}^{1,n}(C^2,G,T_j^i,D_j^i,\ 1\le j\le z)\end{matrix}\right\}
\end{aligned}$$

Then,

$$\begin{aligned}
&Df_{In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\bigcap A_{Out,Mi,In}^{i+1}(A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
&=\left\{\begin{pmatrix} X^{2,i}||X^{1,i},\\ \\ Y^{2,i}||Y^{1,i}\end{pmatrix}\ \middle|\ \begin{matrix} Mi=(M_1^{i+1},\cdots M_z^{i+1}),\\ X^{1,i},Y^{1,i}\in A_{Mi,In}^i(A_j^i,B_j^i,\ 1\le j\le z)\bigcap Df_{Mi}^{i,n}(C^1,G,A_j^i,B_j^i,\ 1\le j\le z)\\ X^{2,i},Y^{2,i}\in A_{Out,Mi}^1(T_j^i,D_j^i,\ 1\le j\le z)\bigcap Df_{In}^{1,n}(C^2,G,T_j^i,D_j^i,\ 1\le j\le z)\end{matrix}\right\}
\end{aligned}$$

It can be concluded that

$$\begin{aligned}
&Df_{In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\bigcap A_{Out,Mi,In}^{i+1}(A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
&= Df_{Out,Mi,In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)
\end{aligned}$$

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

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

Thus,

$$Df_{Out,Mi_1,In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\bigcap Df_{Out,Mi_2,In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)=\varnothing$$

Secondly, due to

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

holds in Lemma 1, we can get:

$$\begin{aligned}
&Df_{Out,In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
=&Df_{In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\bigcap A_{Out,In}^{i+1}(A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
=&Df_{In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\bigcap \bigcup_{Mi\in F_2^d} A_{Out,Mi,In}^{i+1}(A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
=&\bigcup_{Mi\in F_2^d} Df_{In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\bigcap A_{Out,Mi,In}^{i+1}(A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
=&\bigcup_{Mi\in F_2^d} Df_{Out,Mi,In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)
\end{aligned}$$

□

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,n and $0\le i\le q-1$, then

$$\begin{aligned}
&\#Df_{Out,In}^{i+1,n}(C,G,A_j^{i+1},B_j^{i+1},\ 1\le j\le z)\\
=&\sum_{Mi\in F_2^d}\#Df_{Out,Mi}^{1,n}(C_i^2,G,T_j^i,D_j^i,\ 1\le j\le z)\\
&\times\#Df_{Mi,In}^{i,n}(C_i^1,G,A_j^i,B_j^i,\ 1\le j\le z).
\end{aligned}$$

holds.

Theorem 7: For $X^{1,i+1},Y^{1,i+1}\in F_2^{(i+1)\cdot t}$, $1\le j\le z$, $1\le i\le q-1$, given any z basic function $\{f(X^{1,i+1},Y^{1,i+1})_{E_{k_m},A_{k_m}^{i+1},B_{k_m}^{i+1}};\ 1\le m\le z\}$. Supposed that $G\in F_2^{n\times z}$, $C=(J,N)\in(F_2^{n\times(i+1)\cdot t},F_2^{n\times(i+1)\cdot t})$, $Out,In\in F_2^d$, where $d=\sum_{i=0}^{z}k_i$, $In=(E_1,\cdots E_z)$, $J_i^1=J[0:i\cdot t-1]$, $J_i^2=J[i\cdot t:(i+1)\cdot t-1]$, $N_i^1=N[0:i\cdot t-1]$, $N_i^2=N[i\cdot t:(i+1)\cdot t-1]$, $C_i^1=(J^1,N^1), C_i^2=(J^2,N^2)$. Let $C=(J,N)=C_q^1=(J_q^1,N_q^1)$. Then,

$$Df_{In}^{q,n}(C,G,A_j^q,B_j^q,\ 1\le j\le z)=L\prod_{i=0}^{q-1}Md^i\,Q_{In}^T$$

where $L=(1,1,\cdots,1)\in F_2^d$, $Q_{In}\in F_2^d$, of which the sole nonzero component satisfies $Q[In]=1$, and $Md^i\in R^{d\times d}$ satisfying $Md^i[Out,In_1]=\#Df_{Out,In_1}^{1,n}(C_i^2,G,T_j^i,D_j^i,\ 1\le j\le z)$, $0\le i\le q-1$, $0\le Out,In_1\le 2^d-1$.

Proof. For $1\le i\le q$, define vector $Num_{In}^i\in F_2^d$ as follow:

$$Num_{In}^i[Out]=Df_{Out,In}^{i,n}(C_i^1,G_0,G_j,A_j^i,B_j^i,\ 1\le j\le z)$$

where $0\le Out\le 2^d-1$.

According to the **theorem 5** we have:

$$Df_{In}^{q,n}(C,G,A_j^q,B_j^q,\ 1\le j\le z)=L\cdot Num_{In}^q$$

And by the definition, we see that $Num_{In}^1=Md^0\cdot Q_{In}^T$.

In addition, according to the **corollary 2**, for $1\le i\le q-1$, $0\le Out\le 2^d-1$, we have

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

Namely,

$$Num_{In}^{i+1}=Md^i\cdot Num_{In}^i$$

Thus, the theorem holds. □

5.2 indirect method

In this part, we will use the Markov chain to complete the proof of the **Theorem 7:**
Theorem 7: For $X^{1,i+1}, Y^{1,i+1} \in F_2^{(i+1)\cdot t}$, $1 \le j \le z$, $1 \le i \le q-1$, given any z basic function $\{f(X^{1,i+1}, Y^{1,i+1})_{E_{k_m}, A^{i+1}_{k_m}, B^{i+1}_{k_m}};\ 1 \le m \le z\}$. Supposed that $G \in F_2^{n\times z}$, $C = (J, N) \in (F_2^{n\times(i+1)\cdot t}, F_2^{n\times(i+1)\cdot t})$, $Out, In \in F_2^d$, where $d = \sum_{i=0}^{z} k_i$, $In = (E_1, \cdots E_z)$, $J_i^1 = J[0 : i\cdot t-1]$, $J_i^2 = J[i\cdot t : (i+1)\cdot t-1]$, $N_i^1 = N[0 : i\cdot t-1]$, $N_i^2 = N[i\cdot t : (i+1)\cdot t-1]$, $C_i^1 = (J^1, N^1)$, $C_i^2 = (J^2, N^2)$. Let $C = (J, N) = C_q^1 = (J_q^1, N_q^1)$ .If $X^{1,i+1}, Y^{1,i+1}$ are chosen uniformly at random, Then,

$$Pr((X^{1,i+1}, Y^{1,i+1}) \in Df_{In}^{q,n}(C, G, A_j^q, B_j^q,\ 1 \le j \le z)) = L \prod_{i=0}^{q-1} Md^i\ Q_{In}^T$$

where $L = (1, 1, \cdots, 1) \in F_2^d$, $Q_{In} \in F_2^d$, of which the sole nonzero component satisfies $Q[In] = 1$, and $Md^i \in R^{d\times d}$ satisfying $Md^i[Out, In_1] = \frac{1}{2^z}\#Df^{1,n}_{Out,In_1}(C_i^2, G, T_j^i, D_j^i,\ 1 \le j \le z)$, $0 \le i \le q-1$, $0 \le Out, In_1 \le 2^d - 1$.

Proof. Supposed that the state $T^{i+1,n}_{Out,In}(C^1_{i+1}, G, A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z)$ means that $(X^{1,i+1}, Y^{1,i+1}) \in Df^{i+1,n}_{Out,In}(C, G, A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z)$; the state $F^{i+1,n}_{Out,In}(C^1_{i+1}, G, A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z)$ means that $(X^{1,i+1}, Y^{1,i+1}) \in Df^{i+1,n}_{Out,In}(C, G, A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z)^*$. Thus, we can find that any two of the above sates are disjoint and the union of all the above state is Ω according to the Property 5-6.
Secondly, for $1 \le s \le n$, due to

$$\begin{aligned}
&h_s(X^{1,i+1}, Y^{1,i+1}) = \bigoplus_{m=1}^{z} G[s, m] * f(X^{1,i+1}, Y^{1,i+1})_{E_m, A_m^{i+1}, B_m^{i+1}} \\
&= \bigoplus_{M=1}^{z} G[s, m] * f(X^{2,i}, Y^{2,i})_{M_m^i, T_m^i, D_m^i} \cdot 2^{i\cdot t} + \bigoplus_{m=1}^{z} G_j[s, m] * f(X^{1,i}, Y^{1,i})_{E_m, A_m^i, B_m^i} \cdot \\
&= h_s(X^{1,i}, Y^{1,i}) \cdot 2^{i\cdot t} + h_s(X^{2,i}, Y^{2,i})
\end{aligned}$$

If we know the value of $X^{1,i}, Y^{1,i} \in F_2^{i\cdot t}$, then the probability of which sate $X^{1,i+1}, Y^{1,i+1}$ belong to is depend on the state that $X^{1,i}, Y^{1,i}$ belong to. Thus, we can use it to build a Markov chain.
For $1 \le i \le q-1$, $O_1, O_2 \in F_2^d$:

$$Pr(T^{i+1,n}_{O_1,In}(C^1_{i+1}, G, A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) | T^{i,n}_{O_2,In}(C_i^1, G, A_j^i, B_j^i,\ 1 \le j \le z)) = Md^i[O_1, O_2]$$
$$Pr(T^{i+1,n}_{O_1,In}(C^1_{i+1}, G, A^{i+1}_j, B^{i+1}_j,\ 1 \le j \le z) | F^{i,n}_{O_2,In}(C_i^1, G, A_j^i, B_j^i,\ 1 \le j \le z)) = 0$$

Thus, the one step transform matrix form i to $i+1$ is:

$$\begin{Bmatrix} Md^i, O \\ *, * \end{Bmatrix}$$

Then, the $q-1$ step transform matrix is

$$\begin{Bmatrix} \prod_{i=1}^{q-1} Md^i, O \\ *, * \end{Bmatrix}$$

Define vector $V_{In} \in F_2^d$ as follow:

$$V_{In}[Out] = Df^{0,n}_{Out,In}(C_0^1, G_0, G_j, A_j^0, B_j^0,\ 1 \le j \le z)$$

where $0 \leq Out \leq 2^d - 1$. Then $V_{In} = Md^0 * Q_{In}^T$. According to the property of Markov chain, we get

$$Pr((X^{1,i+1}, Y^{1,i+1}) \in Df_{In}^{q,n}(C, G, A_j^q, B_j^q,\ 1 \leq j \leq z)) = L \prod_{i=1}^{q-1} Md^i\ V_{In} = L \prod_{i=0}^{q-1} Md^i\ Q_{In}^T$$

□

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 $Cor_{In}^q \begin{pmatrix} \gamma, \lambda, V, W, \\ A_j^q, B_j^q\ 1 \leq j \leq z \end{pmatrix}$ and $Df_{In}^{m,n}(C, G, A_j^q, B_j^q,\ 1 \leq j \leq z)$ is about $O(m)$.

5.3 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 $f(x, y)_{E,A_2,B_2}$, the following equation holds.

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

Thus, according to the **theorem 6** and the **theorem 7**, we have:
1. The formula for calculating the boomerang connective probability and its variant :
Corollary 3(BCT): Let F be $(x, y) \xrightarrow{F} (x, x \boxplus y)$, an element of BCT [4] defined by

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

where $\alpha, \beta, \gamma, \lambda \in F_2^{2n}$. Then, for $0 \leq i \leq n-1$, 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 $M_{d[i]} \in F_2^{16\times 16}$ is defined as

$$\begin{aligned} &M_{d[i]}[Out, In] \\ =&Df_{Out,In}^{1,1}((\alpha[i], \beta[i]), (0, 0), \{(0, 1), (0, \overline{\gamma[i]}), (0, \lambda[i])\}, \{(0, 1), (\alpha[i], \overline{\gamma[i]}), (\beta[i], \lambda[i])\}) \\ =&\# \left\{ (x, y) \left| \begin{array}{c} e_4 \oplus e_3 \oplus e_1 \oplus e_2 = 0,\ carry_{e_1}\left(y, x\right)[1] = o_1, \\ carry_{e_2}\left(y \oplus x \oplus e_1 \oplus \lambda[i], x \oplus 1 \oplus \gamma\left[i\right]\right)[1] = o_2, \\ carry_{e_3}\left(y \oplus \beta\left[i\right], x \oplus \alpha\left[i\right]\right)[1] = o_3, \\ carry_{e_4}\left(y \oplus \beta\left[i\right] \oplus x \oplus \alpha\left[i\right] \oplus e_3 \oplus \lambda[i], x \oplus 1 \oplus \alpha\left[i\right] \oplus \gamma\left[i\right]\right)[1] = o_4; \\ where\ carry_e(x, y)[1] = (x \wedge y) \oplus (x \wedge e) \oplus (e \wedge y)\,;\ x, y, \in F^2. \end{array} \right. \right\} \\ &where\ 0 \leq Out, In \leq 15. Thus, \end{aligned}$$

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

Corollary 4 (BCT^1): Let F be $(x, y) \xrightarrow{F} (x, x \boxplus y)$, an element of BCT^1 [10] defined as

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

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

$$\begin{aligned}
&M_{d[i]}[Out, In] \\
=&Df^{1,1}_{Out,In}((\theta[i], \zeta[i]), (0,0), \{(0,1), (0, \overline{\gamma[i]}), (0, \lambda[i])\}, \{(0,1), (\alpha[i], \overline{\gamma[i]}), (\beta[i], \lambda[i])\}) \\
=&\#\left\{(x,y)\ \middle|\ \begin{array}{c} \alpha[i] = \theta[i],\ \zeta[i] \oplus \beta[i] \oplus e_4 \oplus e_3 \oplus e_1 \oplus e_2 = 0,\ carry_{e_1}(y,x)[1] = o_1, \\ carry_{e_2}(y \oplus x \oplus e_1 \oplus \lambda[i], x \oplus 1 \oplus \gamma[i])[1] = o_2, \\ carry_{e_3}(y \oplus \beta[i], x \oplus \alpha[i])[1] = o_3, \\ carry_{e_4}(y \oplus \beta[i] \oplus x \oplus \alpha[i] \oplus e_3 \oplus \lambda[i], x \oplus 1 \oplus \alpha[i] \oplus \gamma[i])[1] = o_4; \\ where\ carry_e(x,y)[1] = (x \wedge y) \oplus (x \wedge e) \oplus (e \wedge y);\ x, y, \in F^2. \end{array}\right\} \\
&where\ 0 \le Out, In \le 15. Thus,
\end{aligned}$$

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

Corollary 5(BCT^2): Let F be $(x, y) \xrightarrow{F} (x, x \boxplus y)$, an element of BCT^2 [10] defined as

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

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

$$\begin{aligned}
&M_{d[i]}[Out, In] \\
=&Df^{1,1}_{Out,In}((\alpha[i], \beta[i]), (0,0), \{(0,1), (0, \overline{\theta[i]}), (0, \zeta[i])\}, \{(0,1), (\alpha[i], \overline{\gamma[i]}), (\beta[i], \lambda[i])\}) \\
=&\#\left\{(x,y)\ \middle|\ \begin{array}{c} \lambda[i] \oplus \theta[i] \oplus \gamma[i] \oplus \zeta[i] \oplus e_4 \oplus e_3 \oplus e_1 \oplus e_2 = 0, \\ \theta[i] \oplus \gamma[i] = 0,\ carry_{e_1}(y,x)[1] = o_1, \\ carry_{e_2}(y \oplus x \oplus e_1 \oplus \zeta[i], x \oplus 1 \oplus \theta[i])[1] = o_2, \\ carry_{e_3}(y \oplus \beta[i], x \oplus \alpha[i])[1] = o_3, \\ carry_{e_4}(y \oplus \beta[i] \oplus x \oplus \alpha[i] \oplus e_3 \oplus \lambda[i], x \oplus 1 \oplus \alpha[i] \oplus \gamma[i])[1] = o_4; \\ where\ carry_e(x,y)[1] = (x \wedge y) \oplus (x \wedge e) \oplus (e \wedge y);\ x, y, \in F^2. \end{array}\right\} \\
&where\ 0 \le Out, In \le 15. Thus,
\end{aligned}$$

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

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 [5] defined by

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

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

$Q = (0,0,0,0,0,1,0,\cdots,0) \in F_2^{16}$. And the $M_{d[i]} \in F_2^{16\times 16}$ is defined as

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

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

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

Corollary 6-2:(IDBT) Let F be $(x,y)\xrightarrow{F}(x, x\boxplus y)$, an element of DBT [5] defined by

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

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

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

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

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

3. The formula for calculating the difference probability :
Corollary 7:(DDT) Let S be $S(x,y)=x\boxplus y$, an element of DDT [1] defined by

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

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 $M_{d[i]}\in F_2^{4\times 4}$ is defined as

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

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

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

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 [4] defined by

$$DLCT(\alpha,\beta,\lambda) = 2^{-2n}\cdot\sum_{x,y\in F_2^n}(-1)^{\lambda\cdot(S(x\oplus\alpha,y\oplus\beta)\oplus S(x,y))}$$

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

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

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

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

$$DLCT(\alpha,\beta,\lambda) = 2^{-2n}\cdot L\prod_{i=0}^{n-1} M_{a[i]}\,Q^T$$

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 [2] defined by

$$LAT(\mu,\omega,\lambda) = 2^{-2n}\cdot\sum_{x,y\in F_2^n}(-1)^{\mu\cdot x\oplus\omega\cdot y\oplus\lambda\cdot S(x,y)}$$

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 $M_{a[i]}\in F_2^{2\times2}$ is defined as

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

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

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

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

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 [10] defined as

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

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

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

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

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

Corollary 11(DBT^1): Let F be $(x,y) \xrightarrow{F} (x, x \boxplus y)$, an element of DBT^1 [10] defined as

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

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

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

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

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

References

[1] Eli Biham and Adi Shamir. Di erential cryptanalysis of des-like cryptosystems. 1990.

[2] Mitsuru Matsui. On correlation between the order of s-boxes and the strength of des. In *Workshop on Advances in Cryptology-eurocrypt*, 1994.

[3] Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. Cryptology ePrint Archive, Report 2018/161, 2018. https://eprint.iacr.org/2018/161.

[4] Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman. Dlct: A new tool for differential-linear cryptanalysis. Cryptology ePrint Archive, Report 2019/256, 2019. https://eprint.iacr.org/2019/256.

[5] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. application to aes variants and deoxys. 2019.

[6] Helger Lipmaa and Shiho Moriai. Efficient algorithms for computing differential properties of addition. In Mitsuru Matsui, editor, *Fast Software Encryption, 8th International Workshop, FSE 2001 Yokohama, Japan, April 2-4, 2001, Revised Papers*, volume 2355 of *Lecture Notes in Computer Science*, pages 336–350. Springer, 2001.

[7] Johan Wallén. Linear approximations of addition modulo 2^n . In *FSE*, pages 274–289, 2003.

[8] Ernst Schulte-Geers. On ccz-equivalence of addition mod 2^n. *Designs Codes, Cryptography*, 66(1-3):111–127, 2013.

[9] Anne Canteaut, Lukas Kölsch, and Friedrich Wiemer. Observations on the dlct and absolute indicators. Cryptology ePrint Archive, Report 2019/848, 2019. https://eprint.iacr.org/2019/848.

[10] Hosein Hadipour, Nasour Bagheri, and Ling Song. Improved rectangle attacks on skinny and craft. Cryptology ePrint Archive, Report 2020/1317, 2020. https://eprint.iacr.org/2020/1317.

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 $r_1, \cdots, r_z$, supposed that $1 \le j_1 \le j_2 \le z$, $deg \le r_{j_1}, r_{j_2}$, where $d = \sum_{i=1}^{z} r_i$, 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 $1 \le j \le z$, $0 \le j \le q-1$. And there are two basic function series ,of which code are j_1, j_2 respectively, are similar. Then we define the degree of similarity for the two basic function series is deg. Supposed that $G_0 \in F_2^{n\times 2}$, $G_j \in F_2^{n\times r_j}$, $1 \le j \le z$; $C = (J, N) \in (F_2^{n\times q\cdot t}, F_2^{n\times q\cdot t})$, $Out, In_1 \in F_2^d$, $In \in Sim_{deg}^{j_1,j_2}$, where $d = \sum_{i=0}^{z} k_{r_i}$, $In = (E_{k_{r_1},1}, \cdots E_{k_{r_z},z})$. Let $C = (J, N) = C_q^1 = (J_q^1, N_q^1)$. We have:

$$Df_{In}^{q,n}(C, G_0, G_j, A_{k_{r_j},j}^q, B_{k_{r_j},j}^q,\ 1 \le j \le z) = L \prod_{i=0}^{q-1} Md^i\ Q^T$$

where $L = (1, 1, \cdots, 1) \in F_2^{d-deg}$, $Q \in F_2^{d-deg}$, of which the sole nonzero component satisfies $Q[F(In)] = 1$, and $Md^i \in R^{(d-deg)\times(d-deg)}$ satisfying $Md^i[out, in] = \#Df_{F^{-1}(out),F^{-1}(in)}^{1,n}(C_i^2, G_0, G_j, T_{k_{r_j},j}^i, D_{k_{r_j},j}^i,\ 1 \le j \le z)$, $0 \le i \le q-1$, $0 \le out, in \le 2^{d-deg} - 1$.

Proof. According to the **remark 5**, for $1 \le i \le q$, we have :
$Df_{Out,In}^{i,n}(C_i^1, G_0, G_j, A_{k_{r_j},j}^i, B_{k_{r_j},j}^i,\ 1 \le j \le z) = 0$, when $in \notin Sim_{deg}^{j_1,j_2}$ and $out \in Sim_{deg}^{j_1,j_2}$.
$Df_{Out,In}^{i,n}(C_i^1, G_0, G_j, A_{k_{r_j},j}^i, B_{k_{r_j},j}^i,\ 1 \le j \le z) = 0$, when $in \in Sim_{deg}^{j_1,j_2}$ and $out \notin Sim_{deg}^{j_1,j_2}$.
Thus, for $1 \le i \le q$, when $In \in Sim_{deg}^{j_1,j_2}$

$$\begin{aligned}&\sum_{Out\in Sim_{deg}^{j_1,j_2}} \#Df_{Out,In}^{i,n}(C_{i+1}^1, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z)\\ =&\#Df_{In}^{i,n}(C_{i+1}^1, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z)\end{aligned}$$

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

$$\begin{aligned}&\#Df_{Out,In}^{i+1,n}(C_{i+1}^1, G_0, G_j, A_{k_{r_j},j}^{i+1}, B_{k_{r_j},j}^{i+1},\ 1 \le j \le z)\\ =&\sum_{Mi\in Sim_{deg}^{j_1,j_2}} \#Df_{Out,Mi}^{1,n}(C_i^2, G_0, G_j, T_{k_{r_j},j}^i, D_{k_{r_j},j}^i,\ 1 \le j \le z)\\ &\times \#Df_{Mi,In}^{i,n}(C_i^1, G_0, G_j, A_{k_{r_j},j}^i, B_{k_{r_j},j}^i,\ 1 \le j \le z).\end{aligned}$$

Next, use the bijection F to transform $Sim_{deg}^{j_1,j_2}$ 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 $\{f(X^{1,q}, Y^{1,q})_{E_{k_{m,j}}, A_{k_{m,j}}^q, B_{k_{m,j}}^q};\ 1 \le m \le r_j\}_j(X^{1,q}, Y^{1,q} \in F_2^{q\cdot t})$, $1 \le j \le z$; then we can get $T_{k_{r_j},j}^i, D_{k_{r_j},j}^i \in (F_2^t)^{r_j}$ from $A_{k_{m,j}}^q, B_{k_{m,j}}^q$, where $1 \le j \le z$, $0 \le j \le q-1$. And there are two basic function series ,of which code are j_1, j_2 respectively, are similar. Then we define the degree of similarity for the two basic function series is deg. Supposed that $G_j \in F_2^{r_j}$, $1 \le j \le z$; $\gamma, \lambda, v, w \in F_2^{q\cdot t}$, $Out, In_1 \in F_2^d$, $In \in Sim_{deg}^{j_1,j_2}$, where $d = \sum_{i=0}^{z} k_{r_i}$, $In = (E_{k_{r_1},1}, \cdots E_{k_{r_z},z})$. Let $\lambda_q^1 = \lambda, \gamma_q^1 = \gamma, V_q^1 = v, W_q^1 = w$. We have:

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

where $L = (1, 1, \cdots, 1) \in F_2^{d-deg}$, $Q \in F_2^{d-deg}$, of which the sole nonzero component satisfies $Q[F(In)] = 1$, and $Md^i \in R^{(d-deg)\times(d-deg)}$ satisfying $Ma^i[out, in] = Cor_{F^{-1}(out),F^{-1}(in)}^1\begin{pmatrix} \gamma_i^2, \lambda_i^2, V_i^2, W_i^2, \\ T_{k_{r_j},j}^i, D_{k_{r_j},j}^i, G_j\ 1 \le j \le z\end{pmatrix}$, $0 \le i \le q-1$, $0 \le out, in \le 2^{d-deg} - 1$.

Proof. According to the **remark 5**, for $1 \le i \le q$, we have :
$Cor^i_{Out,In}\begin{pmatrix} \gamma_i^1, \lambda_i^1, V_i^1, W_i^1, \\ A^i_{k_{r_j},j}, B^i_{k_{r_j},j}, G_j,\ 1 \le j \le z \end{pmatrix} = 0$, when $in \notin Sim^{j_1,j_2}_{deg}$ 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. □