On Plateaued Functions

Yuliang Zheng, *Senior Member, IEEE,* and Xian-Mo Zhang

***Abstract*—The focus of this correspondence 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, avalanche, 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 Claude Carlet. This solves an interesting problem that arises naturally 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.**

***Index Terms*—Bent functions, cryptography, nonlinear characteristics, partially bent functions, plateaued functions.**

I. 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 avalanche criterion with respect to every nonzero 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 [1]. 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 nonzero linear structures, which are considered to be cryptographically undesirable.

The primary aim of this correspondence is to introduce a new class of functions to facilitate the design of cryptographically good functions. It turns out that some of these cryptographically good functions can maintain all the desirable properties of partially bent functions while not possessing nonzero linear structures. This new class of functions are called *plateaued functions*. To study the properties of plateaued functions, we establish a sequence of inequalities concerning nonlinear characteristics. 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 the converse is not true. Other useful properties of plateaued functions include that they exist both for even and odd numbers of variables, can be balanced and correlation-immune.

The remaining part of the correspondence is organized as follows. Section II introduces basic concepts on Boolean functions that are used. Section III surveys properties of bent functions and partially bent functions that are relevant to this work. This is followed by Sections IV, where the concept of plateaued functions is introduced. Important properties of plateaued functions are studied in Sections V and VI. Section VII investigates relationships between plateaued functions and partially bent functions, while Section VIII shows methods for constructing plateaued functions that have useful cryptographic properties, such as balance, high algebraic degree, strict avalanche criterion (SAC), and correlation immunity. Finally, Section IX closes the correspondence with a pointer to some latest developments in the research into plateaued functions.

II. Boolean Functions

We consider functions from V_n to $\mathrm{GF}(2)$ (or simply functions on V_n), where V_n is the vector space of n tuples of elements from $\mathrm{GF}(2)$. 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

$$\alpha_0 = (0, \ldots, 0, 0)$$
$$\alpha_1 = (0, \ldots, 0, 1), \ldots, \alpha_{2^n-1} = (1, \ldots, 1, 1).$$

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 V_n. f is said to be *balanced* if its truth table contains an equal number of ones and zeros.

Given two sequences $\tilde{a} = (a_1, \ldots, a_m)$ and $\tilde{b} = (b_1, \ldots, b_m)$, their *componentwise product* is defined by $\tilde{a} * \tilde{b} = (a_1 b_1, \ldots, a_m b_m)$ 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 componentwise 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 $\mathrm{GF}(2)$.

Manuscript received September 21, 1999; revised February 25, 2000. The work of X.-M. Zhang was supported by a Queen Elizabeth II Fellowship (227 23 1002). The material in this correspondence was presented in part as "Plateaued Functions" at ICICS'99, Sydney, Australia, November 9–11, 1999.

Y. Zheng is with the School of Network Computing, Monash University, Frankston, Melbourne, Vic. 3199, Australia (e-mail: yuliang.zheng@monash.edu.au).

X.-M. Zhang is with the School of Information Technology and Computer Science, University of Wollongong, Wollongong, NSW 2522, Australia (e-mail: xianmo@cs.uow.edu.au).

Communicated by D. R. Stinson, Associate Editor for Complexity and Cryptography.

Publisher Item Identifier S 0018-9448(01)01348-7.

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:

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

Let ℓ_i, $0 \le i \le 2^n - 1$, be the ith 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 $\alpha_i \in V_n$ corresponds to the binary representation of an integer i, $i = 0, 1, \ldots, 2^n - 1$.

The *Hamming weight* of a $(0, 1)$-sequence ξ, denoted by HW(ξ), 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 1: 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., $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \psi_i)$, where $\psi_1, \psi_2, \ldots, \psi_{2^{n+1}}$ are all the affine functions on V_n.

The following characterization of nonlinearity will be useful (for a proof see for instance [2]).

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 2: 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 autocorrelation of f with a shift α.

Definition 3: Let f be a function on V_n. We say that f satisfies the *avalanche 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 *avalanche criterion of degree* k if it satisfies the avalanche criterion with respect to every nonzero vector α whose Hamming weight is not larger than k (see [3]).

The *strict avalanche criterion (SAC)* [4] is the same as the avalanche 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 avalanche criterion with respect to α.

Definition 4: 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 known 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 nonzero 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 that does not have nonzero linear structures, and 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 [5], [6]. The following definition is closely related to[5, Definition 2.1].

Definition 5: 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 $\langle \xi, \ell\rangle = 0$ for every ℓ, the sequence of a linear function $\varphi(x) = \langle \alpha, x\rangle$ on V_n constrained by $1 \le W(\alpha) \le k$.

The following lemma is the restatement of a relation proved in [1, Sec. II].

Lemma 2: For every function f on V_n, we have

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

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

III. 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

$$\Im = \{i \mid 0 \le i \le 2^n - 1, \langle \xi, \ell_i\rangle \ne 0\}$$
$$\Re = \{\alpha \mid \Delta(\alpha) \ne 0, \alpha \in V_n\}$$

and

$$\Delta_M = \max\{|\Delta(\alpha)|, \alpha \in V_n - \{0\}\}.$$

Note that to be more precise, $\Im$, $\Re$, and Δ_M should have been written as $\Im_f$, $\Re_f$, and $\Delta_{M,f}$, respectively. The subscript is omitted when no confusion occurs.

$\Im$, $\Re$, and Δ_M share an interesting property. Namely, $\#\Im$, $\#\Re$, and Δ_M are invariant under any nonsingular linear transformation on the variables, where $\#$ denotes the cardinal number of a set.

Parseval's equation states that

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j\rangle^2 = 2^{2n}$$

([7, p. 416]). Noticing $\Delta(\alpha_0) = 2^n$, we can see that neither $\Im$ nor $\Re$ is an empty set. $\Im$ reflects the correlation-immune property of f, while $\Re$ reflects its avalanche characteristics and Δ_M forecasts its avalanche property. Therefore, information on $\#\Im$, $\#\Re$, and Δ_M is useful in investigating cryptographic characteristics of f.

Definition 6: 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.

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

vi) the matrix of f is an Hadamard matrix.

An interesting theorem of [1] 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 function 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 [1].

Definition 7: 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 [9, Theorem 2] directly, we have the following.

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 are highly nonlinear and satisfy the SAC. Furthermore, some partially bent functions are balanced. All these properties are useful in cryptography.

IV. Plateaued Functions

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

Definition 8: 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 an r*th-order plateaued function* on V_n. f is also simply called a *plateaued function* on V_n if we ignore the particular order r.

Due to Parseval's equation, the condition that $\#\Im = 2^r$ can be obtained from the condition that "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 have mentioned both conditions in Definition 8.

The following result can be obtained immediately from Definition 8.

Proposition 2: Let f be a function on V_n. Then we have

i) if f is an 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.

To help understand the definition of plateaued functions together with their relationships with affine and bent functions, profiles of $|\langle \xi, \ell_j \rangle|$, $j = 0, 1, \ldots, 2^n - 1$, of plateaued functions are depicted in Fig. 1. The following is a consequence of [9, Theorem 3].

Proposition 3: Every partially bent function is a plateaued function.

An interesting question that arises naturally from Proposition 3 is whether a plateaued function is also partially bent. In the following sections, we characterize plateaued functions and disprove the converse of the proposition.

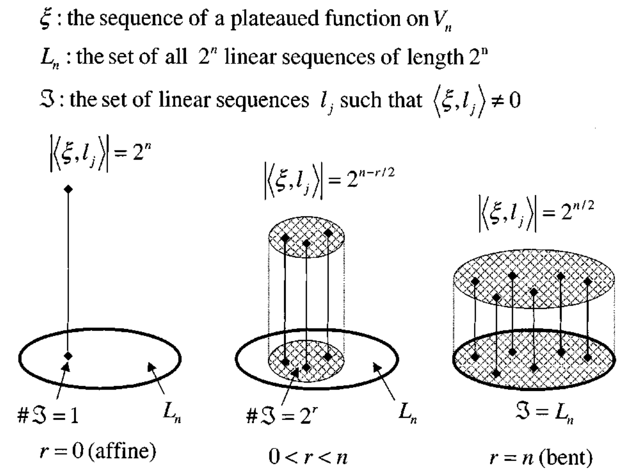

Fig. 1. Profiles of $|\langle \xi, \ell_j \rangle|$ of plateaued (including affine and bent) functions.

V. Characterizations of Plateaued Functions

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

$$c_j = \begin{cases} 1, & \text{if } j \in \Im \\ 0, & \text{otherwise} \end{cases}$$

and $\alpha_j \in V_n$ is the binary representation of an integer j. Write

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

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

$$\Delta(\alpha_j) = 0, \qquad \text{if } \alpha_j \notin \Re \tag{2}$$

we have

$$s_0 2^n + \sum_{\alpha_j \in \Re,\, j>0} s_j \Delta(\alpha_j) = 2^{2n}.$$

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

$$\begin{aligned} 2^n(2^n - \#\Im) &= \sum_{\alpha_j \in \Re,\, j>0} s_j \Delta(\alpha_j) \\ &\leq \sum_{\alpha_j \in \Re,\, j>0} |s_j \Delta(\alpha_j)| \\ &\leq s_M \Delta_M (\#\Re - 1) \end{aligned} \tag{3}$$

where $s_M = \max\{|s_j|, 0 < j \le 2^n - 1\}$. Hence, the following inequality holds:

$$s_M \Delta_M(\#\Re - 1) \ge 2^n(2^n - \#\Im). \tag{4}$$

From (1), we obtain

$$\#\Im \cdot 2^n = \sum_{j=0}^{2^n-1} s_j^2$$

or

$$\#\Im(2^n - \#\Im) = \sum_{j=1}^{2^n-1} s_j^2. \tag{5}$$

Now we prove the first inequality that helps us understand properties of plateaued functions.

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

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

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

Proof: By using (3), the property of Hölder's inequality [10], and (5), we obtain

$$\begin{aligned} 2^{2n} &= \sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) \le \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| \\ &\le \sqrt{\left(\sum_{\alpha_j \in \Re} s_j^2\right)\left(\sum_{\alpha_j \in \Re} \Delta^2(\alpha_j)\right)} \\ &\le \sqrt{\left(\sum_{j=0}^{2^n-1} s_j^2\right)\left(\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)\right)} \\ &= \sqrt{\#\Im 2^n \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)}. \end{aligned} \tag{6}$$

Hence $\frac{2^{3n}}{\#\Im} \le \sum_{j=0}^{2^n-1} \Delta^2(\alpha_j)$. 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 equalities in (6) hold. Hence

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

Applying the property of Hölder's inequality to (7), we conclude that

$$|\Delta(\alpha_j)| = \nu |s_j|, \qquad \alpha_j \in \Re \tag{8}$$

where $\nu > 0$ is a constant. Applying (8) and (5) to (7), we have

$$2^{2n} = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)| = \sqrt{\#\Im 2^n \nu^2 \sum_{j=0}^{2^n-1} s_j^2} = \nu \#\Im 2^n. \tag{9}$$

From (7), we have

$$\sum_{\alpha_j \in \Re} s_j \Delta(\alpha_j) = \sum_{\alpha_j \in \Re} |s_j \Delta(\alpha_j)|.$$

Hence, (8) can be expressed more accurately as follows:

$$\Delta(\alpha_j) = \nu s_j, \qquad \alpha_j \in \Re \tag{10}$$

where $\nu > 0$ is a constant. From (7), it is easy to see that

$$\sum_{\alpha_j \in \Re} s_j^2 = \sum_{j=0}^{2^n-1} s_j^2.$$

Hence

$$s_j = 0, \qquad \text{if } \alpha_j \notin \Re. \tag{11}$$

Combining (10), (11), and (2), we have

$$\nu(s_0, s_1, \ldots, s_{2^n-1}) = (\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1})). \tag{12}$$

Noting (1), we obtain

$$\nu \chi H_n = (\Delta(\alpha_0), \Delta(\alpha_1), \ldots, \Delta(\alpha_{2^n-1})). \tag{13}$$

Furthermore, noting the equation in Lemma 2, we obtain

$$2^n \nu \chi = \left(\langle \xi, \ell_0 \rangle^2, \ldots, \langle \xi, \ell_{2^n-1} \rangle^2\right). \tag{14}$$

It should be pointed out that χ is a real-valued $(0, 1)$-sequence, containing $\#\Im$ ones. 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 (14), 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. Considering 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 that $\sum_{j=0}^{2^n-1} \Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$. □

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

$$p_M = \max\{|\langle \xi, \ell_j \rangle|, \ j = 0, 1, \ldots, 2^n - 1\}$$

where ℓ_j is the jth row of H_n. Using Parseval's equation, we obtain $p_M^2 \#\Im \ge 2^{2n}$. Due to Lemma 1, we obtain

$$N_f \le 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}.$$

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, $p_M = 2^{n-\frac{1}{2}r}$. Once again noting 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, more importantly, 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, $\sum_{j\in\Im}\langle\xi, \ell_j\rangle^2 = 2^{2n}$, together with 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. Then $p_M\sqrt{\#\Im} \ge 2^n$, 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. Then the following statements are equivalent:

i) f is a plateaued function on V_n;
ii) $\sum_{j=0}^{2^n-1}\Delta^2(\alpha_j) = \frac{2^{3n}}{\#\Im}$;
iii) the nonlinearity of f, N_f, satisfies $N_f = 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$;
iv) $p_M\sqrt{\#\Im} = 2^n$;
v) $N_f = 2^{n-1} - 2^{-\frac{n}{2}-1}\sqrt{\sum_{j=0}^{2^n-1}\Delta^2(\alpha_j)}$.

Proof: Due to Theorem 3, Lemmas 3 and 4, i)-iv) hold. v) follows from ii) and iii). □

We now proceed to prove the second inequality that relates $\Delta(\alpha_j)$ to nonlinearity.

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

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

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

$$2^n\sum_{j=0}^{2^n-1}\Delta^2(\alpha_j) = \sum_{j=0}^{2^n-1}\langle\xi, \ell_j\rangle^4 \le p_M^2\sum_{j=0}^{2^n-1}\langle\xi, \ell_j\rangle^2.$$

Applying Parseval's equation to the above equality, we have

$$\sum_{j=0}^{2^n-1}\Delta^2(\alpha_j) \le 2^n p_M^2.$$

Hence

$$p_M \ge 2^{-\frac{n}{2}}\sqrt{\sum_{j=0}^{2^n-1}\Delta^2(\alpha_j)}.$$

Thanks to Lemma 1, we have proved the inequality

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

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 $\#\Im \le 2^n$, we have

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

and

$$2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}} \le 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Hence both inequalities

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

and

$$N_f \le 2^{n-1} - \frac{2^{n-1}}{\sqrt{\#\Im}}$$

are improvements on a more commonly used inequality

$$N_f \le 2^{n-1} - 2^{\frac{n}{2}-1}.$$

VI. Other Cryptographic Properties of Plateaued Functions

Lemma 1 implies that the following statement holds.

Proposition 4: Let f be an 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 [11, Theorem 18].

Lemma 5: Let f be a function on V_n $(n \ge 2)$, ξ be the sequence of f, and p is an integer, $2 \le p \le n$. 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 algebraic degree of f is at most $p-1$.

Using Lemma 5, we obtain:

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

We note that the upper bound on algebraic degree in Proposition 5 is tight for $r < n$. For the case of $r = n$, the nth-order plateaued function is a bent function on V_n. Reference [8] gives a better upper bound on the algebraic degree of a 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 an 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 an rth-order plateaued function on V_n.

Next we show that rth-order plateaued functions have the property that their linearity is bounded from above by $n - r$.

Theorem 6: Let f be an rth-order plateaued function on V_n. Then the linearity of f, denoted by q, satisfies $q \le n - r$, 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 that does not have nonzero linear structures, and 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. Then, $\xi = \eta \times \zeta$, where $\times$ denotes the Kronecker product [12]. From the structure of H_n, we know that each row L of H_n can be expressed as $L = \ell \times e$, where ℓ is a row of H_p and e is a row of H_q. Then we have

$$\langle \xi, L\rangle = \langle \eta, \ell\rangle\langle \zeta, e\rangle. \tag{15}$$

Since h is linear, ζ must be a row of H_q. Replacing e by ζ in (15), we have

$$\langle \xi, L'\rangle = \langle \eta, \ell\rangle\langle \zeta, \zeta\rangle = 2^q\langle \eta, \ell\rangle \tag{16}$$

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

Note that f^* is also an rth-order plateaued function on V_n. Hence, $\langle \xi, L\rangle$ takes the value of $\pm 2^{n-\frac{1}{2}r}$ or 0 only. Due to (16), $\langle \eta, \ell\rangle$ takes the value of $\pm 2^{n-\frac{1}{2}r-q} = \pm 2^{p-\frac{1}{2}r}$ or 0 only. This proves that g is an rth-order plateaued function on V_p. Hence $r \le p$ and $r \le n - q$, i.e., $q \le n - r$.

Assume that $q = n - r$. Then $p = r$. From (16), each $\langle \eta, \ell\rangle$ takes the value of $\pm 2^{\frac{r}{2}} = \pm 2^{\frac{p}{2}}$ or 0 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. As both ζ and e are rows of H_q, $\langle \zeta, e\rangle$ takes the value 2^q or 0 only. From (15), we conclude that $\langle \xi, L\rangle$ takes the value $\pm 2^{q+\frac{p}{2}}$ or 0 only. Recall that f is an rth-order plateaued function on V_n. Hence, $q + \frac{p}{2} = n - \frac{r}{2}$. This implies that $r = p$, i.e., $q = n - r$. $\square$

VII. Relationships Between Partially Bent Functions and Plateaued Functions

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

Theorem 7: For every function f on V_n, we have

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

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

Proof: From Notation 2, we have $s_M \le s_0 = \#\Im$. As a consequence of (4), we obtain the inequality in the theorem. Next we consider the equality in the theorem. Assume that the equality holds, i.e.,

$$\Delta_M(\#\Re - 1)\#\Im = 2^n(2^n - \#\Im). \tag{17}$$

From (3), we have

$$\begin{aligned} 2^n(2^n - \#\Im) &\le \sum_{\alpha_j\in\Re,\, j>0} |s_j\Delta(\alpha_j)| \\ &\le \Delta_M \sum_{\alpha_j\in\Re,\, j>0} |s_j| \\ &\le \Delta_M(\#\Re - 1)\#\Im. \end{aligned} \tag{18}$$

From (17), we can see that all the equalities in (18) hold. Hence,

$$\Delta_M(\#\Re - 1)\#\Im = \sum_{\alpha_j\in\Re,\, j>0} |s_j\Delta(\alpha_j)|. \tag{19}$$

Note that $|s_j| \le \#\Im$ and $|\Delta(\alpha_j)| \le \Delta_M$, for $j > 0$. Hence, from (19), we obtain

$$|s_j| = \#\Im, \qquad \text{whenever } \alpha_j \in \Re \text{ and } j > 0 \tag{20}$$

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

Applying (20) to (5), and noticing that $s_0 = \#\Im$, 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

$$\Delta_M(2^n - \#\Im) \ge 2^n(2^n - \#\Im). \tag{21}$$

We need to examine two cases. Case 1: $\#\Im = 2^n$. Obviously, the equality in (21) holds. Case 2: $\#\Im \ne 2^n$. From (21), we have $\Delta_M \ge 2^n$. Thus, $\Delta_M = 2^n$. This completes the proof. $\square$

Next we consider a nonbent 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 nonbent 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 nonbent 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 nonzero 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

$$(2^n - \Delta_M)(2^n - \#\Im) = 0. \qquad \square$$

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

Theorem 8: Let f be an 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 also an rth-order plateaued function, $\#\Im = 2^r$ and hence $\#\Re = 2^{n-r}$.

ii) $\Longrightarrow$ iii). When $r = n$, we have $\#\Re = 1$ and hence iii) holds. For the case of $r < n$, using Theorem 7, we have

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

which is specialized as

$$2^{n-r} - 1 \le \frac{\Delta_M}{2^n}\,(2^{n-r} - 1). \tag{22}$$

From (22) and the fact that $\Delta_M \le 2^n$, we obtain

$$2^{n-r} - 1 \le \frac{\Delta_M}{2^n}(2^{n-r} - 1) \le 2^{n-r} - 1.$$

Hence $\Delta_M = 2^n$. Since ii) holds, we have $\Delta_M(\#\Re - 1) = 2^{2n-r} - 2^n$.

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, we have iv) $\Longleftrightarrow$ i). □

VIII. Construction of Plateaued Functions and Disproof of the Converse of Proposition 3

A. Existence of Balanced rth-Order Plateaued Functions and Disproof of The Converse of Proposition 3

Lemma 6: For any integer k with $k \ge 2$, there exist $k+1$ nonzero vectors in V_k, say $\gamma_0, \gamma_1, \ldots, \gamma_k$, such that for any nonzero vector $\gamma \in V_k$, we have

$$(\langle \gamma_0, \gamma \rangle, \langle \gamma_1, \gamma \rangle, \ldots, \langle \gamma_k, \gamma \rangle) \ne (0, 0, \ldots, 0)$$

and

$$(\langle \gamma_0, \gamma \rangle, \langle \gamma_1, \gamma \rangle, \ldots, \langle \gamma_k, \gamma \rangle) \ne (1, 1, \ldots, 1).$$

Proof: We choose k linearly independent vectors in V_k, say $\gamma_1, \ldots, \gamma_k$. From linear algebra, $(\langle \gamma_1, \gamma \rangle, \ldots, \langle \gamma_k, \gamma \rangle)$ goes through all the nonzero vectors in V_k exactly once while γ goes through all the nonzero vectors in V_k.

Hence, there exists a unique γ^* satisfying

$$(\langle \gamma_1, \gamma^* \rangle, \ldots, \langle \gamma_k, \gamma^* \rangle) = (1, \ldots, 1).$$

As a consequence, for any nonzero vector $\gamma \in V_k$ with $\gamma \ne \gamma^*$, $\{\langle \gamma_1, \gamma \rangle, \ldots, \langle \gamma_k, \gamma \rangle\}$ contains both one and zero.

Let γ_0 be a nonzero vector in V_k, such that $\langle \gamma_0, \gamma^* \rangle = 0$. Obviously, $\gamma_0 \notin \{\gamma_1, \ldots, \gamma_k\}$. It is easy to see that $\gamma_0, \gamma_1, \ldots, \gamma_k$ satisfy the property in the lemma. □

Let t and k be positive integers with $k < 2^t < 2^k$. Set $n = t + k$ and $r = 2n - 2k = 2t$. We now prove the existence of balanced rth-order plateaued functions on V_n and disproves the converse of Proposition 3. In this section, we will not discuss nth-order and 0th-order plateaued function on V_n as they are simply bent and affine functions, respectively.

Since $t < k$, there exists a mapping P from V_t to V_k satisfying

i) $P(\beta) \ne P(\beta')$ if $\beta \ne \beta'$;

ii) $\gamma_0, \gamma_1, \ldots, \gamma_k \in P(V_t)$, where $P(V_t) = \{P(\beta) | \beta \in V_t\}$;

iii) $0 \notin P(V_t)$ where 0 denotes the zero vector in V_k.

We define a function f on V_{t+k} as follows:

$$f(x) = f(y, z) = P(y)z^T \tag{23}$$

where $x = (y, z)$, $y \in V_t$, and $z \in V_k$. Denote the sequence of f by ξ.

Let L be a row of H_{t+k}. Hence, $L = e \times \ell$ where e is a row of H_t and ℓ is a row of H_k. Once again from the properties of Sylvester–Hadamard matrices, L is the sequence of a linear function V_{t+k}, denoted by ψ, $\psi(x) = \langle \alpha, x \rangle$, $\alpha = (\beta, \gamma)$, and $x = (y, z)$ where $y, \beta \in V_t$ and $z, \gamma \in V_k$. Hence, $\psi(x) = \langle \beta, y \rangle \oplus \langle \gamma, z \rangle$.

Note that

$$\begin{aligned}
\langle \xi, L \rangle &= \sum_{y \in V_t,\, z \in V_k} (-1)^{P(y)z^T \oplus \langle \beta, y \rangle \oplus \langle \gamma, z \rangle} \\
&= \sum_{y \in V_t} (-1)^{\langle \beta, y \rangle} \sum_{z \in V_k} (-1)^{(P(y) \oplus \gamma) z^T} \\
&= 2^k \sum_{P(y) = \gamma} (-1)^{\langle \beta, y \rangle} \\
&= \begin{cases} 2^k (-1)^{\langle \beta, P^{-1}(\gamma) \rangle}, & \text{if } P^{-1}(\gamma) \text{ exists} \\ 0, & \text{otherwise.} \end{cases}
\end{aligned} \tag{24}$$

Thus, f is an rth-order plateaued function on V_n.

Next we prove that f has no nonzero linear structures. Let $\alpha = (\beta, \gamma)$ be a nonzero vector in V_{t+k} where $\beta \in V_t$ and $\gamma \in V_k$

$$\begin{aligned}
\Delta(\alpha) &= \langle \xi, \xi(\alpha) \rangle \\
&= \sum_{y \in V_t,\, z \in V_k} (-1)^{P(y)z^T \oplus P(y \oplus \beta)(z \oplus \gamma)^T} \\
&= \sum_{y \in V_t} (-1)^{P(y \oplus \beta)\gamma^T} \sum_{z \in V_k} (-1)^{(P(y) \oplus P(y \oplus \beta)) z^T}.
\end{aligned} \tag{25}$$

There exist two cases to be considered: $\beta \ne 0$ and $\beta = 0$. When $\beta \ne 0$, due to the property i) of P, we have $P(y) \ne P(y \oplus \beta)$. Hence we have

$$\sum_{z \in V_k} (-1)^{(P(y) \oplus P(y \oplus \beta)) z^T} = 0$$

from which it follows that $\Delta(\alpha) = 0$. On the other hand, when $\beta = 0$, we have

$$\Delta(\alpha) = 2^k \sum_{y \in V_t} (-1)^{P(y)\gamma^T}.$$

Due to Lemma 6, $P(y)\gamma^T$ cannot be a constant. Hence,

$$\sum_{y \in V_t} (-1)^{P(y)\gamma^T} \ne \pm 2^t$$

which implies that $\Delta(\alpha) \ne 2^{t+k}$. Thus, we can conclude that f has no nonzero linear structures.

Finally, due to the property iii) of P, f must be balanced. Therefore, we have the following lemma.

Lemma 7: Let k, t be possible integers with $k < 2^t < 2^k$, $n = t + k$, and $r = 2t$. Then there exists a balanced rth-order plateaued function on V_n that does not have a nonzero linear structure.

Lemma 7 not only indicates the existence of balanced plateaued function of any order r with $0 < r < n$, but also shows that the converse of Proposition 3 is not true.

f has some other interesting properties. In particular, due to Proposition 4, the nonlinearity N_f of f satisfies $N_f = 2^{n-1} - 2^{n-\frac{r}{2}-1}$. Since f is not partially bent, Theorem 2 tells us that $(\#\Im)(\#\Re) > 2^n$. This proves that $\#\Re > 2^{n-r}$. On the other hand, from (25), we have $\#\Re \le 2^k = 2^{n-\frac{1}{2}r}$. Thus, we have $2^{n-r} < \#\Re \le 2^{n-\frac{1}{2}r}$. It is important to note 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 $\boldsymbol{B_n}$ denote the set of bent functions on V_n, $\boldsymbol{P_n}$ denote the set of partially bent functions on V_n, and $\boldsymbol{F_n}$ denote the set of plateaued functions on V_n. Then the above results imply that $\boldsymbol{B_n} \subset \boldsymbol{P_n} \subset \boldsymbol{F_n}$, where $\subset$ denotes the relationship of proper subset. We further let $\boldsymbol{G_n}$ denote the set of plateaued functions on V_n that are not bent and do *not* have nonzero linear structures. The relationships

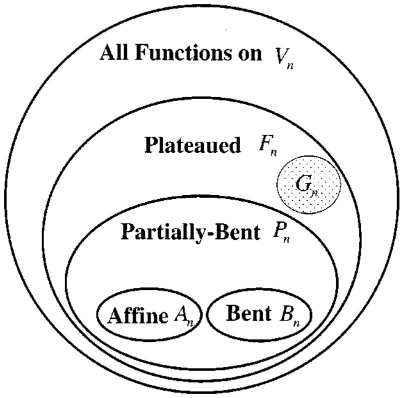

Fig. 2. Relationship among bent, partially bent, and plateaued functions.

among these classes of functions are shown in Fig. 2. Lemma 7 ensures that $\boldsymbol{G_n}$ is nonempty.

B. Constructing Balanced rth-Order Plateaued Functions Satisfying SAC

Next we consider how to improve the function in the proof of Lemma 7 so as to obtain an rth-order plateaued function on V_n satisfying the SAC, in addition to all the properties mentioned in Section VIII-A.

Note that if $r > 2$, i.e., $t > 1$, then from Section VIII-A, we have $\#\Re \leq 2^{n-\frac{1}{2}r} < 2^{n-1}$. 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 avalanche criterion. Therefore, we can choose a nonsingular $n \times n$ matrix A over GF(2) such that $g(x) = f(xA)$ satisfies the SAC (see [13]). The nonsingular linear transformation A does not alter any of the properties of f discussed in Section VIII-A. Thus, we have the following lemma.

Lemma 8: Let n be a positive number and r be any even number with $0 < r < n$. Then, there exists a balanced rth-order plateaued function on V_n that does not have a nonzero linear structure and satisfies the SAC.

C. Constructing Balanced rth-Order Plateaued Functions Satisfying SAC and Having Maximum Algebraic Degree

We can further improve the function described in Section VIII-B so as to obtain an rth-order plateaued functions on V_n that have the highest algebraic degree and satisfy all the properties mentioned in Section VIII-B.

Reference [7, Theorem 1, Ch. 13] allows us to verify that the following lemma is true.

Lemma 9: Let g be a function on V_n. Then the degree of g is equal to n if and only if $\#\{\alpha | g(\alpha) = 1, \alpha \in V_n\}$ is odd.

As $k > t$, it is easy to construct two mappings P' and P'' from V_t to V_k such that both satisfy properties i)–iii), mentioned in Section VIII-A, furthermore, $P'(\alpha) = P''(\alpha)$ for $\alpha \neq 0$, and $P'(0) \neq P''(0)$.

Note that $P'(\alpha) = P''(\alpha)$ if $\alpha \neq 0$, and $P'(0) \neq P''(0)$. Due to Lemma 9, it is easy to see that a component function of $P' \oplus P''$ has degree t, and hence a component function of P' or P'' has degree t. Without loss of generality, we assume that a component function of P' has degree t, also P' is identified with P, which we used in Sections VIII-A and VIII-B. Hence, the function f has degree $t + 1$.

We have now constructed an rth-order plateaued function with algebraic degree $\frac{r}{2} + 1$. Applying the discussions in Sections VIII-A and VIII-B, we can obtain an rth-order plateaued function on V_n having algebraic degree $\frac{r}{2} + 1$ and satisfying all the properties of the function constructed in Sections VIII-A and VIII-B. It should be noted that the function constructed in this subsection achieves the highest possible algebraic degree given in Proposition 5. Thus, the upper bound on the algebraic degree of plateaued functions, mentioned in Proposition 5, is tight. Hence, we have the following result.

Theorem 9: Let k, t be possible integers with $k < 2^t < 2^k$, $n = t+k$, and $r = 2t$. Then there exists a balanced rth-order plateaued function on V_n that does not have a nonzero linear structure, satisfies the SAC, and has the highest possible algebraic degree $\frac{r}{2} + 1$.

D. Constructing Balanced rth-Order Plateaued and Correlation Immune Functions

Let V_n, ξ be the sequence of f and ℓ_i denote the ith row of H_n, $i = 0, 1, \ldots, 2^n - 1$. Recall that in Notation 1, we defined

$$\Im_f = \{i \,|\, 0 \leq i \leq 2^n - 1, \langle \xi, \ell_i \rangle \neq 0\}.$$

Now let

$$\aleph_f = \{\alpha_i \,|\, 0 \leq i \leq 2^n - 1, i \in \Im_f\}.$$

$\aleph_f$ will be used in the following description of constructing plateaued functions that are correlation immune.

Lemma 10: Let f be a function on V_n, ξ be the sequence of f, and ℓ_i denote the ith row of H_n. Also let W be an r-dimensional linear subspace of V_n such that $\aleph_f \subseteq W$, and $s = \lfloor \frac{n}{r} \rfloor$, where $\lfloor \frac{n}{r} \rfloor$ denotes the maximum integer not larger than $\frac{n}{r}$. Then, there exists a nonsingular $n \times n$ matrix B on GF(2) such that $h(y) = f(yB)$ is an $(s-1)$th-order correlation-immune function.

Proof: For the sake of convenience, let 0_i denote the all-zero sequence of length i and 1_i denote the all-one sequence of length i. Define $\sigma_j \in V_n$, $j = 1, \ldots, r$, as follows:

$$\begin{aligned} \sigma_1 &= (1_s, 0_s, \ldots, 0_s, 0_{n-(r-1)s}) \\ \sigma_2 &= (0_s, 1_s, 0_s, \ldots, 0_s, 0_{n-(r-1)s}) \\ &\cdots \\ \sigma_{r-1} &= (0_s, \ldots, 0_s, 1_s, 0_{n-(r-1)s}) \\ \sigma_r &= (0_s, \ldots, 0_s, 1_{n-(r-1)s}). \end{aligned}$$

Since $n \geq rs$, the length of $1_{n-(r-1)s}$ is at least s. Note that the linear combinations of $\sigma_1, \ldots, \sigma_r$ form an r-dimensional linear subspace U of V_n, and each nonzero vector in U has a Hamming weight of at least s. Since both W and U are r-dimensional, there exists a nonsingular $n \times n$ matrix B on GF(2) satisfying $UB = W$, where $UB = \{\gamma B | \gamma \in U\}$. Define a function h on V_n such that $h(y) = f(yB)$. Since $\aleph_f \subseteq W$, we have $\aleph_h \subseteq U$. Let α be a nonzero vector in V_n whose Hamming weight is at most $s - 1$. Obviously, $\alpha \notin U$ and hence $\alpha \notin \aleph_h$. Therefore, for any sequence ℓ of a linear function $\varphi(x) = \langle \alpha, x \rangle$ on V_n, constrained by $1 \leq W(\alpha) \leq s - 1$, we have $\langle \eta, \ell_i \rangle = 0$, where η denotes the sequence of h. This proves that $h(y) = f(yB)$ is an $(s-1)$th-order correlation-immune function. □

By using the method described in Section VIII-A, we can construct plateaued functions that are correlation-immune, highly nonlinear, and do not have nonzero linear structures. More specifically, since $k \geq t+1$, there exists a $(t+1)$-dimensional subspace of V_k. Denote the subspace by W. In the proof of Lemma 6, we can impose on the mapping P a condition that $P(V_t) \subset W$. From (24), we have $\alpha = (\beta, \gamma) \in \aleph_f$ if and only if $P^{-1}(\gamma)$ exists, where $\beta \in V_t$ and $\gamma \in V_k$. In other words, $\aleph_f = (V_t, P(V_t))$ where

$$(V_t, P(V_t)) = \{(\beta, \gamma) | \beta \in V_t, \gamma \in P(V_t)\}.$$

Hence, $\aleph_f \subset (V_t, W)$. Note that (V_t, W) is a $(2t+1)$-dimensional subspace of V_{t+k}. From Lemma 10, we know that there exists a nonsingular $n \times n$ matrix B on $\mathrm{GF}(2)$ such that $h(y) = g(yB)$ is an $(s-1)$th-order correlation-immune function, where $s = \lfloor \frac{t+k}{2t+1} \rfloor$ or $s = \lfloor \frac{n}{r+1} \rfloor$. The function h satisfies all the other useful properties mentioned in Section VIII-A. That is, in addition to being correlation-immune, h is balanced, highly nonlinear, and does not have nonzero linear structures. Furthermore, h satisfies $2^{n-r} < \#\Re_h \le 2^{n-\frac{1}{2}r}$. Hence we have proved the following.

Theorem 10: Let t and k be positive integers with $k < 2^t < 2^k$. Let $n = k + t$ and $r = 2t$. Then, there exists an rth-order plateaued function on V_n that is also an $(s-1)$th-order correlation-immune function, where $s = \lfloor \frac{n}{r+1} \rfloor$ or $s = \lfloor \frac{t+k}{2t+1} \rfloor$, and does not have a nonzero linear structure.

IX. Conclusion

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. We have further demonstrated methods for constructing plateaued functions that have many cryptographically desirable properties including balance, SAC, high algebraic degree, as well as high nonlinearity and correlation immunity.

Building on the results obtained in this work, more recently we have introduced *complementary* plateaued functions. These functions have made it possible for us to discover new methods for constructing bent functions, as well as highly nonlinear balanced functions. Details on these new developments can be found in [14]. Finally, we note that a close relationship between plateaued functions and highly nonlinear correlation-immune functions has recently been identified in [15].

Acknowledgment

The authors wish to thank the anonymous referees whose comments have helped improve the presentation of this correspondence.

References

[1] C. Carlet, "Partially bent functions," *Des., Codes Cryptogr.*, vol. 3, pp. 135–145, 1993.

[2] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Advances in Cryptology—EUROCRYPT'89 (Lecture Notes in Computer Science)*. Berlin, Heidelberg, New York: Springer-Verlag, 1990, vol. 434, pp. 549–562.

[3] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions," in *Advances in Cryptology—EUROCRYPT'90 (Lecture Notes in Computer Science)*. Berlin, Heidelberg, New York: Springer-Verlag, 1991, vol. 437, pp. 155–165.

[4] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology—CRYPTO'85 (Lecture Notes in Computer Science)*. Berlin, Heidelberg, New York: Spinger-Verlag, 1986, vol. 219, pp. 523–534.

[5] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Advances in Cryptology—CRYPTO'91 (Lecture Notes in Computer Science)*. Berlin, Heidelberg, New York: Springer-Verlag, 1991, vol. 576, pp. 87–100.

[6] X. G. Zhen and J. L. Massey, "A spectral characterization of correlation-immune combining functions," *IEEE Trans. Inform. Theory*, vol. 34, pp. 569–571, May 1988.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1978.

[8] O. S. Rothaus, "On 'bent' functions," *J. Combin. Theory*, vol. Ser. A, no. 20, pp. 300–305, 1976.

[9] J. Wang, "The linear kernel of Boolean functions and partially bent functions," *Syst. Sci. Math. Sci.*, vol. 10, pp. 6–11, 1997.

[10] F. Erwe, *Differential And Integral Calculus*. Edinburgh, Scotland: Oliver & Boyd, 1967.

[11] X. M. Zhang, Y. Zheng, and H. Imai, "Duality of Boolean functions and its cryptographic significance," in *Advances in Cryptology—ICICS'97 (Lecture Notes in Computer Science)*. Berlin, Heidelberg, New York: Springer-Verlag, 1997, vol. 1334, pp. 159–169.

[12] R. Yarlagadda and J. E. Hershey, "Analysis and synthesis of bent sequences," *Proc. Inst. Elec. Eng. (Pt. E)*, vol. 136, pp. 112–123, 1989.

[13] J. Seberry, X. M. Zhang, and Y. Zheng, "Improving the strict avalanche characteristics of cryptographic functions," *Inform. Processing Lett.*, vol. 50, pp. 37–41, 1994.

[14] Y. Zheng and X. M. Zhang, "Relationships between bent functions and complementary plateaued functions," in *Proc. 2nd Int. Conf. Information Security and Cryptology (ICISC'99) (Lecture Notes in Computer Science)*, ser. . Berlin, Heidelberg, New York: Springer-Verlag, 1999, vol. 1787, pp. 60–75.

[15] Y. Zheng and X. M. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions," in *Pre-Proc. Selected Areas in Cryptography, 7th Annu. Int. Workshop, SAC2000*, 2000, pp. 258–269.