On primary construction of Plateaued functions

Tian-Feng Sun[a*], Bin Hu[b], Yan Liu[c], Li-Ping Xu[d]

Information Science and Technology Institute, Zheng Zhou, China

[a*]enjoy2152013@163.com, [b]hb2110@126.com, [c]awhxxsbb@126.com, [d]xlp948431@163.com

Keywords: Boolean Functions, Plateaued Functions, Nonlinearity, Resiliency, Stream Ciphers.

Abstract. To resist different kinds of attacks, Boolean functions used in the cryptosystem should have good cryptographic properties. The Plateaued functions, a large class of Boolean functions containing Bent functions and Partial-Bent functions, are good choices. Therefore, the study of construction and cryptographic properties of Plateaued functions has received wide attention. However, until now, there are few primary constructions known to us, in which one does not assume the existence of previously defined functions to define new ones. Moreover, most of them have some drawbacks. In this paper, a new primary construction of Plateaued functions is given. And we show in particular that most of the existing primary constructions of Plateaued functions can be reduced to ours.

Introduction

It is well known that nonlinear Boolean functions play a very important role in the design of cryptosystem. To resist various attacks, good characteristics, including balance, high algebraic degree, high nonlinearity, propagation characteristics, high resiliency order and so on, must be considered. The importance of each characteristic depends on the choice of the cryptosystem. High nonlinearity and resiliency order are two most important criteria in all situations.

Bent functions permit to resist linear attacks in the best possible way by achieving optimum nonlinearity. Unfortunately, they are not balanced and exist only in even dimensions, which inspired scholars to search for new classes of Boolean functions whose elements still have high nonlinearity and can be balanced for both odd and even dimensions. The class of Partially-Bent functions was put forward by Carlet in [1], which has high nonlinearity, resiliency order and good propagation characteristics. However, when they are not Bent, Partially-Bent functions have by definition non-zero linear structures, which makes them improper for direct cryptographic use. Thanks to the class of Plateaued functions presented by Zheng and Zhang in [2], this drawback can be covered. Plateaued functions provide some examples of good trade-off among all the properties needed in the design of cryptosystem. For example, Maitra and Sarkar in [3] have shown us that the nonlinearity and resiliency order of Boolean functions are strongly bounded. The best compromise between the two properties is achieved by Plateaued functions only. As a result, the study of Plateaued functions becomes necessary and important. As for the construction of Plateaued functions, there only exist three main classes (see [4-6]). The class in [7] is in fact a subclass of [4]. Moreover, in the past several years, few primary constructions have been given. As for the second construction and other constructions, they are also important to obtain Boolean functions approaching or achieving the best trade-off among the cryptographic properties. And these constructions can be seen in [8-15].

We propose in this paper a new primary construction of Plateaued functions, which can contain those three main constructions as subclasses. The organization of this paper is as follows. Some basic concepts and notions are presented in Section 2. We give a list of the known constructions of Plateaued functions in Section 3, put forward our construction in Section 4 and investigate its characteristics in Section 5. In Section 6, we show that the former three main classes can be reduced to our construction. Finally, Section 7 concludes the paper.

Preliminaries

We denote the set of all n-variable Boolean functions by B_n, the addition in F_2 by $\oplus$ and the addition in Z by $+$. We denote by $\oplus_{i\in\ldots}$ and $\sum_{i\in\ldots}$ the corresponding multiple sums. The support of a Boolean function $f \in B_n$ is defined as $supp(f) = \{(x_1, x_2, \mathbf{L}, x_n) \in F_2^n \mid f(x_1, x_2, \mathbf{L}, x_n) = 1\}$. The weight of a function $f \in B_n$ is $wt(f) = \# supp(f)$. A function $f \in B_n$ is balanced if $wt(f) = 2^{n-1}$.

Any $f \in B_n$ can be uniquely represented as a polynomial over F_2 in n variables of the form:

$$f(x_1, x_2, \mathbf{L}, x_n) = a_0 \oplus \oplus_{1\le i\le n} a_i x_i \oplus \oplus_{1\le i<j\le n} a_{i,j} x_i x_j \oplus \mathbf{L} \oplus a_{1,2,\mathbf{L},n} x_1 x_2 \mathbf{L}\, x_n,$$

where the coefficients $a_0, a_i, a_{i,j}, \mathbf{L}, a_{1,2,\mathbf{L},n} \in \{0,1\}$. This representation is called the algebraic normal form (ANF). The algebraic degree, denoted by $\deg(f)$, is the number of variables in the highest order term with nonzero coefficient. A Boolean function is affine if there only exist terms of degree at most 1 in the ANF and the set of all affine functions is denoted by A_n. An affine function with $a_0 = 0$ is called a linear function. Any linear function on F_2^n can be denoted by $l \cdot x = l_1 x_1 \oplus l_2 x_2 \oplus \mathbf{L} \oplus l_n x_n$, where $l = (l_1, l_2, \mathbf{L}, l_n)$, $x = (x_1, x_2, \mathbf{L}, x_n) \in F_2^n$, and "$\cdot$" denotes the dot (inner) product of two vectors.

The Walsh transform of $f \in B_n$ is an integer valued function over F_2^n defined by $W_f(l) = \sum_{x\in F_2^n} (-1)^{f(x)\oplus l\cdot x}$.

It satisfies Parseval's relation: $\sum_{l\in F_2^n} [W_f(l)]^2 = 2^{2n}$. (1)

A Boolean function $f \in B_n$ is said to be Plateaued if its Walsh transform only takes the three values 0 and $\pm l$, where l is some positive integer and must be a power 2^r with $r \ge n/2$. We call l the amplitude[6] of Plateaued functions.

The study of the Walsh spectrum of quadratic function can be found in [16, 17].

Suppose $f \in B_n$ is a quadratic function. The bilinear form associated with f is defined by $B_f(x, y) = f(0) \oplus f(x) \oplus f(y) \oplus f(x \oplus y)$. The kernel of $B_f(x, y)$ is subspace of F_2^n defined by $rad(f) = \{x \in F_2^n \mid \forall y \in F_2^n, B_f(x, y) = 0\}$.

Lemma 1[16,17] Suppose $f \in B_n$ is a quadratic function and $B_f(x, y)$ is the binary form associated with it, then the Walsh spectrum of f depends only on the dimension of the kernel of $B_f(x, y)$, denoted by t, then the weight distribution of the Walsh spectrum of f is as follow:

$W_f(l)$	Number of l
0	$2^n - 2^{n-t}$
$2^{(n+t)/2}$	$2^{n-t-1} + (-1)^{f(0)} 2^{(n-t-2)/2}$
$-2^{(n+t)/2}$	$2^{n-t-1} - (-1)^{f(0)} 2^{(n-t-2)/2}$

A Boolean function $f \in B_n$ is said to be Plateaued with the order r if its Walsh transform W_f only takes the three values 0 and $\pm 2^{n-r/2}$.

Many properties of Boolean function can be deduced from its Walsh spectra. For ever Boolean function $f \in B_n$, the nonlinearity N_f and its Walsh transform W_f satisfy the relation:

$$N_f = 2^{n-1} - \frac{1}{2}\max_{l \in F_2^n} |W_f(l)|. \tag{2}$$

Because of the relation (1), N_f is upper bounded by $2^{n-1} - 2^{n/2-1}$. This bound is tight for every n even. The functions achieving it are called bent.

A Boolean function $f \in B_n$ is said to be balanced if and only if $W_f(0) = 0$, and to be m-resilient if and only if its Walsh transform satisfies $W_f(l) = 0$, for all $l \in F_2^n$ such that $0 \le wt(l) \le m$.

Known Constructions of Plateaued Functions

In this section, we review some known primary constructions of Plateaued functions.

3.1 Marorana-McFarland's Functions

Camion and Carlet generalized in [4] the class of Marorana-McFarland's Functions. We shall call MM the generalized class defined as follows:

Definition 1[4] For any positive integers r and s such that $n=r+s$, a MM function f is defined by

$$f_{f,g}(x,y) = x \cdot f(y) \oplus g(y) \tag{3}$$

where f is any function from F_2^s into F_2^r and g is any Boolean function on F_2^s.

Let $f_{f,g}$ be a function in MM. For any pair $(a,b) \in F_2^r \times F_2^s$, the value at (a,b) of the Walsh transform $W_{f_{f,g}}$ of $f_{f,g}$ equals $2^r \sum_{y \in f^{-1}(a)} (-1)^{b \cdot y \oplus g(y)}$. Two sufficient conditions are given in the following proposition on which $f_{f,g}$ in MM is Plateaued.

Proposition 1[4] Let $f_{f,g}$ be a function defined on $F_2^r \times F_2^s$ and belonging to MM. If f is injective (resp. takes exactly 2 times each value of Im(f)), then $f_{f,g}$ is Plateaued of amplitude 2^r (resp. 2^{r+1}).

A drawback of MM functions is that their restrictions obtained by keeping y constant in their input are affine, that is, these functions are in fact the concatenations of affine functions.

3.2 Generalized Marorana-McFarland's Functions

A construction generalizing construction MM and avoiding the drawback that these functions are the concatenations of affine functions was proposed in [5]. We denote it by GMM. The functions it produces are in fact the concatenation of quadratic functions instead of affine functions.

Definition 2[5] Let n and r be positive integers such that $r < n$. Denote the integer part $\lfloor r/2 \rfloor$ by t and $n-r$ by s. Let y be a mapping from F_2^s to F_2^t and let $y_1, \mathbf{L}\, y_t$ be its coordinate functions. Let f be a mapping from F_2^s to F_2^r and let $f_1, \mathbf{L}\, f_r$ be its coordinate functions. Let g be a Boolean function on F_2^s. The function $f_{y,f,g}$ is defined on $F_2^n = F_2^r \times F_2^s$ as

$$f_{y,f,g}(x,y) = \oplus_{i=1}^{t} x_{2i-1} x_{2i} y_i(y) \oplus x \cdot f(y) \oplus g(y),\ x \in F_2^r,\ y \in F_2^s. \tag{4}$$

MM's functions correspond to the case where y is the null mapping.

Lemma 2[5] Let $f_{y,f,g}$ be defined as in Definition 2. Then for every $a \in F_2^r$ and every $b \in F_2^s$, we have $W_{f_{y,f,g}}(a,b) = \sum_{y \in E_a} 2^{r-wt(y(y))} (-1)^{\oplus_{i=1}^{t}(f_{2i-1}(y) \oplus a_{2i-1})(f_{2i}(y) \oplus a_{2i}) \oplus g(y) \oplus b \cdot y}$, where E_a is the superset of

$f^{-1}(a)$ equal if r is even to $E_a = \{y \in F_2^s \mid \forall i \le t, y_i(y) = a_{2i-1} \Rightarrow f_{2i-1}(y) = a_{2i-1}, f_{2i-1}(y) = a_{2i-1}\}$ and if r is odd to $E_a = \{y \in F_2^s \mid \forall i \le t, y_i(y) = a_{2i-1} \Rightarrow f_{2i-1}(y) = a_{2i-1}, f_{2i-1}(y) = a_{2i-1}, f_r(y) = a_r\}$.

Proposition 3[5] Let $f_{y,f,g}$ be defined as in Definition 2. If y has constant weight and if E_a has size 0 or 1 for every a (resp. 0 or 2 for every a), then $f_{y,f,g}$ is Plateaued.

3.3 Q's Functions

Functions in the class GMM are built as the concatenations of quadratic functions chosen in such a way that we can efficiently compute their Walsh spectra. Carlet and Prouff present another way of concatenating quadratic functions in [6].We denote the class by Q.

Definition 3[6] For any positive integers *r* and *s* such that *n*=*r*+*s*, an Q function f is defined by

$$f_{f_1,f_2,f_3,g}(x,y) = (x \cdot f_1(y))(x \cdot f_2(y)) \oplus x \cdot f_3(y) \oplus g(y),\ x \in F_2^r,\ y \in F_2^s, \tag{5}$$

where f_1, f_2 and f_3 are three functions from F_2^s into F_2^r and g is a Boolean function on F_2^s.

Proposition 4[6] Let $f_{f_1,f_2,f_3,g}(x,y)$ be a function in Q such that $f_2(y) \ne 0$ for every $y \in F_2^s$. Let E be the set of all $y \in F_2^s$ such that the vectors $f_1(y)$ and $f_2(y)$ are linearly independent. Then, for every $a \in F_2^r$ and every $b \in F_2^s$, we have

$$W_{f_{f_1,f_2,f_3,g}}(a,b) = 2^{r-1} \sum_{\substack{y \in E;\\ f_3(y)+a \in \{0, f_1(y), f_2(y)\}}} (-1)^{g(y)\oplus b\cdot y} - 2^{r-1} \sum_{\substack{y \in E;\\ f_3(y)+a = f_1(y)+f_2(y)}} (-1)^{g(y)\oplus b\cdot y}$$
$$+2^r \sum_{\substack{y \in F_2^s \setminus E;\\ f_3(y)+a = f_1(y)}} (-1)^{g(y)\oplus b\cdot y}$$

Proposition 5[6] Let $f_{f_1,f_2,f_3,g}(x,y)$ be defined as in Definition 3. Assume that, for every $y \in F_2^s$, the vectors $f_1(y)$ and $f_2(y)$ are linearly independent. If the 2-demensional flats $f_3(y) + < f_1(y), f_2(y) >$ (where y ranges over F_2^s) are pairwise disjoint , then $f_{f_1,f_2,f_3,g}(x,y)$ is Plateaued of amplitude 2^{r-1}.

Proposition 6[6] Let $f_{f_1,f_2,f_3,g}(x,y)$ be defined as in Definition 3. Assume that $f_2(y) \ne 0$ for every $y \in F_2^s$. For every $a \in F_2^r$, let F_a' be the set of all $y \in F_2^s$ such that the vectors $f_1(y)$ and $f_2(y)$ are linearly independent and such that a belongs to the flat $f_3(y) + < f_1(y), f_2(y) >$. Let F_a'' be the set of all $y \in F_2^s$ such that the vectors $f_1(y)$ and $f_2(y)$ are linearly dependent and $a = f_1(y) + f_3(y)$. If, for every $a \in F_2^r$, the number $\#F_a' + 2\#F_a'' = 0$ *or* 2, then $f_{f_1,f_2,f_3,g}(x,y)$ is Plateaued of amplitude 2^r.

A New Construction of Boolean Functions Leading to Plateaued Functions

Functions in class MM are built as the concatenations of affine functions, while functions in class GMM and Q are built as the concatenations of quadratic functions. The Walsh spectra of these three classes of functions can be efficiently computed. The aim of this section is to present another way of concatenating quadratic functions, whose Walsh spectra can also be efficiently computed.

Firstly, let $(a_{ij})_{nn}, (b_{ij})_{nn}, \mathbf{L}$ stand for a matrix of order n.

Note: Let the set $\{(a_{ij})_{nn} \mid \forall\ 1 \le i < j \le n, a_{ji} = 0\}$ denoted by U_n. Suppose that $f \in B_n$ is a quadratic function with $a_0 = 0$, then the ANF of f is $f(x_1, x_2, \mathbf{L}, x_n) = \oplus_{1 \le i \le n} a_i x_i + \oplus_{1 \le i < j \le n} a_{i,j} x_i x_j$. And we find that f can be also written in the form:

$$f(x) = x(a_{ij})_{nn} x^T \tag{6}$$

where $x = (x_1, x_2, \mathbf{L}, x_n) \in F_2^n$, $(a_{ij})_{nn} \in U_n$ and $a_{ii} = a_i$, $a_{ij} = a_{i,j}$.

We concatenate now the functions in this Note:

Definition 4 For any positive integers r and s such that $n = r + s$, we call TF the class of all Boolean functions f in the form:

$$f_{z,g}(x, y) = xz(y)x^T \oplus g(y), x \in F_2^r, y \in F_2^s, \tag{7}$$

where z is a mapping from F_2^s to U_r and g is any Boolean function on F_2^s.

In order to compute the Walsh spectra of the TF functions, we investigate the dimension of the kernel of binary form associate with the functions in (6) at first.

Suppose that $f \in B_n$ is a quadratic function with $a_0 = 0$ and $f(x) = x(a_{ij})_{nn} x^T$, then the bilinear form associated with f can be written as $B_f(x, y) = f(0) \oplus f(x) \oplus f(y) \oplus f(x \oplus y)$ $= 0 \oplus x(a_{ij})_{nn} x^T \oplus y(a_{ij})_{nn} y^T \oplus (x \oplus y)(a_{ij})_{nn}(x \oplus y)^T$ $x(b_{ij})_{nn} y^T$.

Next, we describe more details of implication for the matrix $(b_{ij})_{nn}$.

Let d be a mapping from U_n to the set $\{(c_{ij})_{nn} \mid \forall\ 1 \le i \le n, c_{ii} = 0\ ; \forall\ 1 \le i < j \le n, c_{ij} = c_{ji}\}$ such that for every $(a_{ij})_{nn} \in U_n$, $d((a_{ij})_{nn}) = (c_{ij})_{nn}$, where $c_{ij} = c_{ji} = a_{ij}, 1 \le i < j \le n$.

Without loss of generality, we assume that there exists the monomial x_1 and $x_1 x_2$ in the ANF of f, then the elements $0 \oplus x_1 \oplus y_1 \oplus (x_1 \oplus y_1) = 0$ and $0 \oplus x_1 x_2 \oplus y_1 y_2 \oplus (x_1 \oplus y_1)(x_2 \oplus y_2) = x_1 y_2$ $\oplus x_2 y_1$ exist in the ANF of $B_f(x, y)$. Therefore, we obtain the relation between d and $(b_{ij})_{nn}$ such that $(b_{ij})_{nn} = d((a_{ij})_{nn})$.

Let $D(rad(f))$ be the dimension of the kernel of $B_f(x, y)$. Then $rad(f) = \{x \in F_2^n \mid \forall y \in F_2^n,$ $B_f(x, y) = 0\} = \{x \in F_2^n \mid \forall y \in F_2^n, x(b_{ij})_{nn} y^T = 0\} = \{x \in F_2^n \mid x(b_{ij})_{nn} = \overline{0}\}$, thus, we can conclude that $D(rad(f)) = n - R((b_{ij})_{nn}) = n - R(d((a_{ij})_{nn}))$, where $R((b_{ij})_{nn})$ is the rank of $(b_{ij})_{nn}$.

According to Lemma 1, we put forward the computation of the Walsh spectra of the TF functions as follow.

Theorem 1 Let $f_{z,g}$ be defined as in Definition 4. Denote $xz(y)x^T$ by $F_y(x)$ and $D(rad(F_y))$ by t_y. Denote the set $\{w \in F_2^r \mid W_{F_y}(w) = 0\}$ by $W_{F_y}^0$, the set $\{w \in F_2^r \mid W_{F_y}(w) = 2^{(n+t_y)/2}\}$ by $W_{F_y}^+$ and the set $\{w \in F_2^r \mid W_{F_y}(w) = -2^{(n+t_y)/2}\}$ by $W_{F_y}^-$. Then for every $a \in F_2^r$ and every $b \in F_2^s$, we have

$$\begin{aligned} W_{f_{z,g}}(a, b) &= \sum_{(x,y) \in F_2^r \times F_2^s} (-1)^{xz(y)x^T \oplus g(y) \oplus ax \oplus by} \\ &= \sum_{y \in F_2^s} (-1)^{g(y) \oplus by} \sum_{x \in F_2^r} (-1)^{xz(y)x^T \oplus ax} \\ &= \sum_{y \in F_2^s} x_{a,z}(y) 2^{(r+t_y)/2} (-1)^{g(y) \oplus by} \\ &= \sum_{y \in F_2^s} x_{a,z}(y) 2^{(2r - R(dz(y)))/2} (-1)^{g(y) \oplus by} \end{aligned},$$

where $x_{a,z}$ is a mapping from F_2^s to $\{0, 1, -1\}$ such that for every $y \in F_2^s$,

$$x_{a,z}(y) = \begin{cases} 0, a \in W_{F_y}^0 \\ 1, a \in W_{F_y}^+ \\ -1, a \in W_{F_y}^- \end{cases}.$$

Theorem 2 Let $f_{z,g}$ be defined as in Definition 4. We denote $R(dz(y))$ by t_0 and assume that t_0 is constant for every $y \in F_2^s$. For every $a \in F_2^r$, let F_a be the set of all $y \in F_2^s$ such that $x_{a,z}(y) \neq 0$. If, for every $a \in F_2^r$, $\#F_a = 0$ *or* 1 (resp. 0 or 2), then $f_{z,g}$ is Plateaued of amplitude $2^{r-t_0/2}$ (resp. $2^{r+1-t_0/2}$).

Proof. According to the hypothesis and proposition 9, if $\#F_a = 0$ or 1 (resp. 0 or 2), then $W_{f_{z,g}}(a,b)$ equals 0 or $\pm 2^{(2r-t_0)/2}$ (resp. 0 or $\pm 2^{(2r-t_0+2)/2}$). ■

Remark: Because of that for every $(a_{ij})_{rr} \in U_r$, the diagonal elements of the matrix $d((a_{ij})_{rr})$ are all equal to 0, there exist at least 2^r matrixes of U_r such that the rank of their images after mapping d are all the same. Thus, the condition that $R(dz(y))$ is constant for every $y \in F_2^s$ is easy to satisfy.

We call the class of those Plateaued functions TF_1 (resp. TF_2) in TF constructed in the way of making $\#F_a = 0$ *or* 1 (resp. 0 or 2) for every $a \in F_2^r$.

Study of the Class TF_1 and TF_2

According to Equality (3) and Theorem 2, the nonlinearity of any Boolean function in class TF_1 (resp. TF_2) is $2^{n-1} - 2^{(2r-t_0)/2-1}$ (resp. $2^{n-1} - 2^{(2r-t_0)/2}$).

The following two propositions investigate the resiliency order of TF_1 and TF_2.

Proposition 9 Let $f_{z,g}$ be defined as in Definition 4. Let D be the set of all $a \in F_2^r$ such that $x_{a,z}(y) \neq 0$ for some $y \in F_2^s$. Let k be the minimum weight of the elements of D. If, for every $a \in F_2^r$, $\#F_a = 0$ *or* 1, the resiliency order m of $f_{z,g}$ equals $k-1$ and k is upper bounded by $\max\{t \in N : \sum_{i=0}^{t} \binom{r}{i} \leq 2^r - \#D\} + 1$.

Proof. According to the hypothesis and Theorem 1 and 2, $W_{f_{z,g}}(a,b)$ equals $\pm 2^{(2r-t_0)/2}$ if and only if $a \in D$. If (a,b) has weight smaller than or equal to $k-1$, then a has weight smaller than or equal to $k-1$ and does not belong to D, which implies that $W_{f_{z,g}}(a,b) = 0$. Therefore, $f_{z,g}$ has resiliency order at least $k-1$. Moreover, suppose that $f_{z,g}$ has resiliency order larger than or equal to k, then $W_{f_{z,g}}(a,b) = 0$ for any $a \in F_2^r$ having weight k, which contradicts the hypothesis on k and D. Thus, the resiliency order of $f_{z,g}$ equals $k-1$.

Since, by hypothesis, every vector of weight smaller than or equal to $k-1$ belong to D^c, we deduce that $\sum_{i=0}^{k-1} \binom{r}{i} \leq 2^r - \#D$ and then $k \leq \max\{t \in N : \sum_{i=0}^{t} \binom{r}{i} \leq 2^r - \#D\} + 1$. ■

Proposition 10 Let $f_{z,g}$ be defined as in Definition 4, D and k be defined as in Proposition 9. If, for every $a \in F_2^r$, $\#F_a = 0$ *or* 2, the resiliency order m of $f_{z,g}$ equals $k-1$ or k and k is upper bounded by $\max\{t \in N : \sum_{i=0}^{t} \binom{r}{i} \leq 2^r - \#D\} + 1$.

Proof. According to the hypothesis and Theorem 1 and 2, $W_{f_{z,g}}(a,b)$ equals $\pm 2^{(2r-t_0+2)/2}$ if and only if $a \in D$. If (a,b) has weight smaller than or equal to $k-1$, then a has weight smaller than or

equal to $k-1$ and does not belong to D, which implies that $W_{f_{z,g}}(a,b)=0$. Therefore, $f_{z,g}$ has resiliency order at least $k-1$.

Suppose that a is an element of D with Hamming weight being k and let y_1 and y_2 be two elements of F_2^s such that $x_{a,z}(y_1)\neq 0$ and $x_{a,z}(y_2)\neq 0$. According to Proposition 9, for every $b\in F_2^s$, the restriction of $W_{f_{z,g}}$ to $\{a\}\times F_2^s$ can be written as following:

$$\frac{1}{2^{(2r-t_0)/2}}W_{f_{z,g}}(a,b)=\pm[(-1)^{g(y_1)\oplus by_1}-(-1)^{g(y_2)\oplus by_2}]=\pm 2[b\cdot(y_1+y_2)\oplus g(y_1)\oplus g(y_2)] \text{ or}$$

$$\frac{1}{2^{(2r-t_0)/2}}W_{f_{z,g}}(a,b)=\pm[(-1)^{g(y_1)\oplus by_1}+(-1)^{g(y_2)\oplus by_2}]=\pm 2[b\cdot(y_1+y_2)\oplus g(y_1)\oplus g(y_2)+1].$$

When the vectors y_1 and y_2 are distinct, the linear function $b\to b\cdot(y_1+y_2)$ is not constant on the set $\{b\in F_2^s \mid wt(b)\leq 1\}$, and then there always exists an element $b\in F_2^s$ with Hamming weight $wt(b)\leq 1$ such that $W_{f_{z,g}}(a,b)\neq 0$. And this implies that the resiliency order of $f_{z,g}$ is strictly upper bounded by $k+1$. Thus, we conclude that the resiliency order of $f_{z,g}$ equals $k-1$ or k. The proof of the k's bound is the same as Proposition 11. ■

Relation among these four Constructions

In this section, we shall deduce that those three classes of functions, namely MM, GMM and Q, can be reduced to TF functions.

6.1 MM's reduction

Denote the set $\{(a_{ij})_{rr} \mid (a_{ij})_{rr}\in U_r\ ;\forall\ 1\leq i<j\leq r, a_{ij}=0\}$ by U_r^{MM}. Obviously, the set U_r^{MM} is a subset of U_r. Let z_{MM} be a mapping from F_2^s to U_r^{MM}, then the function $f_{z_{MM},g}(x,y)=xz_{MM}(y)x^T\oplus g(y)$ is actually the function $f_{f,g}(x,y)=x\cdot f(y)\oplus g(y)$ in definition 1. And for every $y\in F_2^s$, $d(z_{MM}(y))=(0)_{rr}$, hence, $R(d(z_{MM}(y)))=0$. Then for every $a\in F_2^r$ and every $b\in F_2^s$, we have $W_{f_{z_{MM},g}}(a,b)=\sum_{(x,y)\in F_2^r\times F_2^s}(-1)^{xz_{MM}(y)x^T\oplus g(y)\oplus ax\oplus by}=\sum_{y\in F_2^s}x_{a,z}(y)$ $2^{(2r-R(dz_{MM}(y)))/2}(-1)^{g(y)\oplus by}=2^r\sum_{y\in F_2^s}x_{a,z_{MM}}(y)(-1)^{g(y)\oplus by}$.

If f is injective (resp. takes exactly 2 times each value of Im(f)), then for every $a\in F_2^r$, there exists at most one (resp. 0 or 2) $y\in F_2^s$ such that $\sum_{x\in F_2^r}(-1)^{xf(y)\oplus a\cdot x}\neq 0$, while this condition can be deduced to that for every $a\in F_2^r$, there exists at most one (resp. 0 or 2) $y\in F_2^s$ such that $x_{a,z_{MM}}(y)\neq 0$, that is $\#F_a=0$ or 1 (resp. $\#F_a=0$ or 2).

Hence, the MM functions can be reduced to TF functions.

6.2 GMM's reduction

Let U_r^{GMM} be the set of $(a_{ij})_{rr}\in U_r$ such that for every $1\leq i\leq t, 1\leq j\leq r$, $a_{2i-1,2i}, a_{jj}=0$ *or* 1 and the rest positions are all 0. Let z_{GMM} be a mapping from F_2^s to U_r^{GMM}, then the function $f_{z_{GMM},g}(x,y)=xz_{GMM}(y)x^T\oplus g(y)$ is actually the function $f_{y,f,g}(x,y)=\oplus_{i=1}^t x_{2i-1}x_{2i}y_i(y)\oplus x\cdot f(y)$ $\oplus g(y)$ in definition 2.

Theorem 3 Let $f_{y,f,g}$ be defined as in Definition 2. If y has constant weight, we denote it by r_0, then for every $y\in F_2^s$, $R(d(z_{GMM}(y)))=2r_0$.

Proof. Due to that the binary form of affine functions is equal to 0, we consider y only. If y has constant weight, that is, for every $y\in F_2^s$, the number of 1 in the vector $(y_1(y),\mathbf{L}y_t(y))$ is constant and equal to r_0, and this condition is equivalent to that the number of 1 in the set

$\{a_{12}, a_{34}, \mathbf{L}, a_{(2t-1)(2t)}\}$ is r_0. Assume that r is an even integer, then $t = r/2$. We get the following matrix:

$$A' = \begin{bmatrix} \begin{matrix} 0 & a_{12} \\ a_{21} & 0 \end{matrix} & & & \\ & \begin{matrix} 0 & a_{34} \\ a_{43} & 0 \end{matrix} & & \\ & & \mathbf{O} & \\ & & & \begin{matrix} 0 & a_{(r-1)(r)} \\ a_{(r)(r-1)} & 0 \end{matrix} \end{bmatrix},$$

where $a_{12} = a_{21}, \mathbf{L}, a_{(r-1)(r)} = a_{(r)(r-1)}$. We can find that $A' \in R(d(z_{GMM}(F_2^s)))$. Obviously, if the number of 1 in the set $\{a_{12}, a_{34}, \mathbf{L}, a_{(r-1)(r)}\}$ is r_0, the order of this matrix A' is $2r_0$.

In a similar way, we can proof this theorem is still hold in the case that r is an odd integer. Therefore, we conclude that if $wt(y) = r_0$, then for every $y \in F_2^s$, $R(d(z_{GMM}(y))) = 2r_0$. ■

Theorem 3 tells us that for every $a \in F_2^r$ and every $b \in F_2^s$, if $wt(y) = r_0$, we have $W_{f_{z_{GMM}}, g}(a,b) = 2^{r-r_0} \sum_{y \in F_2^s} x_{a, z_{GMM}}(y)(-1)^{g(y) \oplus by}$.

If for every $a \in F_2^r$, $\#E_a = 0$ *or* 1 (resp. 0 or 2), then there exists at most one (resp. 0 or 2) $y \in F_2^s$ such that $\sum_{x \in F_2^r} (-1)^{\oplus_{i=1}^t x_{2i-1} x_{2i} y_i(y) \oplus x \cdot f(y) \oplus a \cdot x} \neq 0$, and this condition can be deduced to that for every $a \in F_2^r$, there exists at most one (resp. 0 or 2) $y \in F_2^s$ such that $x_{a, z_{GMM}}(y) \neq 0$, that is $\#F_a = 0$ or 1 (resp. $\#F_a = 0$ or 2).

Hence, the GMM functions can be reduced to TF functions.

6.3 Q's reduction

Let U_r^Q be the set of all $(a_{ij})_{rr} \in U_r$ such that $(x \cdot f_1(y))(x \cdot f_2(y)) \oplus x \cdot f_3(y)$ can be written in the form $x(a_{ij})_{rr} x^T$ when y run through F_2^s. Let z_Q be a mapping from F_2^s to U_r^Q, then the function $f_{z_Q, g}(x, y) = xz_Q(y)x^T \oplus g(y)$ is actually the function $f_{f_1, f_2, f_3, g}(x, y) = (x \cdot f_1(y))(x \cdot f_2(y)) \oplus x \cdot f_3(y) \oplus g(y)$ in definition 3.

Theorem 4 Let $f_{f_1, f_2, f_3, g}(x, y)$ be defined as in Definition 3. Assume that for every $y \in F_2^s$, the vectors $f_1(y)$ and $f_2(y)$ are linearly independent, that is $E = F_2^s$, then for every $y \in F_2^s$, $R(d(z_Q(y))) = 2$.

Proof. Due to that the binary form of affine functions is equal to 0, we consider f_1 and f_2 only. Because of that $E = F_2^s$, for every $y \in F_2^s$, the vector $f_1(y) \neq 0$, $f_2(y) \neq 0$ and $f_1(y) \neq f_2(y)$.

For any given $y \in F_2^s$, let the vector $f_1(y)$ be $(u_1, u_2, \mathbf{L}, u_r)$, the vector $f_2(y)$ be $(v_1, v_2, \mathbf{L}, v_r)$, without loss of generality, we assume that $u_{i_l} = v_{j_k} = 1$, where $1 \le l \le k \le r$, and 0 elsewhere, then $(x \cdot f_1(y))(x \cdot f_2(y)) = (u_{i_1} x_{i_1} \oplus \mathbf{L} \oplus u_{i_l} x_{i_l})(v_{j_1} x_{j_1} \oplus \mathbf{L} \oplus v_{j_k} x_{j_k}) \quad x(b_{ij})_{rr} x^T$, where $(b_{ij})_{rr} \in U_r$.

Denote the set $\{i_1, \mathbf{L}, i_l\}$ by I, the set $\{j_1, \mathbf{L}, j_k\}$ by J and the set $\{1, 2, \mathbf{L}, r\}$ by R, then the set $\{x_i : i \in R\}$ can be divided into four classes as follow:

(1) $\{x_i \mid i \in R \setminus (I \cup J)\}$

(2) $\{x_i \mid i \in I \setminus (I \cap J)\}$

(3) $\{x_i \mid i \in J \setminus (I \cap J)\}$

(4) $\{x_i \mid i \in I \cap J\}$

Due to that for every $y \in F_2^s$, the vector $f_1(y) \neq 0$, $f_2(y) \neq 0$ and $f_1(y) \neq f_2(y)$, we get that if the set $\{x_i \mid i \in I \cap J\} \neq \varnothing$, then there exists at most one $\varnothing$ of the two sets $\{x_i \mid i \in I \setminus (I \cap J)\}$ and $\{x_i \mid i \in J \setminus (I \cap J)\}$. If the set $\{x_i \mid i \in I \cap J\} = \varnothing$, then both the sets $\{x_i \mid i \in I \setminus (I \cap J)\}$ and $\{x_i \mid i \in J \setminus (I \cap J)\}$ are not $\varnothing$. The set $\{x_i \mid i \in R \setminus (I \cup J)\}$ is possibly equal to $\varnothing$. For every $i^{(1)} \in R \setminus (I \cup J)$, $i^{(1)}$th row of the matrix $d((b_{ij})_{rr})$ will be all 0. For every $i^{(2)} \in I \setminus (I \cap J)$, $i^{(2)}$th row of the matrix $d((b_{ij})_{rr})$ will be $(v_1, v_2, \mathbf{L}, v_r)$. For every $i^{(3)} \in J \setminus (I \cap J)$, $i^{(3)}$th row of the matrix $d((b_{ij})_{rr})$ will be $(u_1, u_2, \mathbf{L}, u_r)$. For every $i^{(4)} \in I \cap J$, $i^{(4)}$th row of the matrix $d((b_{ij})_{rr})$ will be $(u_1 + v_1, u_2 + v_2, \mathbf{L}, u_r + v_r)$.

In summary, we conclude that for every $y \in F_2^s$, $R(d(z_Q(y))) = 2$. ■

Assume that $E = F_2^s$. Then for every $a \in F_2^r$ and every $b \in F_2^s$, we have $W_{f_{f_1,f_2,f_3,g}}(a,b) = 2^{r-1} \sum_{\substack{y \in E; \\ f_3(y)+a \in \{0, f_1(y), f_2(y)\}}} (-1)^{g(y) \oplus b \cdot y} - 2^{r-1} \sum_{\substack{y \in E; \\ f_3(y)+a = f_1(y)+f_2(y)}} (-1)^{g(y) \oplus b \cdot y}$ and $W_{f_{z_Q},g}(a,b) = 2^{r-1} \sum_{y \in F_2^s} x_{a,z_Q}(y) (-1)^{g(y) \oplus by}$.

If the 2-demensional flats $f_3(y) + < f_1(y), f_2(y) >$ are pairwise disjoint for every $y \in F_2^s$, that is, for $y \in F_2^s$, the vectors $f_3(y), f_1(y) + f_3(y), f_2(y) + f_3(y)$ and $f_1(y) + f_2(y) + f_3(y)$ are pairwise unequal, then it can be deduced that for every $a \in F_2^r$, there exists at most one $y \in F_2^s$ such that $x_{a,z_Q}(y) \neq 0$, that is $\# F_a = 0$ or 1.

Let the set F_a' and F_a'' be defined in proposition 6. If $\# F_a' + 2 \# F_a'' = 0 \; or \; 2$, then $(\# F_a'' = 0 \; and \; \# F_a' = 0 \; or \; 2)$ or $(\# F_a'' = 0 \; or \; 1 \; and \; \# F_a' = 0)$, and the first case can be deduced to that for every $y \in F_2^s$, $R(d(z_Q(y))) = 2$ and for every $a \in F_2^r$, there exists zero or two $y \in F_2^s$ such that $x_{a,z_Q}(y) \neq 0$, that is $\# F_a = 0$ or 2, while the second case can be deduced to that for every $y \in F_2^s$, $R(d(z_Q(y))) = 0$ and for every $a \in F_2^r$, there exists at most one $y \in F_2^s$ such that $x_{a,z_Q}(y) \neq 0$, that is $\# F_a = 0$ or 1.

So much for that, we complete the reduction of these three constructions.

Remark:(1) Class TF has a simpler definition than these three classes recalled at subsection 3.1, 3.2 and 3.3. And the Walsh spectrum of TF functions is also simpler to compute. Notice that its size $(2^{(r^2+r)/2})^{2^s} \times 2^{2^s} = 2^{[(r^2+r)/2+1]2^s}$ is not smaller than $(2^{2^s})^t \times (2^r)^{2^s} \times 2^{2^s} = 2^{(t+r+1)2^s}$ (where $t = \lfloor r/2 \rfloor$) of GMM and lager than $[(2^r)^{2^s}]^3 \times 2^{2^s} = 2^{(3r+1)2^s}$ of Q when $r \geq 6$.

(2) The rank of the matrix $(b_{ij})_{nn}$ of these three classes, that is MM, GMM and Q, is equal to 0 or an even integer. However, the class TF's can be any integer smaller than or equal to r, therefore, our construction can generate different functions that these three constructions can't.

Conclusions

In this paper, we propose a new primary construction namely TF, which has been proved that it is a large class containing the class MM, GMM and Q. However, how to construct Plateaued functions with good properties more efficiently will be still an open problem, and we will concentrate our effort on this problem unceasingly.

Acknowledgment

We would like to thank the editors' careful reading of the manuscript and their constructive comments.

Funding

The work was supported by Natural Science Foundation of China [grant numbers 61272041].

References

[1] C. Carlet, Partially Bent functions, Designs, Codes and Cryptography, 3 (1993) 135-145.
[2] Y. Zheng, and X.M. Zhang, On Plateaued functions, IEEE Transactions on information theory, 47 (2001) 1215-1223.
[3] P. Sarkar, S.Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, in: M. Bellare (Ed.), Advances in Cryptology-CRYPTO 2000, Springer, Berlin, 2000, pp. 515-532.
[4] P. Camion, C. Carlet, P. Charpin and N. Sendrier, On Correlation-immune functions, in: M. Bellare (Ed.) Advances in Cryptology-CRYPTO'91, Springer, Berlin, 1991, pp. 86-100.
[5] C. Carlet, A larger Class of Cryptographic Boolean functions via a study of the Marorana-McFarland Construction, in: M. Bellare (Ed.) Advances in Cryptology- CRYPTO 2002, Springer, Berlin, 2002, pp. 68-100.
[6] C. Carlet, E. Prouff, On Plateaued functions and their construction, in: T. Johansson (Ed.), FSE 2003, Springer, Berlin, 2003, pp. 54-73.
[7] Y. Zheng, X.M. Zhang, Plateaued functions, in: V. Varadharajan, Y.Mu (Eds.), Advances in Cryptology-CRYPTO'99, Springer, Berlin, 1999, pp. 284-300.
[8] W.G. Zhang, E. Pasalic, Generalized Maiorana-McFarland Construction of Resilient Boolean Functions With High Nonlinearity and Good Algebraic Properties, IEEE Transactions on information theory, 60 (2014) 6681 -6695.
[9] W.Q. Wang, G.Z. Xiao, Decomposition and Construction of Plateaued Functions, Chinese Journal of Electronics, 18 (2009) 686-688.
[10] G.P. Gao, T.W. Cusick and W.F. Liu, Families of rotation symmetric functions with useful cryptographic properties, IEEE Transactions on Information Security, 8 (2014) 297-302.
[11] A. Cesmelioglu, W. Meidl, Bent Functions of Maximal Degree, IEEE Transactions on information theory, 58 (2012) 1186-1190.
[12] T.H. Yue, The characterizations of binary vector-output Plateaued functions, In: V. Varadharajan (Ed.), IEEE Transactions Conference on Networking and Information Security, IEEE Computer Society, Washington, 2010, pp. 396-400.
[13] C. Carlet, On the secondary constructions of resilient and Bent functions, Progress in Computer Science and Applied Logic, 23 (2004) 3-28.
[14] Y.V. Tarannikov, On resilient Boolean functions with maximum possible nonlinearity, in: M. Bellare, Proceedings of INDOCRYPT 2000, Springer, Berlin, 2000, pp. 19-30.
[15] W.G. Zhang, G.Z. Xiao, Constructions of almost optimal resilient Boolean functions on large even number of variables, IEEE Transactions on information theory, 55 (2009) 5822-5831.
[16] A. Canteau, P. Charpin and G.M. Kyureghyan, A new class of monomial Bent functions , Finite fields and their Applications, 14 (2008) 221-241.
[17] O.S. Rothaus, On Bent functions, Journal of Combinatorial theory, 20 (1976) 300-305.