Plateaued Functions

Yuliang Zheng[1] and Xian-Mo Zhang[2]

[1] Monash University, Frankston, Melbourne, VIC 3199, Australia
yuliang.zheng@monash.edu.au, http://www.pscit.monash.edu.au/~yuliang/
[2] The University of Wollongong, Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au

Abstract. The focus of this paper is on nonlinear characteristics of cryptographic Boolean functions. First, we introduce the notion of plateaued functions that have many cryptographically desirable properties. Second, we establish a sequence of strengthened inequalities on some of the most important nonlinearity criteria, including nonlinearity, propagation and correlation immunity, and prove that critical cases of the inequalities coincide with characterizations of plateaued functions. We then proceed to prove that plateaued functions include as a proper subset all partially-bent functions that were introduced earlier by Carlet. This settles an open question that arises from previously known results on partially-bent functions. In addition, we construct plateaued, but not partially-bent, functions that have many properties useful in cryptography.

Key Words

Bent Functions, Cryptography, Nonlinear Characteristics, Partially-Bent Functions, Plateaued Functions.

1 Motivations

In the design of cryptographic functions, one often faces the problem of fulfilling the requirements of a multiple number of nonlinearity criteria. Some of the requirements contradict others. The most notable example is perhaps bent functions — while these functions achieve the highest possible nonlinearity and satisfy the propagation criterion with respect to every non-zero vector, they are not balanced, not correlation immune and exist only when the number of variables is even.

Another example that clearly demonstrates how some nonlinear characteristics may impede others is partially-bent functions introduced in [2]. These functions include bent functions as a proper subset. Partially-bent functions are interesting in that they can be balanced and also highly nonlinear. However, except those that are bent, all partially-bent functions have non-zero linear structures, which are considered to be cryptographically undesirable.

The primary aim of this paper is to introduce a new class of functions to facilitate the design of cryptographically good functions. It turns out that these cryptographically good functions maintain all the desirable properties of partially-bent functions while possess no non-zero liner structures. This class of functions are called *plateaued functions*. To study the properties of plateaued functions, we establish a sequence of inequalities concerning nonlinear characteristics of functions. We show that plateaued functions can be characterized by the critical cases of these inequalities. In particular, we demonstrate that plateaued functions reach the upper bound on nonlinearity given by the inequalities.

We also examine relationships between plateaued functions and partially-bent functions. We show that partially-bent functions must be plateaued while that the converse is not true. This disproves a conjecture and motivates us to construct plateaued functions without non-zero linear structures. Other useful properties of plateaued functions include that they exist for both even and odd numbers of variables, can be balanced and correlation immune.

2 Boolean Functions

Definition 1. *We consider functions from V_n to $GF(2)$ (or simply functions on V_n), V_n is the vector space of n tuples of elements from $GF(2)$. Usually we write a function f on V_n as $f(x)$, where $x = (x_1, \ldots, x_n)$ is the variable vector in V_n. The* truth table *of a function f on V_n is a $(0,1)$-sequence defined by $(f(\alpha_0),\ f(\alpha_1), \ldots,\ f(\alpha_{2^n-1}))$, and the* sequence *of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$, where $\alpha_0 = (0, \ldots, 0, 0)$, $\alpha_1 = (0, \ldots, 0, 1)$, $\ldots$, $\alpha_{2^{n-1}-1} = (1, \ldots, 1, 1)$. The* matrix *of f is a $(1,-1)$-matrix of order 2^n defined by $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$ where $\oplus$ denotes the addition in $GF(2)$. f is said to be* balanced *if its truth table contains an equal number of ones and zeros.*

Given two sequences $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$, their *component-wise product* is defined by $\tilde{a} * \tilde{b} = (a_1 b_1, \cdots, a_m b_m)$ and the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as the sum of the component-wise multiplications, where the operations are defined in the underlying field. In particular, if $m = 2^n$ and $\tilde{a}$, $\tilde{b}$ are the sequences of functions f and g on V_n respectively, then $\tilde{a} * \tilde{b}$ is the sequence of $f \oplus g$ where $\oplus$ denotes the addition in $GF(2)$.

An *affine* function f on V_n is a function that takes the form of $f(x_1, \ldots, x_n) = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c$, where $\oplus$ denotes the addition in $GF(2)$ and $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

A $(1,-1)$-matrix A of order m is called a *Hadamard* matrix if $AA^T = mI_m$, where A^T is the transpose of A and I_m is the identity matrix of order m. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

$$H_0 = 1,\ H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix},\ n = 1, 2, \ldots.$$

Let ℓ_i, $0 \le i \le 2^n - 1$, be the i row of H_n. Then ℓ_i is the sequence of a linear function $\varphi_i(x)$ defined by the scalar product $\varphi_i(x) = \langle \alpha_i, x \rangle$, where $\alpha_i \in V_n$ is the binary representation of integer i, $i = 0, 1, \ldots, 2^n - 1$.

The *Hamming weight* of a $(0,1)$-sequence ξ, denoted by $W(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_n, the *Hamming distance* $d(f,g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$, where $x = (x_1, \ldots, x_n)$.

Definition 2. *The* nonlinearity *of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \varphi_i)$ where φ_1, φ_2, ..., $\varphi_{2^{n+1}}$ are all the affine functions on V_n.*

The following characterizations of nonlinearity will be useful (for a proof see for instance [6]).

Lemma 1. *The nonlinearity of f can be expressed by*

$$N_f = 2^{n-1} - \frac{1}{2} \max\{|\langle \xi, \ell_i \rangle|, 0 \le i \le 2^n - 1\}$$

where ξ is the sequence of f and ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.

Definition 3. *Let f be a function on V_n. For a vector $\alpha \in V_n$, denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Thus $\xi(0)$ is the sequence of f itself and $\xi(0) * \xi(\alpha)$ is the sequence of $f(x) \oplus f(x \oplus \alpha)$. Set $\Delta(\alpha) = \langle \xi(0), \xi(\alpha) \rangle$, the scalar product of $\xi(0)$ and $\xi(\alpha)$. $\Delta(\alpha)$ is also called the auto-correlation of f with a shift α.*

Definition 4. *Let f be a function on V_n. We say that f satisfies the* propagation criterion with respect to α *if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function, where $x = (x_1, \ldots, x_n)$ and α is a vector in V_n. Furthermore f is said to satisfy the* propagation criterion of degree k *if it satisfies the propagation criterion with respect to every non-zero vector α whose Hamming weight is not larger than k (see [7]).*

The *strict avalanche criterion (SAC)* [11] is the same as the propagation criterion of degree one.

Obviously, $\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, i.e., f satisfies the propagation criterion with respect to α.

Definition 5. *Let f be a function on V_n. $\alpha \in V_n$ is called a* linear structure *of f if $|\Delta(\alpha)| = 2^n$.*

For any function f, $\Delta(\alpha_0) = 2^n$, where $\alpha_0 = 0$, the zero vector on V_n. Hence the zero vector is a linear structure of every function on V_n. It is easy to verify that the set of all linear structures of a function f form a subspace of V_n, whose dimension is called the *linearity of f*. It is also well-known that if f has non-zero linear structures, then there exists a nonsingular $n \times n$ matrix B over $GF(2)$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y, z)$, $x \in V_n$, $y \in V_p$, $z \in V_q$, $p + q = n$, g

is a function on V_p and g has no non-zero linear structures, h is a linear function on V_q. Hence q is equal to the linearity of f.

There exist a number of equivalent definitions of correlation immune functions [1, 4]. It is easy to verify that the following definition is equivalent to Definition 2.1 of [1]:

Definition 6. *Let f be a function on V_n and let ξ be its sequence. Then f is called a* kth-order correlation immune function *if and only if $\langle \xi, \ell \rangle = 0$ for every ℓ, the sequence of a linear function $\varphi(x) = \langle \alpha, x \rangle$ on V_n constrained by $1 \leq W(\alpha) \leq k$.*

The following lemma is the re-statement of a relation proved in Section 2 of [2].

Lemma 2. *For every function f on V_n, we have*

$$(\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1}))H_n = (\langle \xi, \ell_0 \rangle^2, \langle \xi, \ell_1 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2).$$

where ℓ_i is the ith row of H_n, $j = 0, 1, \ldots, 2^n - 1$.

3 Bent Functions and Partially-bent Functions

Notation 1 *Let f be a function on V_n, ξ the sequence of f and ℓ_i denote the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Set $\Im = \{i \mid 0 \leq i \leq 2^n - 1,\ \langle \xi, \ell_i \rangle \neq 0\}$, $\Re = \{\alpha \mid \Delta(\alpha) \neq 0,\ \alpha \in V_n\}$ and $\Delta_M = \max\{|\Delta(\alpha)| | \alpha \in V_n,\ \alpha \neq 0\}$*

It is easy to verify that $\#\Im$, $\#\Re$ and Δ_M are invariant under any nonsingular linear transformation on the variables, where $\#$ denotes the cardinal number of a set.

Since $\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}$ (Parseval's equation, Page 416, [5]) and $\Delta(\alpha_0) = 2^n$, neither $\Im$ nor $\Re$ is an empty set. $\Im$ reflects the correlation immunity property of f, while $\Re$ reflects its propagation characteristics and Δ_M forecasts the avalanche property of the function. Therefore information on $\#\Im$, $\#\Re$ and Δ_M is useful in determining important cryptographic characteristics of f.

Definition 7. *A function f on V_n is called a* bent function *[8] if $\langle \xi, \ell_i \rangle^2 = 2^n$ for every $i = 0, 1, \ldots, 2^n - 1$, where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$.*

A bent function on V_n exists only when n is even, and it achieves the maximum nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$. From [8] and Parseval's equation, we have the following:

Theorem 1. *Let f be a function on V_n and ξ denote the sequence of f. Then the following statements are equivalent: (i) f is bent, (ii) for each i, $0 \leq i \leq 2^n - 1$, $\langle \xi, \ell_i \rangle^2 = 2^n$ where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$, (iii) $\#\Re = 1$, (iv) $\Delta_M = 0$, (v) the nonlinearity of f, N_f, satisfies $2^{n-1} - 2^{\frac{1}{2}n-1}$, (vi) the matrix of f is an Hadamard matrix.*

An interesting theorem of [2] explores a relationship between $\#\Im$ and $\#\Re$. This result can be expressed as follows.

Theorem 2. *For any function f on V_n, we have $(\#\Im)(\#\Re) \geq 2^n$, where the equality holds if and only if there exists a nonsingular $n \times n$ matrix B over $GF(2)$ and a vector $\beta \in V_n$ such that $f(xB \oplus \beta) = g(y) \oplus h(z)$, where $x = (y, z)$, $x \in V_n$, $y \in V_p$, $z \in V_q$, $p + q = n$, g is a bent on V_p and h is a linear function on V_q.*

Based on the above theorem, the concept of *partially-bent* functions was also introduced in the same paper [2].

Definition 8. *A function on V_n is called a* partially-bent function *if $(\#\Im)(\#\Re) = 2^n$.*

One can see that partially-bent functions include both bent functions and affine functions. Applying Theorem 2 together with properties of linear structures, or using Theorem 2 of [10] directly, we have

Proposition 1. *A function f on V_n is a partially-bent function if and only if each $|\Delta(\alpha)|$ takes the value of 2^n or 0 only. Equivalently, f is a partially-bent function if and only if $\Re$ is composed of linear structures.*

Some partially-bent functions have a high nonlinearity and satisfy the SAC or the propagation criterion of a high degree. Furthermore, some partially-bent functions are balanced. All these properties are useful in cryptography.

4 Plateaued Functions

Now we introduce a new class of functions called plateaued functions. Here is the definition.

Definition 9. *Let f be a function on V_n and ξ denote the sequence of f. If there exists an even number r, $0 \leq r \leq n$, such that $\#\Im = 2^r$ and each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, then f is called a* rth-order plateaued function *on V_n. f is also called a* plateaued function *on V_n if we ignore the particular order r.*

Due to Parseval's equation, the condition $\#\Im = 2^r$ can be obtained from the condition "each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$". For the sake of convenience, however, we mentioned both conditions in Definition 9.

The following result can be obtained immediately from Definition 9.

Proposition 2. *Let f be a function on V_n. Then we have (i) if f is a rth-order plateaued function then r must be even, (ii) f is an nth-order plateaued function if and only if f is bent, (iii) f is a 0th-order plateaued function if and only if f is affine.*

Th following is a consequence of Theorem 3 of [10].

Proposition 3. *Every partially-bent function is a plateaued function.*

In the coming sections we characterize plateaued functions and disprove the converse of Proposition 3.

5 Characterizations of Plateaued Functions

First we introduce Hölder's Inequality [3]. It states that for real numbers $a_j \geq 0$, $b_j \geq 0$, $j = 1, \ldots, k$, p and q with $p > 1$ and $\frac{1}{p} + \frac{1}{q} = 1$, the following is true: $(\sum_{j=1}^{k} a_j^p)^{1/p} (\sum_{j=1}^{k} b_j^q)^{1/q} \geq \sum_{j=1}^{k} a_j b_j$ where the quality holds if and only if there exists a constant $\nu \geq 0$ such that $a_j = \nu b_j$ for each $j = 1, \ldots, k$.

In particular, set $p = q = 2$ in Hölder's Inequality. We conclude

$$\sum_{j=1}^{k} a_j b_j \leq \sqrt{(\sum_{j=1}^{k} a_j^2)(\sum_{j=1}^{k} b_j^2)} \tag{1}$$

where the quality holds if and only if there exists a constant $\nu \geq 0$ such that $a_j = \nu b_j$ for each $j = 1, \ldots, k$.

Notation 2 *Let f be a function on V_n and ξ denote the sequence of f. Let χ denote the real valued $(0,1)$-sequence defined as $\chi = (c_0, c_1, \ldots, c_{2^n-1})$ where $c_j = \begin{cases} 1 \text{ if } \alpha_j \in \Im \\ 0 \text{ otherwise} \end{cases}$ and $\alpha_j \in V_n$, that is the binary representation of integer j. Write*

$$\chi H_n = (s_0, s_1, \ldots, s_{2^n-1}) \tag{2}$$

where each s_j is an integer.

We note that $\chi \begin{bmatrix} \langle \xi, \ell_0 \rangle^2 \\ \langle \xi, \ell_1 \rangle^2 \\ \vdots \\ \langle \xi, \ell_{2^n-1} \rangle^2 \end{bmatrix} = \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}$ where the second equality holds thanks to Parseval's equation. By using Lemma 2, we have $\chi H_n \begin{bmatrix} \Delta(\alpha_0) \\ \Delta(\alpha_1) \\ \vdots \\ \Delta(\alpha_{2^n-1}) \end{bmatrix} = 2^{2n}$. Noticing $\Delta(\alpha_0) = 2^n$, we obtain $s_0 2^n + \sum_{j=1}^{2^n-1} s_j \Delta(\alpha_j) = 2^{2n}$. Since

$$\Delta(\alpha_j) = 0 \text{ if } \alpha_j \notin \Re \tag{3}$$

$s_0 2^n + \sum_{\alpha_j \in \Re, j>0} s_j \Delta(\alpha_j) = 2^{2n}$. As $s_0 = \#\Im$, where $\#$ denotes the cardinal number of a set, we have $\sum_{\alpha_j \in \Re, j>0} s_j \Delta(\alpha_j) = 2^n(2^n - \#\Im)$. Note that

$$2^n(2^n - \#\Im) = \sum_{\alpha_j \in \Re, j>0} s_j \Delta(\alpha_j) \leq \sum_{\alpha_j \in \Re, j>0} |s_j \Delta(\alpha_j)| \leq s_M \Delta_M (\#\Re - 1) \tag{4}$$

Hence the following inequality holds.

$$s_M \Delta_M(\#\Re - 1) \geq 2^n(2^n - \#\Im) \tag{5}$$

From (2),

$$\#\Im \cdot 2^n = \sum_{j=0}^{2^n-1} s_j^2 \text{ or } \#\Im(2^n - \#\Im) = \sum_{j=1}^{2^n-1} s_j^2 \tag{6}$$

Theorem 3. *Let f be a function on V_n and ξ denote the sequence of f. Then*

$$\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) \geq \frac{2^{3n}}{\#\Im}$$

where the equality holds if and only if f is a plateaued function.

Proof. By using (4), (1) and (6), we obtain

$$\begin{aligned} 2^{2n} &\leq \sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) \leq \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| \leq \sqrt{(\sum_{\alpha_j \in \Re} s_j^2)(\sum_{\alpha_j \in \Re} \Delta^2(\alpha_j))} \\ &\leq \sqrt{(\sum_{j=0}^{2^n-1} s_j^2)(\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j))} \leq \sqrt{\#\Im 2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)} \end{aligned} \tag{7}$$

Hence $\frac{2^{3n}}{\#\Im} \leq \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)$. We have proved the inequality in the theorem.

Assume that the equality in the theorem holds i.e., $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$. This implies that all the qualities in (7) hold. Hence

$$\begin{aligned} 2^{2n} &= \sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| = \sqrt{(\sum_{\alpha_j \in \Re} s_j^2)(\sum_{\alpha_j \in \Re} \Delta^2(\alpha_j))} \\ &= \sqrt{(\sum_{j=0}^{2^n-1} s_j^2)(\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j))} = \sqrt{\#\Im 2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)} \end{aligned} \tag{8}$$

Applying the property of Hölder's Inequality to (8), we conclude that

$$|\Delta(\alpha_j)| = \nu |s_j|, \alpha_j \in \Re \tag{9}$$

where $\nu > 0$ is a constant. Applying (9) and (6) to (8), we have

$$2^{2n} = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| = \sqrt{\#\Im 2^n \nu^2 \sum_{j=0}^{2^n-1} s_j^2} = \nu \#\Im 2^n \tag{10}$$

From (10), we have $\sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)|$. Hence (9) can be expressed more accurately as follows

$$\Delta(\alpha_j) = \nu s_j, \, \alpha_j \in \Re \tag{11}$$

where $\nu > 0$ is a constant. From (8), it is easy to see that $\sum_{\alpha_j \in \Re} s_j^2 = \sum_{j=0}^{2^n-1} s_j^2$. Hence

$$s_j = 0 \text{ if } \alpha_j \notin \Re \tag{12}$$

Combining (11), (12) and (3), we have

$$\nu(s_0, s_1, \ldots, s_{2^n-1}) = (\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1})) \tag{13}$$

Comparing (13) and (2), we obtain

$$\nu \chi H_n = (\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1})) \tag{14}$$

Further comparing (14) and the equation in Lemma 2, we obtain

$$2^n \nu \chi = (\langle \xi, \ell_0 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2) \tag{15}$$

Noticing that χ is a real valued $(0,1)$-sequence, containing $\#\Im$ ones and by using Parseval's equation, we obtain $2^n \nu(\#\Im) = 2^{2n}$. Hence $\nu(\#\Im) = 2^n$, and there exists an integer r with $0 \le r \le n$ such that $\#\Im = 2^r$ and $\nu = 2^{n-r}$. From (15) it is easy to see that $\langle \xi, \ell_j \rangle^2 = 2^{2n-r}$ or 0. Hence r must be even. This proves that f is a plateaued function.

Conversely assume that f is a plateaued function. Then there exists an even number r, $0 \le r \le n$, such that $\#\Im = 2^r$ and $\langle \xi, \ell_j \rangle^2 = 2^{2n-r}$ or 0, Due to Lemma 2, we have $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = 2^{-n} \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4 = 2^{-n} \cdot 2^r \cdot 2^{4n-2r} = 2^{3n-r}$. Hence we have proved $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$.

Lemma 3. *Let f be a function on V_n and ξ denote the sequence of f. Then the nonlinearity N_f of f satisfies $N_f \le 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$, where the equality holds if and only if f is a plateaued function.*

Proof. Set $p_M = \max\{|\langle \xi, \ell_j \rangle| \mid j = 0, 1, \ldots, 2^n - 1\}$, where ℓ_j is the jth row of H_n, $0 \le j \le 2^n - 1$. Using Parseval's equation, we obtain $p_M^2 \#\Im \ge 2^{2n}$. Due to Lemma 1, $N_f \le 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$.

Assume that f is a plateaued function. Then there exists an even number r, $0 \le r \le n$, such that $\#\Im = 2^r$ and each $\langle \xi, \ell_j \rangle^2$ takes either the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$. Hence $p_M = 2^{n-\frac{1}{2}r}$. By using Lemma 1, we have $N_f = 2^{n-1} - 2^{n-\frac{1}{2}r-1} = 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$.

Conversely assume that $N_f = 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$. From Lemma 1, we have also $N_f = 2^{n-1} - \frac{1}{2} p_M$. Hence $p_M \sqrt{\#\Im} = 2^n$. Since both p_M and $\sqrt{\#\Im}$ are integers and powers of two, we can let $\#\Im = 2^r$, where r is an integer with $0 \le r \le n$. Hence $p_M = 2^{n-\frac{r}{2}}$. Obviously r is even. From Parseval's equation, $\sum_{j \in \Im} \langle \xi, \ell_j \rangle^2 = 2^{2n}$, and the fact that $p_M^2 \#\Im = 2^{2n}$, we conclude that $\langle \xi, \ell_j \rangle^2 = 2^{2n-r}$ for all $j \in \Im$. This proves that f is a plateaued function.

From the proof of Lemma 3, we can see that Lemma 3 can be stated in a different way as follows.

Lemma 4. *Let f be a function f on V_n and ξ denote the sequence of f. Set $p_M = \max\{|\langle \xi, \ell_j \rangle|| \ j = 0, 1, \ldots, 2^n - 1\}$, where ℓ_j is the jth row of H_n, $0 \leq j \leq 2^n - 1$. Then $p_M \sqrt{\#\Im} \geq 2^n$ where the equality holds if and only if f is a plateaued function.*

Summarizing Theorem 3, Lemmas 3 and 4, we conclude

Theorem 4. *Let f be a function on V_n and ξ denote the sequence of f. Set $p_M = \max\{|\langle \xi, \ell_j \rangle|| \ j = 0, 1, \ldots, 2^n - 1\}$, where ℓ_j is the jth row of H_n, $0 \leq j \leq 2^n - 1$. Then the following statements are equivalent: (i) f is a plateaued function on V_n, (ii) there exists an even number r, $0 \leq r \leq 2^n$, such that $\#\Im = 2^r$ and each $\langle \xi, \ell_j \rangle^2$ takes the value of 2^{2n-r} or 0 only, where ℓ_j denotes the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, (iii) $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$, (iv) the nonlinearity of f, N_f, satisfies $N_f = 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$, (v) $p_M \sqrt{\#\Im} = 2^n$, (vi) $N_f = 2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$.*

Proof. Due to Definition 9, Theorem 3, Lemmas 3 and 4, (i), (ii), (iii), (iv) and (v) hold. (vi) follows from (iii) and (iv).

Theorem 5. *Let f be a function on V_n and ξ denote the sequence of f. Then the nonlinearity N_f of f satisfies*

$$N_f \leq 2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$$

where the equality holds if and only if f is a plateaued function on V_n.

Proof. Set $p_M = \max\{|\langle \xi, \ell_j \rangle|| \ j = 0, 1, \ldots, 2^n - 1\}$. Multiplying the equality in Lemma 2 by itself, we have $2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4 \leq p_M^2 \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2$. Applying Parseval's equation to the above equality, we have $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) \leq 2^n p_M^2$. Hence $p_M \geq 2^{-\frac{n}{2}} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$. By using Lemma 1, we have proved the inequality $N_f \leq 2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$. The rest part of the theorem can be proved by using Theorem 4.

Theorem 3, Lemmas 3 and 4 and Theorem 4 represent characterizations of plateaued functions.

To close this section, let us note that since $\Delta(\alpha_0) = 2^n$ and $\#\Im \leq 2^n$, we have $2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)} \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ and $2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}} \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. Hence both inequalities $N_f \leq 2^{n-1} - 2^{-\frac{n}{2}-1} \sqrt{\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}$ and $N_f \leq 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$ are improvements on a more commonly used inequality $N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

6 Other Cryptographic Properties of Plateaued Functions

By using Lemma 1, we conclude

Proposition 4. *Let f be a rth-order plateaued function on V_n. Then the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{n-\frac{r}{2}-1}$.*

The following result is the same as Theorem 18 of [13].

Lemma 5. *Let f be a function on V_n ($n \geq 2$), ξ be the sequence of f, and p is an integer, $2 \leq p \leq n$. If $\langle \xi, \ell_j \rangle \equiv 0 \pmod{2^{n-p+2}}$, where ℓ_j is the jth row of H_n, $j = 0, 1, \ldots, 2^n - 1$, then the degree of f is at most $p - 1$.*

Using Lemma 5, we obtain

Proposition 5. *Let f be a rth-order plateaued function on V_n. Then the algebraic degree of f, denoted by $deg(f)$, satisfies $deg(f) \leq \frac{r}{2} + 1$.*

We note that the upper bound on degree in Proposition 5 is tight for $r < n$. For the case of $r = n$, the function, mentioned in Proposition 5, is a bent function on V_n. [8] gives a better upper bound on degree of bent function on V_n. That bound is $\frac{n}{2}$.

The following property of plateaued functions can be verified by noting their definition.

Proposition 6. *Let f be a rth-order plateaued function on V_n, B be any nonsingular $n \times n$ matrix over $GF(2)$ and α be any vector in V_n. Then $f(xB \oplus \alpha)$ is also a rth-order plateaued function on V_n.*

Theorem 6. *Let f be a rth-order plateaued function on V_n. Then the linearity of f, q, satisfies $q \leq n - r$, where the equality holds if and only if f is partially-bent.*

Proof. There exists a nonsingular $n \times n$ matrix B over $GF(2)$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y, z)$, $y \in V_p$, $z \in V_q$, $p + q = n$, g is a function on V_p and g has no non-zero linear structures, h is a linear function on V_q. Hence q is equal to the linearity of f. Set $f^*(x) = f(xB)$.

Let ξ, η and ζ denote the sequences of f^*, g and h respectively. It is easy to verify $\xi = \eta \times \zeta$, where $\times$ denotes the Kronecker product [12]. From the structure of H_n, each row of H_n, L, can be expressed as $L = \ell \times e$, where ℓ is a row of H_p and e is a row of H_q. It is easy to verify

$$\langle \xi, L \rangle = \langle \eta, \ell \rangle \langle \zeta, e \rangle \tag{16}$$

Since h is linear, ζ is a row of H_q. Replace e by ζ in (16), we have

$$\langle \xi, L' \rangle = \langle \eta, \ell \rangle \langle \zeta, \zeta \rangle = 2^q \langle \eta, \ell \rangle \tag{17}$$

where $L' = \ell \times \zeta$ is still a row of H_n.

Note that f^* is also a rth-order plateaued function on V_n. Hence $\langle \xi, L \rangle$ takes the value of $\pm 2^{n-\frac{1}{2}r}$ or zero only. Due to (17), $\langle \eta, \ell \rangle$ takes the value of $\pm 2^{n-\frac{1}{2}r-q} = \pm 2^{p-\frac{1}{2}r}$ or zero only. This proves that g is a rth-order plateaued function on V_p. Hence $r \leq p$ and $r \leq n-q$, i.e., $q \leq n-r$.

Assume that $q = n-r$. Then $p = r$. From (17), each $\langle \eta, \ell \rangle$ takes the value of $\pm 2^{\frac{r}{2}} = \pm 2^{\frac{p}{2}}$ or zero only, where ℓ is any row of H_p. Hence applying Parseval's equation to g, we can conclude that for each row ℓ of H_p, $\langle \eta, \ell \rangle$ cannot take the value of zero. In other words, for each row ℓ of H_p, $\langle \eta, \ell \rangle$ takes the value of $\pm 2^{\frac{p}{2}}$ only. Hence we have proved that g is a bent function on V_p. Due to Theorem 2, f is partially-bent. Conversely, assume that f is partially-bent. Due to Theorem 2, g is a bent function on V_p. Hence each $\langle \eta, \ell \rangle$ takes the value of $\pm 2^{\frac{p}{2}}$ only, where ℓ is any row of H_p. Note that both ζ and e are rows of H_q hence $\langle \zeta, e \rangle$ takes the value 2^q or zero only. From (16), we conclude that $\langle \xi, L \rangle$ takes the value $\pm 2^{q+\frac{p}{2}}$ or zero only. Recall f is a rth-order plateaued function on V_n. Hence $q + \frac{p}{2} = n - \frac{r}{2}$. This implies that $r = p$, i.e., $q = n-r$.

7 Relationships between Partially-bent Functions and Plateaued Functions

To examine more profound relationships between partially-bent functions and plateaued functions, we introduce one more characterization of partially-bent functions as follows.

Theorem 7. *For every function f on V_n, we have*

$$\frac{2^n - \#\Im}{\#\Im} \leq \frac{\Delta_M}{2^n}(\#\Re - 1)$$

where the equality holds if and only if f is partially-bent.

Proof. From Notation 2, we have $s_M \leq s_0 = \#\Im$. As a consequence of (5), we obtain the inequality in the theorem. Next we consider the equality in the theorem. Assume that the equality holds, i.e.,

$$\Delta_M(\#\Re - 1)\#\Im = 2^n(2^n - \#\Im) \tag{18}$$

From (4),

$$\begin{aligned} 2^n(2^n - \#\Im) &\leq \sum_{\alpha_j \in \Re, j>0} |s_j \Delta(\alpha_j)| \\ &\leq \Delta_M \sum_{\alpha_j \in \Re, j>0} |s_j| \leq \Delta_M(\#\Re - 1)\#\Im \end{aligned} \tag{19}$$

From (18), we can see that all the equalities in (19) hold. Hence

$$\Delta_M(\#\Re - 1)\#\Im = \sum_{\alpha_j \in \Re, j>0} |s_j \Delta(\alpha_j)| \tag{20}$$

Note that $|s_j| \le \#\Im$ and $|\Delta(\alpha_j)| \le \Delta_M$, for $j > 0$. Hence from (20), we obtain

$$|s_j| = \#\Im \text{ whenever } \alpha_j \in \Re \text{ and } j > 0 \tag{21}$$

and $|\Delta(\alpha_j)| = \Delta_M$ for all $\alpha_j \in \Re$ with $j > 0$.

Applying (21) to (6), and noticing $s_0 = \#\Im$, we obtain $\#\Im \cdot 2^n = \sum_{j=0}^{2^n-1} s_j^2 \ge \sum_{\alpha_j \in \Re} s_j^2 = (\#\Re)(\#\Im)^2$. This results in $2^n \ge (\#\Re)(\#\Im)$. Together with the inequality in Theorem 2, it proves that $(\#\Re)(\#\Im) = 2^n$, i.e., f is a partially-bent function.

Conversely assume that f is a partially-bent function, i.e., $(\#\Im)(\#\Re) = 2^n$. Then the inequality in the theorem is specialized as

$$\Delta_M(2^n - \#\Im) \ge 2^n(2^n - \#\Im) \tag{22}$$

We need to examine two cases. Case 1: $\#\Im = 2^n$. Obviously the equality in (22) holds. Case 2: $\#\Im \ne 2^n$. From (22), we have $\Delta_M \ge 2^n$. Thus $\Delta_M = 2^n$. This completes the proof.

Next we consider a non-bent function f. With such a function we have $\Delta_M \ne 0$. Thus from Theorem 7, we have the following result.

Corollary 1. *For every non-bent function f on V_n, we have*

$$(\#\Im)(\#\Re) \ge \frac{2^n(2^n - \#\Im)}{\Delta_M} + \#\Im$$

where the equality holds if and only if f is partially-bent (but not bent).

Proposition 7. *For every non-bent function f, we have*

$$\frac{2^n(2^n - \#\Im)}{\Delta_M} + \#\Im \ge 2^n$$

where the equality holds if and only if $\#\Im = 2^n$ or f has a non-zero linear structure.

Proof. Since $\Delta_M \le 2^n$, the inequality is obvious. On the other hand, it is easy to see that the equality holds if and only if $(2^n - \Delta_M)(2^n - \#\Im) = 0$.

From Proposition 7, one observes that for any non-bent function f, Corollary 1 implies Theorem 2.

Theorem 8. *Let f be a rth-order plateaued function. Then the following statements are equivalent: (i) f is a partially-bent function, (ii) $\#\Re = 2^{n-r}$, (iii) $\Delta_M(\#\Re - 1) = 2^{2n-r} - 2^n$, (iv) the linearity q of f satisfies $q = n - r$.*

Proof. (i) $\Longrightarrow$ (ii). Since f is a partially-bent function, we have $(\#\Im)(\#\Re) = 2^n$. As f is a rth-order plateaued function, $\#\Im = 2^r$ and hence $\#\Re = 2^{n-r}$.

(ii) $\Longrightarrow$ (iii). It is obviously true when $r = n$. Now consider the case of $r < n$. Using Theorem 7, we have $\frac{2^n - \#\Im}{\#\Im} \leq \frac{\Delta_M}{2^n}(\#\Re - 1)$ which is specialized as

$$2^{n-r} - 1 \leq \frac{\Delta_M}{2^n}(2^{n-r} - 1) \tag{23}$$

From (23) and the fact that $\Delta_M \leq 2^n$, we obtain $2^{n-r} - 1 \leq \frac{\Delta_M}{2^n}(2^{n-r} - 1) \leq 2^{n-r} - 1$. Hence $\Delta_M = 2^n$ or $r = n$. (iii) obviously holds when $\Delta_M = 2^n$. When $r = n$, we have $\#\Re = 1$ and hence (iii) also holds.

(iii) $\Longrightarrow$ (i). Note that (iii) implies $\frac{2^n - \#\Im}{\#\Im} = \frac{\Delta_M}{2^n}(\#\Re - 1)$ where $\#\Im = 2^r$. By Theorem 7, f is partially-bent.

Due to Theorem 6, (iv) $\Longleftrightarrow$ (i).

8 Construction of Plateaued Functions and Disproof of The Converse of Proposition 3

Lemma 6. *For any positive integers t and k with $k < 2^t < 2^k$, there exist 2^t non-zero vectors in V_k, say β_0, β_1, ..., β_{2^t-1}, such that for any non-zero vector $\beta \in V_k$, the 2^t-set $\{\varphi_{\beta_0}(\beta), \varphi_{\beta_1}(\beta), \ldots, \varphi_{\beta_{2^t-1}}(\beta)\}$, contains both zero and one, where φ_β is the linear function on V_k defined by $\varphi_\beta(x) = \langle \beta, x \rangle$.*

Proof. We choose k linearly independent vectors in V_k, say $\beta_1, \ldots, \beta_k$. From linear algebra, $(\langle \beta_1, \beta \rangle, \ldots, \langle \beta_k, \beta \rangle)$ goes through all the non-zero vectors in V_k exactly once while β goes through all the non-zero vectors in V_k.

Hence there exists a unique β^* satisfying $(\langle \beta_1, \beta^* \rangle, \ldots, \langle \beta_k, \beta^* \rangle) = (1, \ldots, 1)$. Furthermore, for any non-zero vector $\beta \in V_k$ with $\beta \neq \beta^*$, $\{\langle \beta_1, \beta \rangle, \ldots, \langle \beta_k, \beta \rangle\}$ contains both one and zero.

Let β_0 be a non-zero vector in V_k, such that $\langle \beta_0, \beta^* \rangle = 0$. Obviously $\beta_0 \notin \{\beta_1, \ldots, \beta_k\}$. If $2^t > k + 1$, choose other $2^t - k - 1$ non-zero vectors in V_k, $\beta_{k+1}, \ldots, \beta_{2^t-1}$, such that $\beta_0, \beta_1, \ldots, \beta_k, \beta_{k+1}, \ldots, \beta_{2^t-1}$ are mutually distinct. It is easy to see that for any non-zero vector $\beta \in V_k$, $\{\beta_0, \beta_1, \ldots, \beta_{2^t-1}\}$ contains both one and zero. This proves the lemma.

The following example proves the existence of rth-order plateaued functions on V_n, where $0 < r < n$, and disproves the converse of Proposition 3. We note that in this section, we will not discuss nth-order and 0th-order plateaued function on V_n as they are bent and affine functions respectively.

Example 1. Let t and k be positive integers with $k < 2^t < 2^k$. Let $\beta_0, \beta_1, \ldots, \beta_{2^t-1}$ be the 2^t non-zero vectors in V_k defined in Lemma 6. Let ξ_j denote the sequence of φ_{β_j}, $j = 0, 1, \ldots, 2^t - 1$. Set $\xi = \xi_0, \xi_1, \ldots, \xi_{2^t-1}$. Let $n = k + t$ and f be the function on V_n whose sequence is ξ.

By using the properties of H_n, it is easy to verify that each $\langle \xi, \ell_j \rangle$ takes the value of $\pm 2^k$ or 0 only, where ℓ_i is the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Using Parseval's equation, we obtain $\#\Im = 2^{2n-2k}$. Let $r = 2n - 2k = 2t$. Then f is a rth-order plateaued function on V_n. Due to $n = k + t$, $r = 2n - 2k = 2t$ and $t < k$, $0 < r < n$ holds.

We now consider $\Delta(\alpha)$ with the function f. Let $\alpha = (\gamma, \beta)$ where $\gamma \in V_t$, $\beta \in V_k$. Note that

$$\Delta(\alpha) = \begin{cases} \sum_{\gamma_j \oplus \gamma_i = \gamma} \langle \xi_j, \xi_i(\beta) \rangle, \text{ if } \gamma \neq 0 \\ \sum_{j=0}^{2^t-1} \langle \xi_j, \xi_j(\beta) \rangle, \quad \text{if } \gamma = 0 \text{ but } \beta \neq 0 \end{cases} \tag{24}$$

where $\gamma_j \in V_t$ is the binary representation of an integer j, $j = 0, 1, \ldots, 2^n - 1$.

Since $\varphi_{\beta_j} \neq \varphi_{\beta_i}$ if $j \neq i$, where $\varphi_\beta(x) = \langle \beta, x \rangle$, $\varphi_{\beta_j}(x) \oplus \varphi_{\beta_i}(x \oplus \beta)$ is a non-zero linear function and hence balanced. We have now proved $\langle \xi_j, \xi_i(\beta) \rangle = 0$ for $j \neq i$. Hence $\Delta(\alpha) = 0$ when $\gamma \neq 0$.

On the other hand, for any linear function φ on V_k, we have $\varphi(x) \oplus \varphi(x \oplus \beta) = \varphi(\beta)$. Hence $\langle \xi_j, \xi_j(\beta) \rangle = 2^k$ if and only if $\varphi_{\beta_j}(\beta) = 0$. In addition, $\langle \xi_j, \xi_j(\beta) \rangle = -2^k$ if and only if $\varphi_{\beta_j}(\beta) = 1$. By using Lemma 6, we have $\Delta(\alpha) = \sum_{j=0}^{2^t-1} \langle \xi_j, \xi_j(\beta) \rangle \neq \pm 2^t \cdot 2^k = \pm 2^n$ for $\beta \neq 0$.

In summary, we have

$$\Delta(\alpha) \begin{cases} = 0 & \text{if } \gamma \neq 0 \\ \neq \pm 2^n & \text{if } \gamma = 0 \text{ and } \beta \neq 0 \\ = 2^n & \text{if } \alpha = 0 \end{cases} \tag{25}$$

Since f is a rth-order plateaued function on V_n and $r < n$, f is not bent, on the other hand, (25) shows that f has non-zero linear structures. Hence we conclude that f is not partially-bent. Hence we have proved that f is plateaued but not partially-bent. This disproves the converse of Proposition 3.

f has some other interesting properties. In particular, due to Proposition 4, the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{n-\frac{r}{2}-1}$. Note that the sequence of any non-zero linear function is $(1, -1)$-balanced. Hence each ξ_j and $\xi = \xi_0, \xi_1, \ldots, \xi_{2^t-1}$ are $(1, -1)$-balanced. This implies that f is $(0, 1)$-balanced. Since the function f is not partially-bent, by using Theorem 2, we have $(\#\Im)(\#\Re) > 2^n$. This proves that $\#\Re > 2^{n-r}$. On the other hand, from (25), we have $\#\Re \leq 2^k = 2^{n-\frac{1}{2}r}$. Thus we can conclude that $2^{n-r} < \#\Re \leq 2^{n-\frac{1}{2}r}$.

We end this example by noting that such functions as f exist on V_n both for n even and odd.

Now we summarize the relationships among bent, partially-bent and plateaued functions. Let $\mathbf{B_n}$ denote the set of bent functions on V_n, $\mathbf{P_n}$ denote the set of partially-bent functions on V_n and $\mathbf{F_n}$ denote the set of plateaued functions on V_n. Then the above results imply that $\mathbf{B_n} \subset \mathbf{P_n} \subset \mathbf{F_n}$, where $\subset$ denotes the relationship of proper subset. We further let $\mathbf{G_n}$ denote the set of plateaued functions on V_n that do *not* have non-zero linear structures and are not bent functions. The relationships among these classes of functions are shown in Figure 1. Example 1 proves that $\mathbf{G_n}$ is nonempty.

Next we consider how to improve the function in Example 1 so as to obtain a rth-order plateaued function on V_n satisfying the SAC and all the properties mentioned in Example 1.

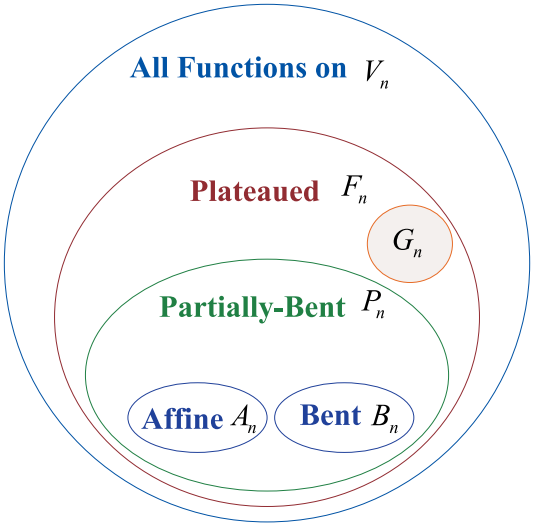

Fig. 1. Relationship among bent, partially bent, and plateaued functions

Example 2. Note that if $r > 2$, i.e., $t > 1$, then from Example 1, $\#\Re \le 2^{n-\frac{1}{2}r} < 2^{n-1}$. In other words, $\#\Re^c > 2^{n-1}$ where $\Re^c$ denotes the complementary set of $\Re$. Hence there exist n linearly independent vectors in $\Re^c$. In other words, there exist n linearly independent vectors with respect to which f satisfies the propagation criterion. Hence we can choose a nonsingular $n \times n$ matrix A over $GF(2)$ such that $g(x) = f(xA)$ satisfies the SAC (see [9]). The nonsingular linear transformation A does not alter any of the properties of f in Example 1

We can further improve the function in Example 2 so as to obtain a rth-order plateaued functions on V_n having the highest degree and satisfying all the properties in Example 1.

Example 3. Given any vector $\delta = (i_1, \ldots, i_s) \in V_t$, we define a function on V_t by $D_\delta(y) = (y_1 \oplus \bar{i_1}) \cdots (y_t \oplus \bar{i_s})$ where $y = (y_1, \ldots, y_t)$ and $\bar{i} = 1 \oplus i$ indicates the binary complement of i.

Let $\xi_{i_1 \cdots i_p}$, $(i_1, \ldots, i_p) \in V_p$, be the sequence of a function $f_{i_1 \cdots i_p}(x_1, \ldots, x_q)$ on V_q. Let ξ be the concatenation of $\xi_{0\cdots00}$, $\xi_{0\cdots01}$, $\ldots$, $\xi_{1\cdots11}$, namely, $\xi = (\xi_{0\cdots00}, \xi_{0\cdots01}, \ldots, \xi_{1\cdots11})$. It is easy to verify that ξ is the sequence of a function on V_{q+p} given by

$$f(y_1, \ldots, y_p, z_1, \ldots, z_q) = \bigoplus_{(i_1 \cdots i_p) \in V_p} D_{i_1 \cdots i_p}(y_1, \ldots, y_p) f_{i_1 \cdots i_p}(z_1, \ldots, z_q). \quad (26)$$

Let $\delta_j \in V_t$ is the binary representation of integer j, $j = 0, 1, \ldots, 2^t - 1$. Write $\psi_{\delta_0} = \varphi_{\beta_0}$, $\psi_{\delta_1} = \varphi_{\beta_1}$, $\ldots$, $\psi_{\delta_{2^t-1}} = \varphi_{\beta_{2^t-1}}$, where $\beta_0, \beta_1, \ldots, \beta_{2^t-1}$ are the same with those in Example 1 and $\varphi_\beta = \langle \beta, x \rangle$.

Due to (26), the function f on V_{t+k}, mentioned in Example 1 can be expressed as $f(y,z) = \bigoplus_{\delta \in V_t} D_\delta(y)\psi_\delta(z)$.

Case 1: $\bigoplus_{\delta \in V_t} \psi_\delta \neq 0$. Write $\bigoplus_{\delta \in V_t} \psi_\delta = \psi$, where ψ must be a non-zero linear function on V_k. Note that each $D_\delta(y)$ contains $y_1 \cdots y_t$. Hence the term $y_1 \cdots y_t \psi(z)$ survives in the final algebraic normal form representation of $f(y,z)$ and hence the degree of f is $t+1 = \frac{r}{2}+1$.

Case 2: $\bigoplus_{\delta \in V_t} \psi_\delta = 0$, i.e., $\bigoplus_{j=0}^{2^t-1} \varphi_{\beta_j} = 0$. Note that there exist $2^k - 1$ non-zero vectors in V_k and $2^k - 1 > 2^t$. Hence we can replace $\varphi_{\beta_{2^t-1}}$ by any non-zero linear function φ on V_k, that differs from $\varphi_{\beta_0}, \varphi_{\beta_1}, \ldots \varphi_{\beta_{2^t-1}}$. This reduces Case 2 to Case 1.

We have now constructed a rth-order plateaued function with degree $\frac{r}{2} + 1$. Applying the discussions in Examples 1 and 2, we can obtain a rth-order plateaued function on V_n having degree $\frac{r}{2}+1$ and satisfying all the properties of the function constructed in Example 1.

It should be noted that the function in this example achieves the highest possible algebraic degree given in Proposition 4. Thus the upper bound on the algebraic degree of plateaued functions, mentioned in Proposition 5, is tight.

9 Conclusions

We have introduced and characterized a new class of functions called plateaued functions. These functions bring together various nonlinear characteristics. We have also shown that partially-bent functions are a proper subset of plateaued functions, which settles an open problem related to partially-bent functions. We have further demonstrated methods for constructing plateaued functions that have many cryptographically desirable properties.

Acknowledgement

The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

1. P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91*, volume 576, Lecture Notes in Computer Science, pages 87–100. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
2. Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3:135–145, 1993.
3. Friedhelm Erwe. *Differential And Integral Calculus*. Oliver And Boyd Ltd, Edinburgh And London, 1967.
4. Xiao Guo-Zhen and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, 1988.

5. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.
6. W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.
7. B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.
8. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
9. J. Seberry, X. M. Zhang, and Y. Zheng. Improving the strict avalanche characteristics of cryptographic functions. *Information Processing Letters*, 50:37–41, 1994.
10. J. Wang. The linear kernel of boolean functions and partially-bent functions. *System Science and Mathematical Science*, 10:6–11, 1997.
11. A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.
12. R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.
13. X. M. Zhang, Y. Zheng, and Hideki Imai. Duality of boolean functions and its cryptographic significance. In *Advances in Cryptology - ICICS'97*, volume 1334, Lecture Notes in Computer Science, pages 159–169. Springer-Verlag, Berlin, Heidelberg, New York, 1997.