Two New Constructions of Resilient Boolean Functions Satisfying Propagation Criterion

Chin-Hsin Lin, Shi-Chun Tsai, Rong-Jaye Chen
Department of Computer Science and Information Engineering
National Chiao-Tung University, R.O.C.
lincs@csie.nctu.edu.tw

June 20, 2002

Abstract

Recently the relationships among cryptographic criteria of boolean functions, including balancedness, the algebraic degree, nonlinearity, propagation criterion and correlation immunity, have been widely investagated. In this paper, we will present two constructions of n-variable boolean functions under consideration of resiliency and propagation criterion simultaneously.

1 Introduction

Symmetric-key cryptography system is the most widely used by industrial, financial and commercial sectors all over the world. It has many advantages of high performance, low cost implementation, and easy encryption or decryption. Usually, the Symmetric-key cryptography system can be roughly divided into two classes, block ciphers and stream ciphers. The former contains AES(Advanced Encryption System), RC6, DES and so on, whereas the LFRS-based stream cipher and SEAL belong to the latter. Although there are lots of different cipher systems, a core component of these systems is the cryptographic boolean functions. So the design and analysis of the cryptographic boolean functions is vitally important.

In the design of a good cryptographic boolean function, the following criteria of the cryptographic boolean functions are considered: (1)**algebraic degree**, (2)**balancedness**, (3)**correlation immunity**, (4)**nonlinearity**, and (5)**propagation criterion**.

Among these criteria, most researches focus on nonlinearity, correlation immunity, propagation criterion and their relationships. In [PLL$^+$90], Linden et al show the relation between the Walsh-Hadamard transformation and an n-variable boolean function satisfying the propagation criterion with degree t, denoted with $PC(t)$ which means if f changes with probability $\frac{1}{2}$ whenever the input x changes at least one and most t coordinates. A general method given in [KT97] uses linear codes to design functions satisfying $PC(t)$. In recent researches, the explicit and simple lower bound on the nonlinearity N_f of f with $PC(1)$ is established in [ZZ00],i.e., $N_f \geq 2^{n-1} - 2^{n-1-\frac{1}{2}}$.

Correlation immunity, introduced by Siegenthaler in 1984 [T.S84], has long been one of critical indicator of the cryptographic boolean function on stream cipher. A boolean function f with n-variables is called the m-th-order correlation immune function if when we keep m variables of input constant, the statistical distribution of output is equivalent to the statistical distribution of f. If f is the m-th order correlation immune function and is balanced, f is also called an m-resilient function. The spectral analysis of a boolean function f satisfying correlation immunity of order m was first presented in [GZM88a]. Moreover, the designs of the boolean functions with good correlation immunity have been proposed in [SZZ93][CLLS96]. And the upper bound of nonlinearity, $N_f \leq 2^{n-1} - 2^{n-1-\frac{t}{2}}$, is characterized in [Sar00].

The propagation criterion goes against correlation immunity and the same situation exists between correlation immunity and nonlinearity. So there is no boolean functions satisfying all of good criteria we mentioned above. As a consequence, the relationships between these criteria have been widely investigated. If f is m-th order correlation immune, nonlinearity $N_f \leq 2^{n-1} - 2^m$ for $m > \frac{n}{2} - 1$ and $N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^m$ for $m \leq \frac{n}{2} - 1$ [Sar00]. The relationship between the order of correlation immunity ,m, and the degree of propagation criterion, t, have been provided in [Car93] and [ZZ01]. Moreover, the upper bound of sum of m and t, $m + t \leq n$, has been shown in [ZZ00].

This paper, we want to established a construction of an n-variable boolean function under of consideration of balancedness, the correlation immunity and propagation criterion simultaneously. We present two new constructions for this idea. One is to modified the construction of a boolean function which is balanced and m-th order correlation immune [CLLS96], and the other is through the concept of the equivalence class of boolean functions [BW74]. We also present the link between the equivalence class of boolean functions and cryptographic criteria.

The organization of the rest of the paper is as follows. In Section 2, we provide the basic definitions and notations and show the definition of the Walsh-Hadamard transform. It is the most powerful tool for analyzing boolean functions. We use this tool to describe the definitions and properties of cryptographic criteria. In Section 3, we present a new construction of n-variable and m-resilient boolean function which also satisfies $PC(t)$. Then we introduce the concept of equivalence classes of boolean functions. Based on this, we present another new construction of n-variable and m-resilient boolean function which also satisfies $PC(t)$.

2 Preliminaries and Notations

This section will provide some notations and definitions. We also introduce the cryptographic criteria and the powerful tool–Walsh-Hadamard Transform.

2.1 Boolean functions

We say f is an n-variable boolean function if f is the function from $\{0,1\}^n$ to $\{0,1\}$ ($f : \{0,1\}^n \mapsto \{0,1\}$). For convenience, we use $f(x)$ to represent f with n input variables, $f(x) = f(x_1, x_2, \ldots, x_n)$. The truth table of f is a (0,1)-valued row vector with length 2^n, denoted by $\xi_f = (f(\gamma_0), f(\gamma_1), \ldots, f(\gamma_{2^n-1}))$ where $\gamma_0 = (0,0,\ldots,0)$, $\gamma_1 = (1,0,\ldots,0)$, $\ldots$, and $\gamma_{2^n-1} = (1,1,\ldots,1)$.

Definition 2.1. *Let v_1 and v_2 be the binary vectors of length n. The Hamming weight of the vector is denoted by $hw(v_1)$, the number of 1's in the vector v_1. We denote by $\#(v_1 = v_2)$ (respectively $\#(v_1 \neq v_2)$), the number of places where v_1 and v_2 are equal(respectively unequal). The Hamming distance between v_1 and v_2 is denoted by $hd(v_1, v_2)$, i.e.*

$$hd(v_1, v_2) = \#(v_1 \neq v_2) = hw(v_1 \oplus v_2)$$

Note that we denote bit-wise XOR operator over by $\oplus$.

Besides truth table of f, the following form also can be represent the n-variable function $f(x_1, x_2, ..., x_n)$. It is called algebraic normal(ANF) form:

$$f(x_1, x_2, ..., x_n) = \bigoplus_{u \in \{0,1\}^n} \varphi(u) x_1^{u_1} x_2^{u_2} \dots x_n^{u_n}$$

where the coefficient $\varphi(u) \in \{0, 1\}$ and $u = (u_1, u_2, \dots, u_n)$.

The $deg(f)$ is the algebraic degree, the number of variables of highest order product term with nonzero coefficient in the algebraic normal form.

We call an n-variable function f is an affine function if $deg(f) \leq 1$. It takes the ANF form: $\varphi(\gamma) = 0$ for $hw(\gamma) \geq 2$. Furthermore, f is called the linear function if the constant term $\varphi(\gamma_0)$ is also zero.

2.2 Walsh-Hadamard Transform

Definition 2.2. *Let f be a function on $\{0, 1\}^n$. The Walsh-Hadamard transform of $f(x)$ is defined as*

$$W_f(\omega) = \sum_{x \in 0,1^n} (-1)^{f(x) \oplus <\omega, x>}$$

where $\omega = (\omega_1, \omega_2, ..., \omega_n) \in \{0, 1\}^n$, $< \omega, x >$ is the inner product of ω and x, $< \omega, x >= \bigoplus_{i=1}^n \omega_i x_i$. The Walsh-Hadamard transform is also called the spectral distribution or the spectrum of a boolean function.

The Walsh-Hadamard transform is mostly used in the analysis of an arbitrary boolean function. The value, $W_f(\omega)$, of transform can be viewed as the difference between f and some linear function $< \omega, x >$.

$$\begin{aligned} W_f(\omega) &= \sum_{x \in 0,1^n} (-1)^{f(x) \oplus <\omega, x>} \\ &= \#\{x | f(x) =< \omega, x >\} - \#\{x | f(x) \neq < \omega, x >\} \end{aligned}$$

2.3 Cryptographic Properties for Boolean Functions

2.3.1 Balanced functions

Definition 2.3. *f is an n-variable boolean function. f is the balanced function if*

$$\begin{aligned} \#\{x | f(x) = 1\} &= \#\{x | f(x) = 0\} \\ hw(\xi_f) &= 2^{n-1}. \end{aligned}$$

Lemma 2.4. *Let f be a balanced boolean function. The Walsh-Hadamard transform of f is zero at $\omega = (0, \dots, 0)$, $W_f(0, \dots, 0) = 0$.*

2.3.2 Nonlinearity

The nonlinearity of f is defined to be the minimum Hamming distance between f and all affine functions.

Definition 2.5. *Let f be an n-variable boolean function. The nonlinearity of f, denoted by N_f, is defined as*

$$N_f = \min_{g \in A(n)} hd(\xi_f, \xi_g)$$

where $A(n)$ is the set of all n-variable affine functions.

According to the definition, we know that a boolean function with high nonlinearity is difficult to approximate with some affine function. The value of N_f is also formed by the Walsh-Hadamard transform. Let $L(n)$ be the set of all n-variable linear functions. $L(n)$ is the subset of $A(n)$. Then

$$N_f \quad = \quad 2^{n-1} - \max_{\omega \in \{0,1\}^n} \frac{|W_f(\omega)|}{2}.$$

2.3.3 Correlation Immune and Resilient Boolean functions

Siegenthaler has defined the correlation immunity [T.S84] as a measure of resistance against the ciphertext-only correlation attacks in stream cipher [T.S85]. A boolean function f with n-variables is called the m-th-order correlation immune function if the statistical distribution of output is equivalent to the statistical distribution of f when we keep m variables of input constant. If f is also balanced, then f is called the m-resilient function. Xiao and Massey present the characterization of correlation immune functions on Walsh-Hadamard transform [GZM88a] as follows:

Theorem 2.6. *[GZM88a]An n-variable boolean function is m-th order correlation immune if and only if its Walsh-Hadamard transform W_f satisfies*

$$W_f(\omega) = 0, \textit{ for } 1 \leq hw(\omega) \leq m$$

Moreover, if f is m-resilient resilient then

$$W_f(\omega) = 0, \textit{ for } 0 \leq hw(\omega) \leq m$$

Lemma 2.7. *[T.S84][GZM88a] Let f be an m-th order correlation immune function with n variables. For $m < n - 1$, the maximum algebraic degree of f is $n - m$ and if f is m-resilient then the maximum algebraic degree of f is $n - m - 1$. For $m = n - 1$, f is an n-variable affine function.*

2.3.4 Propagation Criterion

Definition 2.8. *Let f be an n-variable boolean function. The autocorrelation function $R_f(\alpha)$ is defined as*

$$R_f(\alpha) = \sum_x (-1)^{f(x) \oplus f(x \oplus \alpha)}$$

Note that $R_f(0^n)$ is equal to 2^n

An n-variable boolean function f satisfies the propagation criterion with degree t if $f(x)$ changes with a probability of $\frac{1}{2}$ whenever i$(1 \leq i \leq t)$ variables of input are complemented [PLL$^+$90]. Specifically, f is said to satisfy the propagation criterion with degree t if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function for $1 \leq hw(\alpha) \leq t$. We note that $f(x) \oplus f(x \oplus \alpha)$ is also called the directional derivative of f in the direction α.

Definition 2.9. *Let f be an n-variable boolean function satisfying the propagation criterion with degree k. The autocorrelation function $R_f(\alpha)$:*

$$R_f(\alpha) = 0 \text{ for } 1 \leq hw(\alpha) \leq t$$

The *strict avalanche criterion(SAC)* [GZM88b] is equivalent to the propagation criterion with degree 1 and *perfect non-linear* is propagation criterion with degree n.

3 Construction

We have known that propagation criterion will goes against the correlation immunity and nonlinearity. In this section, these important cryptographic properties (resiliency, nonlinearity , propagation criterion and algebraic degree) will be considered simultaneously for the two new construction of a boolean function.

3.1 Construction I

In [SM00], Sarkar and Maitra provided the construction of n-variable and 1-resilient functions satisfying $PC(\frac{n}{2}-1)$, by using $(n-2)$-variable boolean functions which satisfies $PC(n-2)$. We call this construction as **PC-based Construction**. It generates an 1-resilient boolean function satisfying $PC(\frac{1}{2}-1)$, which $def(f) = \frac{n}{2}-1$ and $N_f = 2^{n-1} - 2^{\frac{n}{2}}$.

Now we propose our new method different from **PC-based Construction** , namely **Resilient-based Construction**, to construct an n-variable and m-resilient boolean function which has the algebraic degree d, maximal nonlinearity $N_f = 2^{n-1} - 2^{n-d}$, and satisfies $PC(1)$. This **Resilient-based Construction** is made by modifying the construction of m-resilient functions in [CLLS96]. At first, we introduce an important theorem of this construction.

Theorem 3.1. *[CLLS96] Let n, m and k be three positive integers with $n \geq 4$, $1 \leq m \leq n-3$, $1 \leq k \leq n-m$ and $S_{n,m,k} = \{A_y \mid A_y \in \{0,1\}^k$ where $hw(A_y) \geq m+1$ and $y \in \{0,1\}^{n-k}\}$. For any $a \in S_{n,m,k}$, let $u_a = \#\{y \mid A_y = a$ and $y \in \{0,1\}^{n-k}\}$ and $u = \max_a u_a$. We define a boolean function $f : \{0,1\}^n \to \{0,1\}$ by*

$$\begin{aligned} f(y,x) &= (1 \oplus y_1)(1 \oplus y_2)...(1 \oplus y_{n-k}) < A_{\eta_0}, x > \oplus \\ &\quad (1 \oplus y_1)(1 \oplus y_2)...(y_{n-k}) < A_{\eta_1}, x > \oplus \\ &\quad ...... \oplus \\ &\quad (y_1 y_2 ... y_{n-k}) < A_{\eta_{2^{n-k}-1}}, x > \end{aligned}$$

where $y = (y_1, y_2, ..., y_{n-k}) \in \{0,1\}^{n-k}$, $x = (x_1, x_2, ..., x_k) \in \{0,1\}^k$ and $\eta_i \in \{0,1\}^{n-k}$ is the binary representation of i. Then the following conditions hold:

1. *f is balanced.*
2. *f is an m-th order correlation immune function.*
3. *$N_f = 2^{n-1} - u2^{k-1}$.*
4. *If $\bigoplus_{y \in \{0,1\}^{n-k}} A_y$ is not equal to zero vector then $deg(f) = n-k+1$.*

Lemma 3.2. *[CLLS96] Let f be an n-variable boolean function constructed by Theorem3.1. When $u = \max_a u_a = 1$ and $k = b_1$ where b_1 is defined in Theorem* **??***, we can obtain the maximum nonlinearity*

$$\max_{u,k} N_f = 2^{n-1} - \min_{u,k} u2^{k-1} = 2^{n-1} - 2^{b_1-1} = 2^{n-1} - 2^{k-1}$$

We now take the propagation criterion into consideration and extend Theorem 3.1 to build the **Resilient-based Construction**. The following theorem is an important result for **Resilient-based Construction**.

Theorem 3.3. *Let $f(y_1, y_2, ..., y_{n-k}, x_1, x_2, \dots, x_k)$ be an n-variable and m-resilient boolean function with parameter k. $\eta_i \in \{0,1\}^{n-k}$ is denoted by a binary representation of decimal number i. We say that f satisfies PC(1) if the following conditions hold:*

1. *$\{A_y \mid A_y \in \{0,1\}^k$ wherehw$(A_y) \geq m+1$ and $y \in \{0,1\}^{n-k}\}$*
2. *Let e_j be the boolean vector with length $n-k$ of which the j-th positions is one and the others is zero. Then $< A_y, x > \oplus < A_{y \oplus e_j}, x >$ is not a constant function for $1 \leq j \leq k$ and $y \in \{0,1\}^{n-k}$.*
3. *The sequence $(A_{\eta_0}(i), A_{\eta_1}(i), ..., A_{\eta_{2^{n-k}-1}}(i))$ is balanced for $1 \leq i \leq k$, where $A_y(i)$ means i-th position of the vector A_y. In other words,*

$$\sum_{y \in \{0,1\}^{n-k}} A_y(i) = 2^{n-k-1}$$

Proof. From Theorem 3.1, f is m-resilient functions for condition 1. Next, We define

$$\begin{aligned} g_{y_s} &= f(y_1, ..., y_s \oplus 1, ..., y_{n-k}, x_1, ..., x_k) \\ g_{x_r} &= f(y_1, ..., y_{n-k}, x_1, ..., x_r \oplus 1, ..., x_k) \end{aligned}$$

If $f(y_1, y_2, ..., y_{n-k}, x_1, x_2, ..., x_k)$ satisfies $PC(1)$, we must prove that $f \oplus g_{y_s}$ for $1 \leq s \leq n-k$ and $f \oplus g_{x_r}$ for $1 \leq r \leq k$ are both balanced functions. At first, we consider the condition of $f \oplus g_{y_s}$ for $1 \leq s \leq n-k$.

$$\begin{aligned} f \oplus g_{y_s} &= f(y_1, y_2, ..., y_{n-k}, x_1, x_2, ..., x_k) \oplus f(y_1, ..., y_s \oplus 1, ..., y_{n-k}, x_1, ..., x_k) \\ &= (1 \oplus y_1)(1 \oplus y_2) \dots (1 \oplus y_{n-k}) < (A_{\eta_0} \oplus A_{\eta_0 \oplus e_s}), x > \\ &\quad (1 \oplus y_1)(1 \oplus y_2) \dots (y_{n-k}) < (A_{\eta_1} \oplus A_{\eta_1 \oplus e_s}), x > \oplus \\ &\quad ...... \oplus \\ &\quad (y_1 y_2 \dots y_{n-k}) < (A_{\eta_{2^{n-k}-1}} \oplus A_{\eta_{2^{n-k}-1} \oplus e_s}), x > \end{aligned}$$

Because $< (A_{\eta_i} \oplus A_{\eta_i \oplus e_s}), x >$ is not a constant function, from the proof 1 of Theorem 3.1 we know $f \oplus g_{y_s}$ is balanced.

Next, for $f \oplus g_{x_r}$ where $1 \leq r \leq k$, we have

$$\begin{aligned} f \oplus g_{x_r} &= f(y_1, y_2, ..., y_{n-k}, x_1, x_2, ..., x_k) \oplus f(y_1, ..., y_{n-k}, x_1, ..., x_r \oplus 1 ..., x_k) \\ &= (1 \oplus y_1)(1 \oplus y_2) ... (1 \oplus y_{n-k}) A_{\eta_0}(r) \\ &\quad (1 \oplus y_1)(1 \oplus y_2) ... (y_{n-k}) A_{\eta_1}(r) \oplus \\ &\quad ...... \oplus \\ &\quad (y_1 y_2 ... y_{n-k}) A_{\eta_{2^{n-k}-1}}(r) \end{aligned}$$

Since the vector $(A_{\eta_0}(r), A_{\eta_1}(r), ..., A_{\eta_{2^{n-k}-1}}(r))$ is balanced for all $1 \leq r \leq k$, thus $f \oplus g_{x_r}$ is balanced.

Then we have completed the proof. □

A boolean function f constructed by **Resilient-based Construction**, the nonlinearity is $2^{n-1} - u2^{k-1}$. From Lemma 3.2, when $u = 1$ (i.e. $A_{\eta_i} \neq A_{\eta_j}$ for all $i \neq j$ and A_{η_i},$A_{\eta_j} \in S_{n,m,k}$), we can obtain the maximal nonlinearity which is only determined by k. Next lemma will show what relation exists among n, m, k in **Resilient-based Construction**.

Lemma 3.4. *Let n, m, k be positive integers. If an n-variable and m-resilient boolean function $f(y, x)$ satisfying PC(1) is generated by* ***Resilient-based Construction****, then* $n \geq 5$, $1 \leq m \leq \lfloor \frac{n-3}{2} \rfloor$ *and* $\max\{2m + 2, \lfloor \frac{n}{2} \rfloor + 1\} \leq k \leq n - 1$.

Proof. We choose parameter k and thus $f(y, x)$ is the form of $f(y_1\ , y_2,\ldots, y_{n-k}, x_1, x_2,\ldots\ ,x_k)$. We know that if the set $S_{n,m,k}$ defined in Theorem 3.1 meets the two conditions mentioned in Theorem 3.3, an m-resilient boolean function $f(y, x)$ satisfying PC(1) can be constructed. For the first condition, we can pick out the distinct vectors to make the set $S_{n,m,k}$. At the same time, the nonlinearity of f is maximal. For the second condition, the $(A_{\eta_0}(t), A_{\eta_1}(t), ..., A_{\eta_{2^{n-k}-1}}(t))$ must be balanced for all $1 \leq t \leq k$. This means the sum of Hamming weight of A_y is $k2^{n-k-1}$.And the Hamming weight of A_y is greater than or equal to $m + 1$ for $y \in \{0, 1\}^{n-k}$. So we have

$$hw(A_y) \geq m + 1 \text{ and } \textstyle\sum_y hw(A_y) = k2^{n-k-1}$$
$$(m + 1)2^{n-k} \leq k2^{n-k-1}$$
$$2m + 2 \leq k$$

Since vectors in the set $S_{n,m,k}$ are distinct, $u = 1$ and k must meet the condition:

$$\binom{k}{m+1} + \binom{k}{m+2} + \ldots + \binom{k}{k} \geq 2^{n-k}$$

Then

$$2^k - 2^{n-k} \geq \binom{k}{0} + \binom{k}{1} + \ldots + \binom{k}{m}$$

Therefore, $k > n - k$ and $k \geq \lfloor \frac{n}{2} \rfloor + 1$.

For $k = n$, $f(y, x) = f(x_1, x_2, ..., x_n) =< A_{\eta_0}, x >$ is an linear function and $f(y, x)$ will not satisfy $PC(1)$. Therefore, k is at most $n - 1$. So $\max\{2m + 2, \lfloor \frac{n}{2} \rfloor + 1\} \leq k \leq n - 1$ and we can deduce that $n \geq 5$, $1 \leq m \leq \lfloor \frac{n-3}{2} \rfloor$. □

Lemma 3.5. *A boolean function $f(y, x)$ constructed by* ***Resilient-based Construction*** *with parameter k has the algebraic degree at most $n - k$.*

Proof. From the condition 2 of Theorem 3.3, we know that $\sum_{y\in\{0,1\}^{n-k}} A_y$ is a zero vector. In the ANF of $f(y, x)$, there is no product term $y_1y_2 \ldots y_{n-k}x_i$ for $1 \leq i \leq k$. So algebraic degree of f is at most $n - k$. When $deg(f) = n - k$, the following condition holds:

$$\bigoplus_{\eta_i \leq \eta_j} A_{\eta i} \text{ is not the zero vctor where } hw(\eta_j) = n - k - 1$$

where $\eta_i \leq \eta_j$ means $\eta_i(i)$ implies $\eta_j(i)$. □

Now we use an example to explain this method. Suppose we want to construct a 6-variable and 1-resilient boolean function which satisfies PC(1), then

Step 1. $n = 6$ and $m = 1$, the condition for m and n holds.

Step 2. Then $\max\{2m+2, \lfloor \frac{n}{2} \rfloor + 1\} \leq k$, and we know $4 \leq k \leq 5$. Since $\left(\begin{array}{c} 4 \\ 2 \end{array}\right) + \left(\begin{array}{c} 4 \\ 3 \end{array}\right) + \left(\begin{array}{c} 4 \\ 4 \end{array}\right) > 2^{6-4}$, we have $k = 4$.

Step 3. Choose 4 balanced vectors with length 2^{6-4} to be columns of matrix $\mathcal{A}_{n,m,k}$,

$$\mathcal{A}_{6,1,4} = \begin{bmatrix} A_{\eta 0} \\ A_{\eta 1} \\ A_{\eta 2} \\ A_{\eta 3} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Then check if $A_{\eta 0} \neq A_{\eta 1} \neq A_{\eta 2} \neq A_{\eta 3}$ and $hw(A_{\eta_i}) \geq 2$ for $i = 0, 1, 2, 3$. We find the Hamming weight of $A_{\eta 2} = [0, 0, 0, 1]$ is 1 and adjust the first column of $\mathcal{A}_{6,1,4}$ with the vector $[1, 0, 1, 0]^T$. So we have

$$\mathcal{A}_{6,1,4} = \begin{bmatrix} A_{\eta 0} \\ A_{\eta 1} \\ A_{\eta 2} \\ A_{\eta 3} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Step 4. Construct $f(y, x)$ as follows:

$$\begin{aligned} f(y,x) \quad = \quad & (1 \oplus y_1)(1 \oplus y_2)(x_1 \oplus x_2) \oplus \\ & (1 \oplus y_1)(y_2)(x_1 \oplus x_2) \oplus \\ & (y_1)(1 \oplus y_2))(x_1 \oplus x_4) \oplus \\ & (y_1 y_2)(x_3 \oplus x_4) \end{aligned}$$

Then $f(y, x)$ is 1-resilient function and satisfies $PC(1)$. Since $\sum_{\eta_i \leq \eta_1} A_{\eta_i} = A_{\eta 0} \oplus A_{\eta 1} = (1, 0, 1, 0)$ and $\sum_{\eta_i \leq \eta_2} A_i = A_{\eta 0} \oplus A_{\eta 2} = (0, 1, 0, 1)$, then the algebraic degree of f is 2.

For the following theorem, we can extend the Theorem 3.3 to **Extended-Resilient-Based Construction**. By this construction, an n-variable and m-resilient boolean function f is generated. Moreover, f satisfies $PC(t)$.

Theorem 3.6. *Let $f(y_1, y_2, ..., y_{n-k}, x_1, x_2, \ldots, x_k)$ be an n-variable and m-resilient boolean with parameter k. f is generated by Theorem 3.1. And $\alpha = (b, a)$ is a boolean vector with length n where $b \in \{0, 1\}^{n-k}$ and $a \in \{0, 1\}^k$. We say that f satisfies $PC(t)$ if the following conditions hold:*

1. *$< A_y, x > \oplus < A_{y \oplus b}, x >$ is not a constant function for $1 \leq hw(b) \leq \min\{n - k, t\}$ and $y \in \{0, 1\}^{n-k}$.*

2. *The sequence ($< A_{\eta 0}, a >$, $< A_{\eta 1}, a >$, $\ldots$, $< A_{\eta_{2^{n-k}-1}}, a >$) is balanced for $1 \leq hw(a) \leq \min\{k, t\}$. In other words,*

$$\sum_{y \in \{0,1\}^{n-k}} < A_y, a >= 2^{n-k-1} \text{ for } 1 \leq hw(a) \leq \min\{k, t\}$$

Proof. From the definition of $PC(t)$, we know if f satisfies $PC(t)$ then $f(y,x)\oplus f(y\oplus\alpha_{n-k},x\oplus\alpha_k)$ is balanced for $1\le hw(\alpha)\le t$. Then

$$\begin{array}{rl} & f(y,x)\oplus f(y\oplus b,x\oplus a)\\ = & (1\oplus y_1)(1\oplus y_2)\ldots(1\oplus y_{n-k})(<(A_{\eta0}\oplus A_{\eta0\oplus b}),x>\oplus<A_{\eta0\oplus b},a>)\oplus\\ & (1\oplus y_1)(1\oplus y_2)\ldots(y_{n-k})(<(A_{\eta1}\oplus A_{\eta1\oplus b}),x>\oplus<A_{\eta1\oplus b},a>)\oplus\\ & \ldots\ldots\oplus\\ & (y_1y_2\ldots y_{n-k})<(A_{\eta_{2^{n-k}-1}}\oplus(A_{\eta_{2^{n-k}-1}\oplus b}),x>\oplus<A_{\eta_{2^{n-k}-1}\oplus b},a>) \end{array}$$

Then we consider the following:

case (i). b **is not a zero vector**. We know that $<A_{\eta_i},x>\oplus<A_{\eta_i\oplus b}¿$ is not a constant function for $1\le hw(b)\le\min\{n-k,t\}$. Therefore, no matter what a is, $(<(A_{\eta_i}\oplus A_{\eta_i\oplus b}),x>\oplus<A_{\eta_i\oplus b},a>)$ is always a balanced function. So $f(y,x)\oplus f(y\oplus b,x\oplus a)$ is balanced.

case (ii). b **is a zero vector**. So $<(A_{\eta_i}\oplus A_{\eta_i\oplus b}),x>$ is a constant function. Then

$$\begin{array}{rcl} f(y,x)\oplus f(y\oplus b,x\oplus a) & = & f(y,x)\oplus f(y,x\oplus a)\\ & = & (1\oplus y_1)(1\oplus y_2)\ldots(1\oplus y_{n-k})(<A_{\eta_0},a>)\oplus\\ & & (1\oplus y_1)(1\oplus y_2)\ldots(y_{n-k})(<A_{\eta_1},a>)\oplus\\ & & \ldots\ldots\oplus\\ & & (y_1y_2\ldots y_{n-k})\oplus(<A_{\eta_{2^{n-k}-1}},a>) \end{array}$$

From the condition 2, we know $\bigoplus_{y\in\{0,1\}^{n-k}}<A_y,a>=0$ for $1\le hw(a)\le\min\{k,t\}$. So $f(y,x)\oplus f(y,x\oplus a)$ is balanced for $1\le hw(a)\le\min\{k,t\}$.

Finally, we complete this proof. □

In the following example, we use the **Extended-Resilient-Based Construction** to generate a 9-variable and 1-resilient boolean function $f(y,x)$ which satisfies $PC(2)$. First of all, we decide parameter k. From Lemma 3.4 we know $2\times1+2\le k\le 9-1$ and

$$k=5\quad\binom{5}{2}+\binom{5}{3}+\binom{5}{4}+\binom{5}{5}\ge 2^{9-5}$$

We use the computer to search $2^{9-5}\times 5$ matrix $\mathcal{A}_{9,1,5}$. But $\mathcal{A}_{9,1,5}$ which follows the conditions defined in Lemma **??** and $hw(A_{\eta_i})\ge 2$, is not found when $k=5$. So k is assigned to 6 and we find $2^{9-6}\times 6$ matrix $S_{9,1,6}$:

$$\mathcal{A}_{9,1,6}=\begin{bmatrix}A_{\eta_0}\\A_{\eta_1}\\A_{\eta_2}\\A_{\eta_3}\\A_{\eta_4}\\A_{\eta_5}\\A_{\eta_6}\\A_{\eta_7}\end{bmatrix}=\begin{bmatrix}0&0&1&0&1&0\\1&0&0&0&0&1\\0&1&0&0&1&1\\1&1&1&0&0&0\\0&0&1&1&0&1\\1&0&0&1&1&0\\0&1&0&1&0&0\\1&1&1&1&1&1\end{bmatrix}\text{,when } k=6$$

Thus we can use $\mathcal{A}_{9,1,6}$ to form $f(y,x)$:

$$\begin{aligned} f(y,x) &= (1\oplus y_1)(1\oplus y_2)(1\oplus y_3)(x_3\oplus x_5)\oplus \\ &\quad (1\oplus y_1)(1\oplus y_2)(y_3)(x_1\oplus x_6)\oplus \\ &\quad (1\oplus y_1)(y_2)(1\oplus y_3)(x_1\oplus x_5\oplus x_6)\oplus \\ &\quad (1\oplus y_1)(y_2)(y_3)(x_1\oplus x_2\oplus x_3)\oplus \\ &\quad (y_1)(1\oplus y_2)(1\oplus y_3)(x_3\oplus x_4\oplus x_6)\oplus \\ &\quad (y_1)(1\oplus y_2)(y_3)(x_1\oplus x_4\oplus x_5)\oplus \\ &\quad (y_1)(y_2)(1\oplus y_3)(x_2\oplus x_4)\oplus \\ &\quad (y_1)(y_2)(y_3)(x_1\oplus x_2\oplus x_3\oplus x_4\oplus x_5\oplus x_6) \end{aligned}$$

Therefore, a 9-variable and 1-resilient boolean function $f(y,x)$ is generated. $f(y,x)$ also satisfies $PC(2)$. It is easy to check that for some i and $hw(\eta_i)=2$, $\sum_{\eta_j\le\eta_i} A_{\eta_j}\neq 0$. Thus $def(f)=2$.The nonlinearity $N_f = 2^{9-1}-2^{6-1}=224$.

The **Extended-Resilient-Based Construction** is provided to construct an n-variable and m-resilient boolean function which satisfies $PC(t)$. Unfortunately, it is easy to find the matrix $\mathcal{A}_{n,m,k}$ for $t=1$ but not for $t\geq 2$. Form the previous example, we use the exhausting search to decide the matrix $\mathcal{A}_{n,m,k}$ which meets the conditions in Theorem **??**. It will be open problem of an efficient way to find the matrix $\mathcal{A}_{n,m,k}$ for the future research.

3.2 Construction II

We can construct an n-variable boolean function which is m-resilient and satisfies $PC(t)$ by **the PC-based Construction** or **Extended-Resilient-Based Construction**. However, these constructions can not cover all m-resilient functions which satisfy $PC(t)$ if functions really exist. For example, **the PC-based Construction** is useful only for n is even and $m=1$. And it is impossible that a 1-resilient boolean function which satisfies $PC(1)$ can be generated by **Extended-Resilient-Based Construction** when n is less than 4. So we want to know whether there exists a construction which can generate a boolean function for given cryptographic parameters such as balancedness, the degree of propagation criterion, the order of correlation immunity and nonlinearity. In this section, we present our idea through the equivalence class of boolean functions.

At first, we introduce the concept of equivalence classes of boolean functions. Consider two three-variable boolean functions

$$f(x_1,x_2,x_3) = x_1x_2$$

and

$$g(y_1,y_2,y_3) = y_2y_3\oplus y_2.$$

We observe that $f(x_1,x_2,x_3)$ and $g(y_1,y_2,y_3)$ are equivalent by match variables as $\{x_1\rightarrow y_2, x_2\rightarrow (y_3+1),\ x_3\rightarrow y_1\}$. Two boolean functions are equivalent if there exist input permutation and output shifted by an affine function that can transform one function to the other. In [BW74], the concept of equivalence classes is defined as follows:

Definition 3.7. *[BW74] Let f and g be n-variable boolean function and $f\neq g$. If f is equivalent to g, then there exists an invertible $n\times n$ matrix U ,two n-length binary vectors λ and β, and a binary value c such that*

$$g(x) = f(xU\oplus\lambda)\oplus <\beta,x>\oplus c$$

where $x = (x_1, x_2, \ldots, x_{2^n-1})$.

According to the above definition, we can divide the set of boolean functions with n variables into numerous equivalence classes $\mathcal{E}_{f_i}$. For any boolean function f_j in the equivalence class $\mathcal{E}_{f_i}$, f_j is equivalent to f_i. When n=3, we can find three equivalence classes:

$$\begin{array}{ll} \mathcal{E}_{f_1}: & f_1(x) = x_1x_2x_3 \\ \mathcal{E}_{f_2}: & f_2(x) = x_1x_2 \\ \mathcal{E}_{f_3}: & f_3(x) = 0 \end{array}$$

For $n = 4$ and $n = 5$, the equivalence classes are listed in Appendix A (Table 2 and Table 3). The following theorem will show the characteristic of the equivalence class for the Walsh-Hadamrad transform and the autocorrelation function.

Theorem 3.8. *Let f and g be n-variable boolean functions and f is equivalent to g.Then*

1. $W_g(\omega) = (-1)^{c\oplus<\beta\oplus\omega,\lambda U^{-1}>}W_f((\beta\oplus\omega)(U^{-1})^T)$.
2. $R_g(\alpha) = (-1)^{<\beta,\alpha>}R_f(\alpha U)$.

Proof. We know if f and g are in the same equivalence class. Then

$$g(x) = f(xU \oplus \lambda) \oplus < \beta, x > \oplus c$$

1. For Walsh-Hadamard transform of f and g,

$$\begin{aligned} W_g(\omega) &= \sum_{x\in\{0,1\}^n} (-1)^{g(x)\oplus<\omega,x>} \\ &= \sum_{x\in\{0,1\}^n} (-1)^{(f(xU\oplus\lambda)\oplus<\beta,x>\oplus c)\oplus<\omega,x>} \\ &= (-1)^c \sum_{x\in\{0,1\}^n} (-1)^{f(xU\oplus\lambda)\oplus<\beta\oplus\omega,x>} \\ &= (-1)^c \sum_{z\in\{0,1\}^n} (-1)^{f(z)\oplus<\beta\oplus\omega,(z\oplus\lambda)U^{-1}>} \\ &= (-1)^{c\oplus<\beta\oplus\omega,\lambda U^{-1}>} \sum_{z\in\{0,1\}^n} (-1)^{f(z)\oplus<(\beta\oplus\omega)(U^{-1})^T,z>} \\ &= (-1)^{c\oplus<\beta\oplus\omega,\lambda U^{-1}>}W_f((\beta\oplus\omega)(U^{-1})^T) \end{aligned}$$

2. For autocorrelation functions,

$$\begin{aligned} R_g(\alpha) &= \sum_{x\in\{0,1\}^n} (-1)^{g(x)\oplus g(x\oplus\alpha)} \\ &= \sum_{x\in\{0,1\}^n} (-1)^{f(xU\oplus\lambda)\oplus f((x\oplus\alpha)U\oplus\lambda)\oplus<\beta,\alpha>} \\ &= (-1)^{<\beta,\alpha>} \sum_{z\in\{0,1\}^n} (-1)^{f(z)\oplus f(z\oplus\alpha U)} \\ &= (-1)^{<\beta,\alpha>}R_f(\alpha U) \end{aligned}$$

□

From Theorem 3.8, we note that $W_g(\beta_i)$ may be equal to $W_f(\beta_j)$ or $-W_f(\beta_j)$ if f and g are in the same equivalence class. $|W_g(\omega)| \mapsto |W_f(\omega)|$ is an one-to-one and onto mapping. This is also true for the autocorrelation function of f and g. So we can further characterize the equivalence class by the following definition:

Definition 3.9. *Let $\mathcal{P}$ be a set of patterns and $\mathcal{P} = \{p_1, p_2, \ldots, p_l\}$ where p_i is positive integer or 0. A real-valued set , $S = \{s_1, s_2, \ldots, s_l\}$,with size l is $\mathcal{P}-$patterns if $\{|s_1|,|s_2|,\ldots,|s_l|\} = \mathcal{P}$.*

For example, let $\mathcal{P}$ be a pattern set with eight elements, $\mathcal{P} = \{0, 0, 0, 0, 0, 2, 2, 4\}$. Then $S_1 = \{0,\ 0,\ 0,\ 2,\ -4,\ 2,\ 0,\ 0\}$ is $\mathcal{P} - class$ while $S_2 = \{2,\ 0,\ 0,\ -2,\ 2,\ 0,\ 0,\ 0\}$ is not.

Now we define two pattern sets for a boolean function f_i as follows:

$$\begin{aligned} \mathcal{PW}_{f_i} &= \{|W_{f_i}(\omega)| \text{ for } \omega \in \{0,1\}^n\} \\ \mathcal{PR}_{f_i} &= \{|R_{f_i}(\alpha)| \text{ for } \alpha \in \{0,1\}^n\} \end{aligned}$$

Lemma 3.10. *If f and g are equivalent, then*

1. *the algebraic degree: $deg(f) = deg(g)$,*
2. *$PW_f = PW_g$ and $PR_f = PR_g$,*
3. *nonlinearity: $N_f = N_g$.*

An equivalence class $\mathcal{E}_{f_i}$ can be characterized by a pair of pattern sets, $\mathcal{PW}_{f_i}$ and $\mathcal{PR}_{f_i}$. For n=3, the pattern sets of three equivalence classes are:

$$\begin{aligned} \mathcal{E}_{f_1}\!: \ & \mathcal{PW}_{f_1} = \{2,2,2,2,2,2,2,6\} \\ & \mathcal{PR}_{f_1} = \{4,4,4,4,4,4,4,8\}, \\ \mathcal{E}_{f_2}\!: \ & \mathcal{PW}_{f_2} = \{0,0,0,0,4,4,4,4\} \\ & \mathcal{PR}_{f_1} = \{0,0,0,0,0,0,8,8\}, \\ \mathcal{E}_{f_3}\!: \ & \mathcal{PW}_{f_2} = \{0,0,0,0,0,0,0,8\} \\ & \mathcal{PR}_{f_1} = \{8,8,8,8,8,8,8,8\}, \end{aligned}$$

We list tables of equivalence classes and corresponding pattern sets for $n = 4$ and 5 in the Appendix A. Considering the cryptographic properties of all boolean functions , we can only focus on the pattern sets, $\mathcal{PW}_{f_i}$ and $\mathcal{PR}_{f_i}$, of the equivalence class. Moreover, for a given n, the number of equivalence classes is smaller than the number of boolean functions. When $n = 3$, 2^8 boolean functions are only divided into 3 equivalence classes. When $n = 5$, there are 48 equivalence classes for 2^{32} boolean functions. Thus a boolean function with specific cryptographic properties can be generated by finding its equivalence class.

Now we want to find a 5-variable boolean function g with the algebraic degree 3. We also expect that g is 1-st order correlation immune, satisfies $PC(2)$ and achieves maximum nonlinearity. From the previous section, neither **the PC-based Construction** nor **Extended-Resilient-Based Construction** can be used to generate such function. So we consider the following construction through the equivalence classes. We note that the degree of propagation criterion is 2 and order of correlation immunity is 1. The number of zeros, Z_{R_g} and Z_{W_g}, must meet the following constraints:

$$\begin{aligned} \mathrm{Z}_{R_g} &\geq C_1^5 + C_2^5 = 16 \text{ and} \\ \mathrm{Z}_{W_g} &\geq C_1^5 = 5 \end{aligned}$$

And the maximum nonlinearity for $n = 5$ is $2^{5-1} - 2^{\frac{5+1}{2}} = 8$. By looking up the pattern sets in Table 3 and Table 6, we can find that $\mathcal{E}_{f_{41}}$ meets our requirements. From Theorem 3.8, it is possible to find a matrix U and a vector β such that $W_g(\omega) = 0$ for $hw(\omega) = 1$ and $R_g(\alpha) = 0$ for for $1 \leq hw(\alpha) \leq 2$. Then we obtain

$$\begin{aligned} U &= \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\ \beta &= \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \end{bmatrix} \end{aligned}$$

So g is

$$\begin{aligned} g(x_1, x_2, x_3, x_4, x_5) &= x_3x_2x_1 \oplus x_5x_4 \oplus x_5x_1 \oplus x_4x_2 \oplus x_4x_1 \\ &\quad \oplus x_3x_2 \oplus x_3x_1 \oplus x_2x_1 \oplus x_2 \oplus x_1 \\ \xi_g &= (0,0,0,1,0,1,1,0,0,1,1,1,0,0,0,0, \\ &\quad 0,1,0,0,1,1,0,0,0,0,1,0,1,0,1,0) \end{aligned}$$

From the concept of equivalence class of boolean functions, it is easy to see the cryptographic properties of all boolean functions. We can find a boolean function with some given cryptographic properties by the corresponding equivalence class if the function exists. However, the number of equivalence classes of boolean functions is unknown for $n \geq 6$. It will be an interesting problem to develop an efficient algorithm to find all equivalence classes and corresponding pattern sets.

4 Conclusion

In this paper, we present two new constructions to generated a boolean function which take all these cryptographic properties into considered. One is the **Resilient-based Construction** and the other is the method through the concept of the equivalence classes of boolean function. We link the concept of equivalence classes with the Walsh-Hadamard transform and the autocorrelation function which are both used to analyze cryptographic properties of boolean functions.If there exists an efficient method to find all equivalence classes of boolean functions. For studying cryptographic boolean functions, we can focus on the equivalence classes by the patter sets, $\mathcal{PW}_f$ and $\mathcal{PR}_f$. It is helpful for the design of applications which use cryptographic boolean functions as a core component.

A Equivalence classes for n=3,4 and 5

A.1 Equivalence classes

$\mathcal{E}_{f_i}$	$def(f_i)$	f_i
$\mathcal{E}_{f_1}$	3	$x_1x_2x_3$
$\mathcal{E}_{f_2}$	2	x_1x_2
$\mathcal{E}_{f_3}$	≤ 1	0

Table 1: The equivalence classes for $n = 3$.

$\mathcal{E}_{f_i}$	$def(f_i)$	f_i
$\mathcal{E}_{f_1}$	4	$x_1x_2x_3x_4$
$\mathcal{E}_{f_2}$	4	$x_1x_2x_3x_4 \oplus x_1x_2$
$\mathcal{E}_{f_3}$	4	$x_1x_2x_3x_4 \oplus x_1x_2 \oplus x_3x_4$
$\mathcal{E}_{f_4}$	3	$x_2x_3x_4$
$\mathcal{E}_{f_5}$	3	$x_2x_3x_4 \oplus x_1x_2$
$\mathcal{E}_{f_6}$	2	$x_1x_2 \oplus x_3x_4$
$\mathcal{E}_{f_7}$	2	x_1x_2
$\mathcal{E}_{f_8}$	≤ 1	0

Table 2: The equivalence classes for $n = 4$.

$\mathcal{E}_{f_i}$	$def(f_i)$	f_i
$\mathcal{E}_{f_1}$	5	$x_1x_2x_3x_4x_5$
$\mathcal{E}_{f_2}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2$
$\mathcal{E}_{f_3}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2 \oplus x_3x_4$
$\mathcal{E}_{f_4}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3$
$\mathcal{E}_{f_5}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2$
$\mathcal{E}_{f_6}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4$
$\mathcal{E}_{f_7}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_4x_5$
$\mathcal{E}_{f_8}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5$
$\mathcal{E}_{f_9}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_4x_5$
$\mathcal{E}_{f_{10}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_3x_4$
$\mathcal{E}_{f_{11}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5$
$\mathcal{E}_{f_{12}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2$
$\mathcal{E}_{f_{13}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3$
$\mathcal{E}_{f_{14}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus \oplus x_4x_5$
$\mathcal{E}_{f_{15}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4$
$\mathcal{E}_{f_{16}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus \oplus x_2x_4$
$\mathcal{E}_{f_{17}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4 \oplus \oplus x_3x_5$
$\mathcal{E}_{f_{18}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus \oplus x_3x_5$
$\mathcal{E}_{f_{19}}$	5	$x_1x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus \oplus x_3x_5 \oplus x_4x_5$
$\mathcal{E}_{f_{20}}$	4	$x_2x_3x_4x_5$

$\mathcal{E}_{f_{21}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2$
$\mathcal{E}_{f_{22}}$	4	$x_2x_3x_4x_5 \oplus x_2x_3$
$\mathcal{E}_{f_{23}}$	4	$x_2x_3x_4x_5 \oplus x_2x_3 \oplus x_4x_5$
$\mathcal{E}_{f_{24}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2 \oplus x_3x_4$
$\mathcal{E}_{f_{25}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3$
$\mathcal{E}_{f_{26}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2$
$\mathcal{E}_{f_{27}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_2x_4$
$\mathcal{E}_{f_{28}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4$
$\mathcal{E}_{f_{29}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_4x_5$
$\mathcal{E}_{f_{30}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_3x_4$
$\mathcal{E}_{f_{31}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4 \oplus x_3x_5$
$\mathcal{E}_{f_{32}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2 \oplus x_4x_5$
$\mathcal{E}_{f_{33}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus x_3x_5$
$\mathcal{E}_{f_{34}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5$
$\mathcal{E}_{f_{35}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_4x_5$
$\mathcal{E}_{f_{36}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4 \oplus x_4x_5$
$\mathcal{E}_{f_{37}}$	4	$x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4 \oplus x_3x_5$
$\mathcal{E}_{f_{38}}$	3	$x_1x_2x_3$
$\mathcal{E}_{f_{39}}$	3	$x_1x_2x_3 \oplus x_4x_5$
$\mathcal{E}_{f_{40}}$	3	$x_1x_2x_3 \oplus x_1x_4$
$\mathcal{E}_{f_{41}}$	3	$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5$
$\mathcal{E}_{f_{42}}$	3	$x_1x_2x_3 \oplus x_1x_4x_5$
$\mathcal{E}_{f_{43}}$	3	$x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3$
$\mathcal{E}_{f_{44}}$	3	$x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4$
$\mathcal{E}_{f_{45}}$	3	$x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_5$
$\mathcal{E}_{f_{46}}$	2	x_1x_2
$\mathcal{E}_{f_{47}}$	2	$x_1x_2 \oplus x_3x_4$
$\mathcal{E}_{f_{48}}$	≤ 1	0

Table 3: The equivalence classes for $n = 5$.

A.2 Pattern Sets of Equivalence Classes

Let N be an integer. We denote N_i by the sequence of N's with length i. For example, 2_3 means the sequence $2, 2, 2$.

$\mathcal{E}_{f_i}$	Patterns Sets	
	$\mathcal{PW}_f$	$\mathcal{PR}_f$
$\mathcal{E}_{f_1}$	$2_7 \quad 6_1$	$4_7 \quad 8_1$
$\mathcal{E}_{f_2}$	$0_4 \quad 4_4$	$0_6 \quad 8_2$
$\mathcal{E}_{f_3}$	$0_7 \quad 8_1$	8_8

Table 4: The pattern sets of equivalence class for $n = 3$.

$\mathcal{E}_{f_i}$	Patterns Sets

	$\mathcal{PW}_f$	$\mathcal{PR}_f$
$\mathcal{E}_{f_1}$	$2_{15}\quad 14_1$	$12_{15}\quad 16_1$
$\mathcal{E}_{f_2}$	$2_{12}\quad 6_3\quad 10_1$	$4_{12}\quad 12_3\quad 16_1$
$\mathcal{E}_{f_3}$	$2_{10}\quad 6_6$	$4_{15}\quad 16_1$
$\mathcal{E}_{f_4}$	$0_8\quad 4_7\quad 12_1$	$8_{14}\quad 16_2$
$\mathcal{E}_{f_5}$	$0_6\quad 4_8\quad 8_2$	$0_9\quad 8_6\quad 16_1$
$\mathcal{E}_{f_6}$	4_{16}	$0_{15}\quad 16_1$
$\mathcal{E}_{f_7}$	$0_{12}\quad 8_4$	$0_{12}\quad 16_4$
$\mathcal{E}_{f_8}$	$0_{15}\quad 16_1$	16_{16}

Table 5: The pattern sets of equivalence class for $n = 4$.

$\mathcal{E}_{f_i}$	Patterns Sets	
	$\mathcal{PW}_f$	$\mathcal{PR}_f$
$\mathcal{E}_{f_1}$	$2_{31}\quad 30_1$	$28_{31}\quad 32_1$
$\mathcal{E}_{f_2}$	$2_{28}\quad 14_3\quad 18_1$	$4_{24}\quad 28_7\quad 32_1$
$\mathcal{E}_{f_3}$	$2_{16}\quad 6_{10}\quad 10_6$	$4_{30}\quad 28_1\quad 32_1$
$\mathcal{E}_{f_4}$	$2_{24}\quad 6_7\quad 26_1$	$20_{28}\quad 28_3\quad 32_1$
$\mathcal{E}_{f_5}$	$2_{24}\quad 6_4\quad 10_3\quad 22_1$	$12_{24}\quad 20_4\quad 28_3\quad 32_1$
$\mathcal{E}_{f_6}$	$2_{22}\quad 6_6\quad 10_2\quad 14_1\quad 18_1$	$4_{18}\quad 12_6\quad 20_6\quad 28_1,\quad 32_1$
$\mathcal{E}_{f_7}$	$2_{21},\quad 6_7\quad 10_1\quad 14_3$	$4_{24}\quad 20_7\quad 32_1$
$\mathcal{E}_{f_8}$	$2_{16}\quad 6_{10}\quad 10_6$	$4_{27}\quad 12_3\quad 20_1\quad 32_1$
$\mathcal{E}_{f_9}$	$2_{15}\quad 6_{13}\quad 10_3\quad 14_1$	$4_{24}\quad 12_6\quad 20_1\quad 32_1$
$\mathcal{E}_{f_{10}}$	$2_{22}\quad 6_4\quad 10_4\quad 14_2$	$4_{18}\quad 12_{12}\quad 28_1\quad 32_1$
$\mathcal{E}_{f_{11}}$	$2_{18}\quad 6_{12}\quad 14_1\quad 18_1$	$4_{16}\quad 12_9\quad 20_6\quad 32_1$
$\mathcal{E}_{f_{12}}$	$2_{15}\quad 6_{10}\quad 10_1\quad 22_1$	$12_{21}\quad 20_9\quad 32_1$
$\mathcal{E}_{f_{13}}$	$2_{19}\quad 6_9\quad 10_3\quad 18_1$	$4_{13}\quad 12_{15}\quad 20_3\quad 32_1$
$\mathcal{E}_{f_{14}}$	$2_{15}\quad 6_{15}\quad 10_1\quad 18_1$	$4_{10}\quad 12_{20}\quad 32_1$
$\mathcal{E}_{f_{15}}$	$2_{18}\quad 6_{10}\quad 10_2\quad 14_2$	$4_{20}\quad 12_9\quad 20_2\quad 32_1$
$\mathcal{E}_{f_{16}}$	$2_{16}\quad 6_{10}\quad 10_6$	$4_{25}\quad 12_6\quad 32_1$
$\mathcal{E}_{f_{17}}$	$2_{19}\quad 6_7\quad 10_5\quad 14_1$	$4_{21}\quad 12_{10}\quad 20_1\quad 32_1$
$\mathcal{E}_{f_{18}}$	$2_{16}\quad 6_{10}\quad 10_6$	$4_{25}\quad 12_6\quad 32_1$
$\mathcal{E}_{f_{19}}$	$2_{12}\quad 6_{16}\quad 10_4$	$4_{28}\quad 12_3\quad 32_1$
$\mathcal{E}_{f_{20}}$	$0_{16}\quad 4_{15}\quad 28_1$	$24_{30}\quad 32_2$
$\mathcal{E}_{f_{21}}$	$0_{14}\quad 4_{10}\quad 12_2\quad 16_2$	$0_{17}\quad 8_7\quad 24_7\quad 32_1$
$\mathcal{E}_{f_{22}}$	$0_{16}\quad 4_{10}\quad 12_3\quad 20_1$	$8_{24}\quad 24_6\quad 32_2$
$\mathcal{E}_{f_{23}}$	$0_{16}\quad 4_{10}\quad 12_6$	$8_{30}\quad 32_2$
$\mathcal{E}_{f_{24}}$	$0_8\quad 4_{14}\quad 8_8\quad 12_2$	$0_{17}\quad 8_{13}\quad 24_1\quad 32_1$
$\mathcal{E}_{f_{25}}$	$0_{12}\quad 4_{16}\quad 8_3\quad 24_1$	$16_{25}\quad 24_6\quad 32_1$
$\mathcal{E}_{f_{26}}$	$0_{12}\quad 4_{14}\quad 8_4\quad 20_1$	$8_{19}\quad 16_9\quad 24_3\quad 32_1$
$\mathcal{E}_{f_{27}}$	$0_{10}\quad 4_{16}\quad 8_4\quad 16_2$	$0_{16}\quad 8_4\quad 16_9\quad 24_2\quad 32_1$
$\mathcal{E}_{f_{28}}$	$0_{11}\quad 4_{14}\quad 8_4\quad 12_2\quad 16_1$	$0_{11}\quad 8_{13}\quad 16_6\quad 24_1\quad 32_1$
$\mathcal{E}_{f_{29}}$	$0_{12}\quad 4_{12}\quad 8_4\quad 12_4$	$0_{18}\quad 8_6\quad 16_7\quad 32_1$
$\mathcal{E}_{f_{30}}$	$0_{12}\quad 4_{12}\quad 8_4\quad 12_4$	$0_8\quad 8_{21}\quad 16_1\quad 24_1\quad 32_1$

$\mathcal{E}_{f_{31}}$	0_{8} 4_{14} 8_{8} 12_{2}	0_{15} 8_{14} 16_{2} 32_{1}
$\mathcal{E}_{f_{32}}$	0_{7} 4_{16} 8_{8} 16_{1}	0_{6} 8_{22} 16_{3} 32_{1}
$\mathcal{E}_{f_{33}}$	0_{4} 4_{16} 8_{12}	0_{24} 8_{6} 16_{1} 32_{1}
$\mathcal{E}_{f_{34}}$	0_{9} 4_{15} 8_{6} 12_{1} 16_{1}	0_{9} 8_{16} 16_{6} 32_{1}
$\mathcal{E}_{f_{35}}$	0_{10} 4_{15} 8_{6} 20_{1}	8_{16} 16_{15} 32_{1}
$\mathcal{E}_{f_{36}}$	0_{10} 4_{13} 8_{6} 12_{3}	0_{12} 8_{16} 16_{3} 32_{1}
$\mathcal{E}_{f_{37}}$	0_{6} 4_{15} 8_{10} 12_{1}	0_{15} 8_{16} 32_{1}
$\mathcal{E}_{f_{38}}$	0_{24} 8_{7} 24_{1}	16_{28} 32_{4}
$\mathcal{E}_{f_{39}}$	4_{28} 12_{4}	0_{24} 16_{7} 32_{1}
$\mathcal{E}_{f_{40}}$	0_{22} 8_{8} 16_{2}	0_{18} 16_{12} 32_{2}
$\mathcal{E}_{f_{41}}$	0_{16} 8_{16}	0_{27} 16_{4} 32_{1}
$\mathcal{E}_{f_{42}}$	4_{30} 12_{1} 20_{1}	8_{16} 16_{15} 32_{1}
$\mathcal{E}_{f_{43}}$	0_{19} 8_{12} 16_{1}	0_{9} 8_{16} 16_{6} 32_{1}
$\mathcal{E}_{f_{44}}$	4_{28} 12_{4}	0_{12} 8_{16} 16_{3} 32_{1}
$\mathcal{E}_{f_{45}}$	0_{16} 8_{16}	0_{15} 8_{16} 32_{1}
$\mathcal{E}_{f_{46}}$	0_{28} 16_{4}	0_{24} 32_{8}
$\mathcal{E}_{f_{47}}$	0_{16} 8_{16}	0_{30} 32_{2}
$\mathcal{E}_{f_{48}}$	0_{31} 32_{1}	32_{32}

Table 6: The pattern sets of equivalence class for $n = 5$.

References

[BW74] E.R. Berlekamp and L. R. Welch. **Weight distribution of the cosets of the (32,6) Reed-Muller code**. *IEEE Transactions on Information Theory*, IT-18(1):203–207, 1974.

[Car93] Claude Carlet. **Partially-bent functions**. *Designs, Codes and Cryptography*, 3:135–145, 1993.

[CLLS96] Seongtaek Chee, Sangjin Lee, Daiki Lee, and Soo Hak Sung. **On the correlation immune functions and their nonlinearity**. *Advances in Cryptology - ASIACRYPT'96*, pages 232–243, 1996.

[GZM88a] Xiao Guo-Zhen and James L. Massey. **A spectral characterization of correlation-immune combining functions**. *IEEE Transactions on Information Theory*, 34(3):569–571, 1988.

[GZM88b] Xiao Guo-Zhen and James L. Massey. **The Strict Avalanche Criterion: special properties of boolean functions and extended definition**. *Advances in Cryptology - CRYPTO'88*, pages 450–468, 1988.

[KT97] Kaoru Kurosawa and Takashi. **Design of SAC/PC(l) of order k boolean functions and three other cryptographic criteria**. *Advances in Cryptology - EUROCRYPTO'97*, pages 434–449, 1997.

[PLL$^+$90] Bart Preneel, Wener Van Leekwijck, Luc Van Linden, Rene Govaerts, and Joos Vandewalle. **Propagation characteristic of boolean functions**. *Advances in Cryptology -EUROCRYPT'90*, pages 161–173, 1990.

[Sar00] Palash Sarkar. **Spectral domain analysis of correlation immune and resilient boolean functions**. Technical report, Centre for Applied Cryptographic Research, 2000.

[SM00] P. Sarkar and S. Maitra. **Construction of nonlinear Boolean functions with important cryptographic properties**. *Advances in Cryptology - EUROCRYPT2000*, pages 485–506, 2000.

[SZZ93] Jennifer Seberry, Xian-Mo Zang, and Yuliang Zeng. **On constructions and nonlinearity of correlation immune functions**. *Advances in Cryptology - EUROCRYPTO'93*, pages 181–199, 1993.

[T.S84] T.Siegenthaler. **Correlation-immunity of nonlinear combining functions for cryptographic applications**. *IEEE Transactions on Information Theory*, 30(5):776–780, 1984.

[T.S85] T.Siegenthaler. **Decrypting a class of stream ciphers using ciphertext only**. *IEEE Transactions on Computers*, c-34(1):81–85, 1985.

[ZZ00] Yuliang Zeng and Xian-Mo Zang. **On relationships among avalance, nonlinearity and correlation immunity**. *Advances in Cryptology -ASIACRYPT2000*, pages 460–480, 2000.

[ZZ01] Yuliang Zeng and Xian-Mo Zang. **On plateaued functions**. *IEEE Transation on Information Theory*, IT-47(3):1215–1223, 2001.