New Constructions for Resilient and Highly Nonlinear Boolean Functions

Khoongming Khoo [1] and Guang Gong [2]

[1] Department of Combinatorics and Optimization, [2] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada.
[1] kkhoo@math.uwaterloo.ca, [2] ggong@calliope.uwaterloo.ca

Abstract. We explore three applications of geometric sequences in constructing cryptographic Boolean functions. First, we construct 1-resilient functions of n Boolean variables with nonlinearity $2^{n-1} - 2^{(n-1)/2}$, n odd. The Hadamard transform of these functions is 3-valued, which limits the efficiency of certain stream cipher attacks. From the case for n odd, we construct highly nonlinear 1-resilient functions which disprove a conjecture of Pasalic and Johansson for n even. Our constructions do not have a potential weakness shared by resilient functions which are formed from concatenation of linear functions. Second, we give a new construction for balanced Boolean functions with high nonlinearity, exceeding $2^{n-1} - 2^{(n-1)/2}$, which is not based on the direct sum construction. Moreover, these functions have high algebraic degree and large linear span. Third, we construct balanced vectorial Boolean functions with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ and low maximum correlation. They can be used as nonlinear combiners for stream cipher systems with high throughput.

1 Introduction

Boolean functions, when used in cipher systems, are required to have good cryptographic properties. Some of the important properties are balance, high nonlinearity and resiliency. These properties ensure that the functions are resistant against correlation attacks [25] and linear cryptanalysis [14]. In the 1990's, there were many constructions given for resilient functions with maximum nonlinearity $2^{n-1} - 2^{(n-1)/2}$ (n odd) and $2^{n-1} - 2^{n/2}$ (n even) (see [3] for a summary). In 1999, Pasalic and Johansson conjectured that these achieve the maximum nonlinearity for resilient functions [18]. But in 2000, Sarkar and Maitra demonstrated that there exist resilient functions with higher noninearity for both odd and even n [21]. However, their constructions, as well as the many Maiorana-McFarland type constructions (see [3]), are concatenation of linear functions. As pointed out in [3], this may be a weakness as the function becomes linear when certain input bits are fixed. There are other constructions for highly nonlinear resilient functions not based on concatenation of linear functions [3, 7, 16, 18], which will avoid this potential weakness. It is also desirable for the function to have 3-valued Hadamard transform $0, \pm 2^k$, which limits the efficiency of the soft output joint attack [13]. For vectorial Boolean functions, it is required that they have low maximum correlation for protection against approximation by nonlinear functions of output bits [26].

In this paper, we present some new constructions for highly nonlinear and resilient Boolean functions, not based on concatenation of linear functions, from the theory of geometric sequences by Klapper, Chan and Goresky [12]. First, we consider the problem of constructing highly nonlinear resilient functions. We look at plateaued$(n-1)$ functions, i.e. functions whose Hadamard transform only takes on the values $0, \pm 2^{(n+1)/2}$, n odd. Based on a result of Zhang and Zheng [27], we deduce an efficient test for determining when a plateaued$(n-1)$ function is 1-resilient. From any one such function, we can obtain an infinite number of 1-resilient plateaued$(n-1)$ functions by applying the geometric sequence construction of [12]. These functions have nonlinearity $2^{n-1} - 2^{(n-1)/2}$ (n odd), which is considered high among resilient functions, according to [3]. Moreover, the 3-valued Hadamard transform of our functions limit the number of parity check equations that can be used for the soft output joint attack [13]. By taking the direct sum of our construction for the odd case with the highly nonlinear Patterson-Wiedemann function [19, 20], we construct 1-resilient functions with nonlinearity $> 2^{n-1} - 2^{n/2}$ for even number of input bits n.

Second, we consider the problem of constructing balanced function with nonlinearity exceeding $2^{n-1} - 2^{(n-1)/2}$ when n is odd. Previous approaches have been to take the direct sum of two highly nonlinear functions, one of which is balanced [21, 23]. Our approach is a new one based on recursive composition of a highly nonlinear balanced function with quadratic functions. By applying our construction to the highly nonlinear balanced Boolean functions of [21, 23], we obtain new balanced Boolean functions with high nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$, large linear span and high algebraic degree.

Finally, we consider the problem of constructing balanced vectorial Boolean functions to be used as nonlinear combiners in stream ciphers. Such functions will have higher throughput than 1-bit output functions. However, they need to have high nonlinearity to protect against linear approximation attacks [14, 25], and low maximum correlation to protect against approximation by nonlinear functions of output bits [26]. Our construction yields balanced vectorial Boolean functions with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ and low maximum correlation.

The paper is organised as follows. In Section 2, we give some definitions and preliminaries. In Section 2.3, we derive a useful result on cascaded functions, which is basic to all the construction methods in this paper. In Section 3, we construct highly nonlinear resilient Boolean functions. In Section 4, we construct highly nonlinear balanced Boolean function. In Section 5, we construct nonlinear balanced vectorial Boolean functions with low maximum correlation.

2 Definitions and Preliminaries

2.1 Polynomial and Boolean Functions

Let $GF(2^n)$ be the finite field with 2^n elements and $GF(2^n)^*$ be $GF(2^n) - \{0\}$. Let $q = 2^n$, the trace function from $GF(q^m)$ to the subfield $GF(q)$ is $Tr_q^{q^m}(x) := \sum_{i=0}^{m-1} x^{q^i}$. When there is no confusion, we denote $Tr_2^{2^n}(x)$ by $Tr(x)$. The *Hadamard transform* of a function $f : GF(2^n) \to GF(2)$ is defined to be

$$\hat{f}(\lambda) := \sum_{x \in GF(2^n)} (-1)^{Tr(\lambda x) + f(x)}, \lambda \in GF(2^n).$$

A Boolean function is a function $g : \mathbf{Z}_2^n \to \mathbf{Z}_2$. There is a natural correspondence between Boolean functions g and polynomial functions $f : GF(2^n) \to GF(2)$. Let $\{\alpha_0, \dots, \alpha_{n-1}\}$ be a basis for $GF(2^n)$, this correspondence is given by

$$g(x_0, \dots, x_{n-1}) := f(\alpha_0 x_0 + \dots + \alpha_{n-1} x_{n-1}).$$

For example, this correspondence is used by Patterson and Wiedemann to construct highly nonlinear functions for $n = 15$ [19, 20]. We will also use this correspondence for constructing cryptographically useful Boolean functions.

Let n be odd. As defined in [27], a Boolean function $f : \mathbf{Z}_2^n \to \mathbf{Z}_2$ is a *plateaued function of order r* (denoted *plateaued*(r)) if $\hat{f}(w)^2 = 0, 2^{2n-r}$ for all $w \in \mathbf{Z}_2^n$. In this paper, we will be studying plateaued$(n-1)$ functions, i.e. those functions f satisfying $\hat{f}(w) = 0, \pm 2^{(n+1)/2}$ for all $w \in \mathbf{Z}_2^n$.

The *nonlinearity* of a Boolean function f is defined by

$$N_f := \min\{d(f, a),\ a \text{ affine function}\}$$

where $d(f, a)$ is the number of x for which $f(x) \neq a(x)$. We want the nonlinearity of a function to be as high as possible. The nonlinearity is related to the Hadamard transform by

$$N_f = 2^{n-1} - 1/2 \max_{\lambda} |\hat{f}(\lambda)|. \quad (1)$$

A Boolean function $f : \mathbf{Z}_2^n \to \mathbf{Z}_2$ satisfies the correlation immunity of order k if $\hat{f}(w) = 0$ for all $1 \leq wt(w) \leq k$. If f is also balanced, then we say f is k-resilient.

The *additive autocorrelation* of f at a is defined as:

$$\Delta_f(a) := \sum_x (-1)^{f(x)+f(x+a)}.$$

We say $f : \mathbf{Z}_2^n \to \mathbf{Z}_2$ has a linear structure at a if $\Delta_f(a) = \pm 2^n$. f satisfies the propagation criteria at a if $\Delta_f(a) = 0$. Many useful properties of a Boolean function can be deduced by analysing the relationship between $\Delta_f(a)$ and $\hat{f}(\lambda)$. Some examples include [1, 10, 16, 21, 23, 24, 28, 27].

Consider the polynomial function $f(x) = \sum_i \beta_i x^{s_i}, \beta_i \in GF(2^n)$. The *algebraic degree* $deg(f)$ of the corresponding Boolean function is given by the maximum weight of the exponents $\max_i wt(s_i)$ (see [15]). We want it to be high for algebraic complexity.

The *linear span* of a polynomial function is the number of monomials x^s in its polynomial expression. We want it to be high to defend against interpolation attack [8].

2.2 Vectorial Boolean Functions

There is a natural correspondence between Boolean Sboxes $F : \mathbf{Z}_2^n \to \mathbf{Z}_2^m$ and polynomial functions from $GF(2^n)$ to $GF(2^m)$. Let $\{\alpha_0, \ldots, \alpha_{n-1}\}$ be a basis for $GF(2^n)$ and $\{\beta_0, \ldots, \beta_{m-1}\}$ be a basis for $GF(2^m)$. The correspondence is given by

$$(x_0, \ldots, x_{n-1}) \leftrightarrow \alpha_0 x_0 + \ldots + \alpha_{n-1} x_{n-1}$$
$$(y_0, \ldots, y_{m-1}) \leftrightarrow \beta_0 y_0 + \ldots + \beta_{m-1} y_{m-1}$$

The *nonlinearity* N_F of an S-box is $N_F = min_{b \neq 0} N_{b \cdot F}$ where $b \cdot F$ consists of all linear combination of output bits. When n is odd and $m \geq 2$, $N_F = 2^{n-1} - 2^{(n-1)/2}$ is considered high.

The *maximum correlation* [26] of F at w is

$$C_F(w) = \max_g [Prob(g(F(x)) = w \cdot x) - Prob(g(F(x)) \neq w \cdot x)]. \tag{2}$$

where the maximum is taken over all $g : \mathbf{Z}_2^m \to \mathbf{Z}_2$. We do not consider $w = 0$ because $C_F(0) = 1$ for all F (by letting $g(z) = 0$), instead we require that F be balanced.

Proposition 1. *(Zhang-Chan [26, Theorem 4]) Let $F : \mathbf{Z}_2^n \to \mathbf{Z}_2^m$, the maximum correlation of F satisfies*

$$C_F(w) \leq 2^{m/2-n} max_v |\sum_x (-1)^{v \cdot F(x) + w \cdot x}|$$

Proposition 1 imples that a high nonlinearity will guarantee low maximum correlation, for protection against approximation by nonlinear functions of output bits.

2.3 Hadamard Transform of Cascaded Functions

We derive a useful result on cascaded function that will be applied to construct cryptographic Boolean functions in Section 3, 4 and 5. Let $I(f) = \sum_{x \in GF(2^n)} (-1)^{f(x)}$ be the imbalance of f and the correlation between polynomial functions f and g at $\lambda \in GF(2^n)$ be $C_{f,g}(\lambda) = \sum_{x \in GF(2^n)} (-1)^{f(\lambda x) + g(x)}$.

Lemma 1. *(Klapper, Chan, Goresky [12, Theorem 3]) Let $q = 2^n$, consider $g, h : GF(q) \to GF(2)$. The correlation between the pair of functions*

$$g(Tr_q^{q^m}(x)) \text{ and } h(Tr_q^{q^m}(x^{q^i+1}))$$

at $\Lambda \in GF(q^m)^*$ takes on the values:

1. $q^{m-2}I(g)I(h)$
2. $(q^{m-2}-q^{m-(m-d)/2-2})I(g)I(h) \pm q^{m-(m-d)/2-1}C_{g(x),h(x^2)}(\lambda)$, $\lambda \in GF(q)^*$.

where $d = \gcd(i, m)$.

From Lemma 1, we derive the following result that is basic to all our construction methods.

Theorem 1. *Let* $q = 2^n$, n, n_j *be odd for* $j = 1, \dots, l$ *and let* $f : GF(q) \to GF(2)$. *Define recursively the functions*

$$\begin{aligned} f_0(x) &= f(x) \\ f_j(x) &= f_{j-1}(Tr^{q_j}_{q_{j-1}}(x^{k_j})), j = 1, \dots, l \end{aligned}$$

where $q_0 = q$, $q_j = q_{j-1}^{n_j}$, $k_j = q_{j-1}^{r_j}+1$ *and* $\gcd(r_j, n_j) = 1$. *Then* $\widehat{f_l}(\Lambda)$, $\Lambda \in GF(q_l)^*$ *takes on the values* $0, \pm q^{\frac{n_1 n_2 \cdots n_l - 1}{2}} \hat{f}(\lambda)$, $\lambda \in GF(q)^*$.

Proof. We proceed by induction on j. To prove the base case $j = 1$, we apply Lemma 1 by letting $g(x) = Tr^q_2(x)$ and $h(x) = f(x)$ to find the correlation between the functions

$$g(Tr^{q_1}_{q_0}(x)) = Tr^{q_1}_2(x) \text{ and } h(Tr^{q_1}_{q_0}(x^{k_1})) = f_1(x). \tag{3}$$

Note that $I(g) = I(Tr^q_2) = 0$, $C_{g(x),h(x^2)}(\lambda) = \hat{f}(\lambda^2)$ by the properties of the trace function; and $\widehat{f_1}(\Lambda)$, $\Lambda \in GF(q_1)^*$ is the correlation between the functions in equation (3). By Lemma 1, it takes on the values:

$$0, \pm q^{n_1-(n_1-1)/2-1}\hat{f}(\lambda^2) = \pm q^{(n_1-1)/2}\hat{f}(\lambda^2), \lambda \in GF(q)^*.$$

We can substitute $\hat{f}(\lambda^2)$ with $\hat{f}(\lambda)$ since $\lambda \mapsto \lambda^2$ is a permutation on $GF(q)^*$. Therefore, the base case is true.

Suppose that case $j-1$ is true, i.e. $\widehat{f_{j-1}}(\Lambda)$, $\Lambda \in GF(q_{j-1})^*$ takes on the values $0, \pm q^{(n_1 \cdots n_{j-1}-1)/2}\hat{f}(\lambda)$, $\lambda \in GF(q)^*$. To prove the jth case, we apply Lemma 1 by letting $g(x) = Tr^{q_{j-1}}_2(x)$ and $h(x) = f_{j-1}(x)$ to find the correlation between the functions

$$g(Tr^{q_j}_{q_{j-1}}(x)) = Tr^{q_j}_2(x) \text{ and } h(Tr^{q_j}_{q_{j-1}}(x^{k_j})) = f_j(x). \tag{4}$$

Similar to the proof of the base case, we deduce from Lemma 1 that $\widehat{f_j}(\Lambda)$, $\Lambda \in GF(q_j)^*$ takes on the values:

$$0, \pm q_{j-1}^{n_j-(n_j-1)/2-1} q^{(n_1 \cdots n_{j-1}-1)/2}\hat{f}(\lambda) = \pm q^{(n_1 \cdots n_j - 1)/2}\hat{f}(\lambda), \lambda \in GF(q)^*.$$

Therefore, the statement is true for all $j = 1, \dots, l$ by induction. □

Remark 1. In [12], Klapper, Chan and Goresky proved that if $f(x) = Tr(x^{2^i+1})$ where $\gcd(i, n) = 1$, then $f_l(x)$ in Theorem 1 is plateaued$(N-1)$, $N = nn_1 \cdots n_l$. They called their construction a cascaded GMW sequence. Here we gneralise it so that it applies to any function $f(x)$.

Note that Theorem 1 only holds for $\widehat{f_l}(\Lambda)$ where $\Lambda \neq 0$. The imbalance of $f_l(x)$, which is $\widehat{f_l}(0)$, is given by $q^{n_1 n_2 \cdots n_l - 1}\hat{f}(0)$.

3 New Construction for Resilient Functions

In this section, we explore constructions for resilient plateaued$(n-1)$ functions. Such functions have nonlinearity $2^{n-1} - 2^{(n-1)/2}$ which is considered high among resilient functions according to Carlet [3]. Sarkar and Maitra constructed 1-resilient functions with nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ for odd $n \geq 41$ [21, Theorem 6]. However, their construction [21, Corollary 2], as well as the many Maiorana-McFarland type constructions in the existing literature (see [3]), correspond to concatenation of linear functions. This may be a weakness as the functions become linear when certain input bits are fixed [3]. Our construction will avoid this weakness. Moreover, our functions are 3-valued which makes the soft output joint attack less efficient [13, Corollary 1].

First, we derive an efficient test for 1-resilient plateaued$(n-1)$ functions based on a result of Zheng and Zhang [27]. Then, we prove that by applying the geometric sequence construction of Klapper, Chan and Goresky [12] on certain resilient plateaued$(n-1)$ function, we can obtain an infinite number of resilient highly nonlinear functions from it.

Lemma 2. *(Zheng and Zhang [27, Theorem 2]) Let n be odd and $f: GF(2^n) \to GF(2)$ be a balanced plateaued$(n-1)$ function. If f does not have a non-zero linear structure, then the Boolean form of f is 1-resilient for some basis of $GF(2^n)$, which can be found by the method of [7].*

Remark 2. We stated Lemma 2 in a modified form (from the original in [27]) so that it applies to polynomial functions. Lemma 2 has also been proven in a more general form in [1, Theorem 7]. From the proof of Lemma 2, we see that the set $\{\lambda | \hat{f}(\lambda) = 0\}$ contains n linearly independent vectors. Based on these n vectors, Gong and Youssef gave an algorithm to find a basis of $GF(2^n)$ such that the Boolean form of f is 1-resilient in [7].

The following equation is well-known, e.g. see [1, 27]:

$$1/2^n \sum_{\lambda} \hat{f}(\lambda)^4 = \sum_{a} \Delta_f(a)^2 \tag{5}$$

It can be used to derive Corollary 1 which is a more applicable form of Lemma 2.

Corollary 1. *Let n be odd and $f: GF(2^n) \to GF(2)$ be a balanced plateaued$(n-1)$ function. If there exists $a \in GF(2^n)$ such that $\Delta_f(a) \neq 0$ or $\pm 2^n$, then $N_f = 2^{n-1} - 2^{(n-1)/2}$ and the Boolean form of f is 1-resilient for some basis of $GF(2^n)$.*

Remark 3. To test if a plateaued$(n-1)$ function f is resilient by Lemma 2, we have to check $\Delta_f(a) \neq \pm 2^n$ for all a. By using Corollary 1, we have a more efficient way to test if f is resilient since we have to check very few $\Delta_f(a)$ as we shall see later on.

Remark 4. Let f be a balanced plateaued$(n-1)$ function formed from

$$h(x_1, \ldots, x_n) = g(x_1, \ldots, x_{n-1}) + x_n, \;\; f(x) = h(xA).$$

where g is bent and A is an invertible $n \times n$ matrix. Then $\beta = (00\ldots01)A^{-1}$ satisfies $\Delta_f(\beta) = -2^n$. Therefore, Corollary 1 fails for these functions, which includes all quadratic plateaued$(n-1)$ functions.

We demonstrate some applications with the following two examples. We introduce the cyclotomic coset leaders modulo $2^n - 1$ which are the smallest elements of the sets $\{2^i \times s \mod 2^n - 1, i = 0 \ldots n-1\}$. Because $Tr(x^{2i}) = Tr(x^i)$, we just need to look at the cyclotomic coset leaders in the exponents of $Tr(x^i)$.

Example 1. Let $n = 5$. We exhaustively search for balanced plateaued$(n-1)$ functions $f: GF(2^5) \to GF(2)$ of the form $f(x) = \sum_{i \in I} Tr(x^i)$, where I are the cyclotomic coset leaders $\{1, 3, 5, 7, 11, 15\}$. We obtain six non-quadratic plateaued$(n-1)$ functions (all cubic):

$$Tr(x^7), Tr(x^{11}), Tr(x + x^3 + x^{11}), Tr(x + x^5 + x^7), Tr(x + x^7 + x^{11}), Tr(x + x^3 + x^5 + x^7 + x^{11})$$

Since $\Delta_f(1) = 8$ which is $\neq 0, \pm 2^5$ for all these functions, their Boolean form are all 1-resilient for some basis representation.

Example 2. Let $n = 11$. We exhaustively search for balanced plateaued$(n-1)$ functions $f : GF(2^{11}) \to GF(2)$ of the form $f(x) = \sum_{i \in I} Tr(x^i)$, I are the cyclotomic coset leaders modulo 2047, from a restricted search space of size 119446698. We obtain 426 non-quadratic plateaued$(n-1)$ functions.

By applying Corollary 1 on these functions, we verified that all these functions are 1-resilient in some basis representation. We just list the functions which achieves the maximal algebraic degree $(n+1)/2 = 6$ (bound from [27]) in our list:

$$Tr(x^{71} + x^{309} + x^{359}), Tr(x + x^3 + x^{43} + x^{171} + x^{683}), Tr(x + x^{13} + x^{411} + x^{413} + x^{423})$$
$$Tr(x + x^{25} + x^{71} + x^{309} + x^{359}), Tr(x + x^{57} + x^{231} + x^{343} + x^{683}), Tr(x + x^{63} + x^{95} + x^{189} + x^{315})$$
$$Tr(x + x^{143} + x^{151} + x^{365} + x^{429}).$$

These seven functions satisfy $\Delta_f(1) \neq 0, \pm 2^{11}$. Therefore their Boolean representation are 1-resilient in some basis.

Remark 5. In both examples, all the balanced non-quadratic plateaued$(n-1)$ functions we found by exhaustive search are 1-resilient for some basis representation. This seems to suggest that if we randomly choose a balanced non-quadratic plateaued$(n-1)$ function, there is a high chance it is 1-resilient. Moreover, almost all the functions in our test satisfy $\Delta_f(1) \neq 0, \pm 2^n$. So we can confirm $\Delta_f(a) \neq 0, \pm 2^n$ at the beginning (if we are testing $a = \alpha^i$ from $i = 0, 1, \ldots$ onwards where α generates $GF(2^n)$). This seems to suggest Corollary 1 gives a fast test.

Next, we derive a new construction for 1-resilient plateaued$(n-1)$ functions. Precisely, we show that by composing a 1-resilient plateaued$(n-1)$ function from Corollary 1 with a quadratic function, we can obtain infinitely more functions of the same kind.

Theorem 2. *Let n be odd, $q = 2^n$ and $f : GF(q) \to GF(2)$ be a balanced plateaued$(n-1)$ function. If there exists $a \in GF(q)$ s.t. $\Delta_f(a) \neq 0, \pm q$, then $g : GF(2^N) \to GF(2)$, $N = mn$, defined by*

$$g(x) = f(aTr_q^{q^m}(x^{q^i+1})), \;\; m \text{ odd}, \; \gcd(i, m) = 1$$

is 1-resilient for some basis of $GF(2^N)$ and plateaued$(N-1)$ which implies $N_g = 2^{N-1} - 2^{(N-1)/2}$. Moreover, $deg(g) = 2deg(f)$.

Proof. First, we prove that g is plateaued$(N-1)$. g is balanced because it is a composition of balanced functions. Therefore $\hat{g}(0) = 0$. For $\hat{g}(\lambda)$, $\lambda \neq 0$, we apply Theorem 1 with $l = 1$ to see that $\hat{g}(\lambda)$ takes on the values:

$$0, \pm q^{(m-1)/2} 2^{(n+1)/2} = \pm 2^{(mn+1)/2}.$$

Thus g is plateaued$(N-1)$. The nonlinearity of g is a consequence of equation (1).

Second, we prove that g is 1-resilient. Let $y = Tr_q^{q^m}(x^{q^i+1})$. Then

$$\begin{aligned} g(x+1) &= f(aTr_q^{q^m}((x+1)^{q^i+1})) \\ &= f(a(Tr_q^{q^m}(x^{q^i+1}) + Tr_q^{q^m}(x^{q^i}) + Tr_q^{q^m}(x) + 1)) \\ &= f(a(y+1)), \text{ because } Tr_q^{q^m}(x^{q^i}) = Tr_q^{q^m}(x). \end{aligned}$$

From the above identity and the fact that for each $y \in GF(q)$, there are q^{m-1} elements $x \in GF(q^m)$ such that $y = Tr_q^{q^m}(x^{q^i+1})$, we deduce

$$\begin{aligned} \Delta_g(1) &= \sum_{x \in GF(q^m)} (-1)^{g(x)+g(x+1)} \\ &= q^{m-1} \sum_{y \in GF(q)} (-1)^{f(ay)+f(ay+a)} \\ &= q^{m-1} \Delta_f(a) \neq 0, \pm q^m, \text{ because } \Delta_f(a) \neq 0, \pm q. \end{aligned}$$

By Corollary 1, the Boolean form of g is 1-resilient in some basis of $GF(2^{mn})$.

Third, the algebraic degree is $2deg(f)$ from Theorem 3 part 3. □

Useful properties of our construction:

1. New construction for resilient function with nonlinearity $2^{N-1} - 2^{(N-1)/2}$, N odd, for protection against linear and correlation attacks [25, 14]. Moreover, it is not based on concatenation of linear functions. Therefore it avoids a potential weakness of being linear when certain input bits are fixed.
2. Our function has 3-valued Hadamard transform which prevents the use of all even parity check equations in the soft output joint attack [13, Corollary 1]. This will limit the efficiency of that attack.

Example 3. Let $f : GF(2^5) \to GF(2)$ be any of the plateaued$(n-1)$ functions in Example 1. Suppose we take $f(x) = Tr_2^{2^5}(x + x^5 + x^7)$, $deg(f) = 3$. We apply Theorem 2 with $n = 5, m = 3$ and $i = 1$. Since $\Delta_f(1) \neq 0, \pm 2^5$, we let $a = 1$ and $g(x) = f(Tr_{2^5}^{2^{15}}(x^{33}))$. Then the Boolean form of $g(x)$ has 15 input bits, algebraic degree $= 6$, is 1-resilient for some basis of $GF(2^{15})$ and has nonlinearity $2^{14} - 2^7 = 16256$. By choosing other values of m, we have an infinite number of 1-resilient functions with similar nonlinearity.

Pasalic and Johansson conjectured that the highest nonlinearity for 1-resilient functions with even number of input bits n is $2^{n-1} - 2^{n/2}$. We will disprove this conjecture by constructing functions with higher nonlinearity. This has also been done by Sarkar and Maitra in [21, 22]. We will make use of the Patterson Wiedemann functions with 15 input bits and nonlinearity 16276 from [19, 20]. The following theorem based on the direct sum construction is easy to prove, e.g. see [22].

Proposition 2. *Let $f : \boldsymbol{Z}_2^n \to \boldsymbol{Z}_2$, n odd, be a k-resilient function with nonlinearity $2^{n-1} - 2^{(n-1)/2}$ and $PW : \boldsymbol{Z}_2^{15} \to \boldsymbol{Z}_2$ be the 15-bit Patterson Wiedemann function from [19, 20]. Then*

$$g(x, y) := f(x) + PW(y), x \in \boldsymbol{Z}_2^n, y \in \boldsymbol{Z}_2^{15}$$

has $m = n + 15$ (even) number of input bits, is k-resilient and has nonlinearity

$$N_g = 2^{m-1} - 27/32 \times 2^{m/2} > 2^{m-1} - 2^{m/2}.$$

Moreover, $deg(g) = \max(deg(f), deg(PW))$.

Useful properties of our construction:

1. k-resilient function with high nonlinearity $> 2^{m-1} - 2^{m/2}$ (which disproves the conjecture of [18]) for protection against linear and correlation attacks [25, 14]. Note that Sarkar and Maitra also disproved the conjecture of [18] by concatenation involving linear functions [21, Theorems 7,8 and 9]
2. If we use a 1-resilient function $f(x)$ by exhaustive search in Examples 1,2 or Theorem 2, then both $f(x)$ and the Patterson-Wiedemann function $PW(y)$ are constructed from finite fields which are not concatenation of linear functions. Therefore their direct sum $g(x, y)$ is not one too.

Example 4. We apply Proposition 2 by considering the 1-resilient function $f(x) = Tr_2^{2^5}(x + x^5 + x^7)$, $deg(f) = 3$, from Example 1 and letting $PW(y)$ be the 15-bit Patterson-Wiedemann function with algebraic degree 9 from [19, 20]. Then $g(x, y) = f(x) + PW(y)$, the direct sum of the Boolean form of f and PW, has 20 input bits, is 1-resilient, has nonlinearity $2^{19} - 2^{10} + 160$ and algebraic degree 9.

4 Highly Nonlinear Balanced Boolean Functions

In this section, we construct new classes of balanced Boolean functions with high nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$, n odd, high algebraic degree and large linear span. This is achieved by applying Theorem 1 on the highly nonlinear balanced functions of Sarkar and Maitra [21] and Seberry, Zhang and Zheng [23].

Theorem 3. *Let $q = 2^n$ and n, n_j be odd for $j = 1, \ldots, l$. Let $f : GF(q) \to GF(2)$ be a balanced function with nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ (such as the functions from [21, 23]). Define recursively the functions*

$$f_0(x) = f(x)$$
$$f_j(x) = f_{j-1}(Tr_{q_{j-1}}^{q_j}(x^{k_j})), j = 1, \ldots, l.$$

where $q_0 = q$, $q_j = q_{j-1}^{n_j}$, $k_j = q_{j-1}^{r_j} + 1$ and $\gcd(r_j, n_j) = 1$. f_l corresponds to a Boolean function with $N = nn_1 \cdots n_l$ input bits and

1. *f_l is balanced having high nonlinearity*
$$2^{N-1} - 2^{\frac{N-n}{2}-1} \max_\lambda |\hat{f}(\lambda)| > 2^{N-1} - 2^{(N-1)/2}.$$
2. *If the polynomial expression for f is $\sum_i \beta_i x^{t_i}$, then the linear span of f_l satisfies*
$$LS(f_l) = \sum_i (n_1 n_2^2 \cdots n_l^{2^{l-1}})^{wt(t_i)} \tag{6}$$
Thus $LS(f_l) \geq (n_1 n_2^2 \cdots n_l^{2^{l-1}})^{deg(f)}$.
3. *The algebraic degree of f_l is $2^l deg(f)$.*

Proof. 1. f is balanced implies that f_l is balanced since it is a composition of balanced functions. Therefore, $\widehat{f_l}(0) = 0$. We apply Theorem 1 to see that $\widehat{f_l}(\Lambda)$, $\Lambda \in GF(2^N)^*$ takes on the values:
$$0, \pm(2^n)^{(n_1 \cdots n_l - 1)/2} \hat{f}(\lambda) = 2^{(N-n)/2} \hat{f}(\lambda), \lambda \in GF(q)^*$$
By equation (1),
$$N_{f_l} = 2^{N-1} - 2^{\frac{N-n}{2}-1} \max_\lambda |\hat{f}(\lambda)|.$$
The function f has nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ implies $\max_\lambda |\hat{f}(\lambda)| < 2^{(n+1)/2}$. This implies
$$N_{f_l} > 2^{N-1} - 2^{\frac{N-n}{2}-1} 2^{\frac{n+1}{2}} = 2^{N-1} - 2^{(N-1)/2}.$$

2. Note that $f_l(x)$ can be written as
$$f_l(x) = \sum_i \beta_i g(x)^{t_i}, \beta_i \neq 0, \beta_i \in GF(2^n)$$
where $g(x) = Tr_{q_0}^{q_1}(Tr_{q_1}^{q_2} \ldots Tr_{q_{l-1}}^{q_l}(x^{k_l}) \ldots)^{k_2})^{k_1}$ is a cascaded GMW function from $GF(2^N)$ to $GF(2^n)$ with known linear span $n_1 n_2^2 \cdots n_l^{2^{l-1}}$ [12]. Applying Lemma 2-(i) in [6] to each term $g(x)^{t_i}$, we deduce that for each $i \neq j$, the monomial terms in $g(x)^{t_i}$ and $g(x)^{t_j}$ are distinct. According to Theorem 1 and Lemma 2-(ii) in [6], the number of distinct monomials of $g(x)^{t_i}$ is $(n_1 n_2^2 \cdots n_l^{2^{l-1}})^{wt(t_i)}$. Thus, equation (6) is established.
The inequality $LS(f_l) \geq (n_1 n_2^2 \cdots n_l^{2^{l-1}})^{deg(f)}$ follows from equation (6) because there is at least a monomial in the expression of f that has exponent $deg(f)$.

3. According to the proof of Lemma 2 in [6], we can deduce that when we recursively expand each trace term of f_l using the relation

$$(\sum_i x^{s_i})^{\sum_j 2^{a_j}} = \prod_j \sum_i x^{2^{a_j} s_i},$$

there is no cancellation among the resulting sum of monomials. Therefore the maximal exponent is $2^l max_i wt(t_i) = 2^l deg(f)$ which is the algebraic degree of f_l.

□

The following proposition will ensure our function have high algebraic degree.

Proposition 3. *(Sarkar and Maitra [21, Proposition 2 and 3]) Let $f : \mathbf{Z}_2^N \to \mathbf{Z}_2$ be a balanced Boolean function. When we change up to two bits in the Boolean truth table of f such that the top half and bottom half truth tables have odd weight. The new function f will be balanced, $deg(f) = N - 1$ and the nonlinearity will decrease by at most 2.*

Useful properties of our Construction:

1. Theorem 3 gives a new construction for balanced function f_l with high nonlinearity $> 2^{N-1} - 2^{(N-1)/2}$ not based on taking direct sum.
2. The function can achieve high algebraic degree and large linear span.

For the sake of completeness, we will outline some known constructions for balanced highly nonlinear functions used in Theorem 3.

1. *Seberry, Zhang and Zheng* [23, Theorem 2]: They constructed a balanced function $g : \mathbf{Z}_2^{2k} \to \mathbf{Z}_2$, $k \geq 7$, with high nonlinearity by modifying a bent function. Then they take the direct sum of $g(x)$ with the 15-bit Patterson Wiedemann function $PW(y)$ having nonlinearity $16276 > 2^{14} - 2^7$ [19, 20]. The resulting balanced function

$$h(x, y) = g(x) + PW(y), \;\; x \in \mathbf{Z}_2^{2k}, y \in \mathbf{Z}_2^{15}.$$

has nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ where $n = 2k + 15$. Their construction works for odd $n \geq 29$. (Later, Dobbertin gave a more general method to modify bent functions into balanced function g in [4]).

2. *Sarkar and Maitra* [21, Theorem 13]: They modified the Patterson Wiedemann function PW_r of [19, 20] for $r = 15, 17, 19, 21$ number of input bits to obtain balanced functions f_r with nonlinearity $2^{14} - 2^7 + 6$, $2^{16} - 2^8 + 18$, $2^{18} - 2^9 + 46$ $2^{20} - 2^{10} + 104$ respectively. Then they take the direct sum of f_r with a bent function $g : \mathbf{Z}_2^{2k} \to \mathbf{Z}_2$. The resulting balanced function

$$h(x, y) = g(x) + f_r(y), \;\; x \in \mathbf{Z}_2^{2k}, y \in \mathbf{Z}_2^{r}.$$

has nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$ where $n = 2k + r$. Their construction works for odd $n \geq 15$.

Example 5. We apply Theorem 3 by letting $f(x)$ be the 15-bit balanced function with nonlinearity $2^{14} - 2^7 + 6 = 16262$ from [21], $l = 1$, $n_1 = 3$ and $r_1 = 1$. Then

$$f_1(x) = f(Tr_{2^{15}}^{2^{45}}(x^{2^{15}+1}))$$

is balanced, has 45 input bits and nonlinearity $2^{44} - 2^{(45-15)/2-1} \max_\lambda |\hat{f}(\lambda)| = 2^{44} - 2^{22} + 196608$ where $\max_\lambda |\hat{f}(\lambda)| = 244$. As in Proposition 3, we can change at most 2 bits in the Boolean truth table of f_1 to get a balanced function with nonlinearity $\geq 2^{44} - 2^{22} + 196606$ and algebraic degree 44.

To ensure a large linear span, we could also apply Proposition 3 to the 15-bit function f to get a balanced function with nonlinearity $\geq 2^{14} - 2^7 + 4$ and algebraic degree 14. Then f_1 as defined above will have nonlinearity $\geq 2^{44} - 2^{22} + 131072$, algebraic degree $2 \times 14 = 28$ and linear span $\geq n_1^{deg(f)} = 3^{14} = 4782969$ by Theorem 3. The large linear span of f_1 provides protection against interpolation attack [8].

5 Highly Nonlinear Balanced Vectorial Functions with Low Maximum Correlation

We construct a new class of balanced vectorial Boolean functions with n (odd) input bits that have nonlinearity $2^{n-1} - 2^{(n-1)/2}$ through geometric sequences. They have low maximum correlation bounds by Proposition 1.

$$C_F(w) \leq 2^{m/2-n} 2^{(n+1)/2} = 2^{(m-n+1)/2} \text{ for } w \neq 0. \tag{7}$$

In symmetric cipher applications, this ensures that linear approximation and approximation by nonlinear functions of output bits are difficult. We also point out that the maximum correlation can be further reduced by a factor of $\sqrt{2}$.

In Table 1, we list known balanced plateaued$(m-1)$ functions of the form $Tr(x^k)$, $x \in GF(2^m)$, needed for our construction. Note that when $Tr(x^k)$ is plateaued$(m-1)$, the function $Tr(x^{k^{-1}})$ is also plateaued$(m-1)$. It was conjectured in [2] that Table 1 constains all plateaued$(m-1)$ functions of the form $Tr(x^k)$.

Table 1. r such that $f(x) = Tr(x^k)$ and $Tr(x^{k^{-1}})$ are balanced, plateaued$(m-1)$ for $x \in GF(2^m)$, m odd.

k	condition	reference
$2^r + 1$(Gold)	$\gcd(r, m) = 1$	[5]
$2^{2r} - 2^r + 1$(Kasami)	$\gcd(r, m) = 1$	[11]
$2^{(m-1)/2} + 3$(Niho)	none	Conjecture [17]
$2^{2r} + 2^r - 1$(Welch)	$4r + 1 \equiv 0 \pmod{m}$	[2]

Theorem 4. *Let $q = 2^m$ and m, n_j be odd for $j = 1 \cdots l$. Let $Tr_2^q(x^k), x \in GF(q)$, be balanced and plateaued$(m-1)$ (see Table 1). Define inductively the functions*

$$F_0(x) = x^k$$
$$F_j(x) = F_{j-1}(Tr_{q_{j-1}}^{q_j}(x^{k_j})), j = 1 \cdots l$$

where $q_0 = q$, $q_j = q_{j-1}^{n_j}$, $k_j = q_{j-1}^{r_j} + 1$ and $\gcd(r_j, n_j) = 1$. Let $N = mn_1 n_2 \cdots n_l$ and $F(x) = F_l(x)$ where $F : GF(2^N) \to GF(2^m)$. Then

1. *F is balanced.*
2. *The nonlinearity is $N_F = 2^{N-1} - 2^{(N-1)/2}$.*
3. *The maximum correlation satisfies $C_F(w) < 2^{(m-N+1)/2}$ for all $w \neq 0$.*
4. *The linear span is $(n_1 n_2^2 \cdots n_l^{2^{l-1}})^{wt(r)}$ and the algebraic degree is $deg(F) = 2^l wt(r)$.*

Proof. 1. F is balanced because it is a composition of balanced functions.

2. Let $f(x) = Tr_2^q(F(x))$. Then f is plateaued$(N-1)$ by Theorem 1 and the fact that it is balanced. We will prove the nonlinearity of F by showing that all linear combination of output bits given by $Tr_2^q(bF(x))$, $b \in GF(q)$ is plateaued$(N-1)$. To achieve this, we need the following identity which can be proven by induction on j using the properties of trace function.

$$bF_j(x) = F_j(b^{(kk_1 \cdots k_j)^{-1}} x), \text{ for all } b \in GF(q),\ j = 1, \ldots, l.$$

From this, we deduce that $bF(x) = F(b'x)$ where $b' = b^{(kk_1\cdots k_l)^{-1}}$. And the Hadamard transform of $Tr_2^q(bF(x))$ is given by:

$$\begin{aligned}\sum_x (-1)^{Tr(bF(x))+Tr(\lambda x)} &= \sum_x (-1)^{Tr(F(b'x))+Tr(\lambda x)}, \text{ where } b' = b^{(kk_1\cdots k_l)^{-1}} \\ &= \sum_y (-1)^{Tr(F(y))+Tr((b')^{-1}\lambda y)}, \text{ where } y = b'x \\ &= \hat{f}((b')^{-1}\lambda) = 0, \pm 2^{(N+1)/2},\end{aligned}$$

Thus all linear combination of output bits correspond to Boolean functions with nonlinearity $2^{N-1} - 2^{(N-1)/2}$ by equation (1). Therefore F has the same nonlinearity.

3. The maximum correlation bound is a direct application of Proposition 1, since $\widehat{v \cdot F}(w)$ takes the values $0, \pm 2^{(N+1)/2}$. The inequality is strict because we can deduce from equation (2) that

$$2^N C_F(w) = \max_g \sum_x (-1)^{g(F(x))+w\cdot x}.$$

This should be an integer while $2^N \times$ upper bound $= 2^{(m+N+1)/2}$ is not.
4. The algebraic degree and linear span can be proven in a similar way to Theorem 3 parts 2 and 3.

$\square$

Remark 6. The upper bound for maximum correlation in Theorem 4 holds for all Sboxes with nonlinearity $2^{n-1} - 2^{(n-1)/2}$. For the case $l = 1$, we can prove $C_F(w) \leq 2^{(m-N)/2}$, i.e. the upper bound for maximum correlation can be reduced by a factor of $\sqrt{2}$ [9, Theorem 2].

Example 6. We illustrate the application of Theorem 4 with parameters $l = 1, m = 5, n_1 = 3, k = 13, r_1 = 1$: $F(x) = Tr_{2^5}^{2^{15}}(x^{33})^{13}$. F corresponds to a balanced vectorial Boolean function with 15 input bits and 5 output bits. The function $Tr_2^{2^5}(x^{13})$ is plateaued(4) as it corresponds to the Kasami exponent in Table 1 for $r = 2$. By Theorem 4, the nonlinearity of F is $2^{14} - 2^7 = 16256$. By Remark 6, the maximum correlation satisfies $C_F(w) \leq 2^{(5-15)/2} = 0.03125$, $w \neq 0$. The algebraic degree of F is $2wt(k) = 6$ and its linear span is $n_1^{wt(k)} = 3^3 = 27$.

6 Conclusion

We have applied the theory of geometric sequences, due to Klapper, Chan and Goresky [12], to construct n-variable resilient Boolean functions with nonlinearity $2^{n-1} - 2^{(n-1)/2}$, n odd. Moreover, the Hadamard transforms of these functions are 3-valued, which provides protection against the soft output joint attack [13]. They can be extended to construct highly nonlinear resilient functions that disprove Pasalic and Johansson's conjecture for n even. These functions do not have a weakness shared by Boolean functions formed from concatenating linear functions. We also applied geometric sequences to give a new construction for balanced Boolean functions having high nonlinearity $> 2^{n-1} - 2^{(n-1)/2}$, n odd. This approach is different from previous constructions, which were based on direct sums of highly nonlinear Boolean functions. Finally, we constructed balanced vectorial Boolean functions with high nonlinearity and low maximum correlation. They can be used as combiners for stream ciphers with high throughput.

7 Acknowledgement

We would like to thank one of the referees for his/her helpful comments, and also Douglas R. Stinson for proof reading this paper. Research for this paper is supported by NSERC grant RG-PIN 227700-00. Khoongming Khoo's research is supported by a postgraduate scholarship from DSO National Laboratories, Singapore.

References

1. A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, "Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions", LNCS 1807, *Eurocrypt'2000*, pp. 507-522, Springer-Verlag, 2000.
2. A. Canteaut, P. Charpin and H. Dobbertin, "Binary m-sequences with three-valued cross correlation: a proof of Welch's conjecture", *IEEE Trans. Inform. Theory*, vol. 46 no. 1, pp. 4-8, 2000.
3. C. Carlet, "A Larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction", LNCS 2442, *Crypto'2002*, pp. 549-564, Springer-Verlag, 2002.
4. H. Dobbertin, "Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity", LNCS 1008, *Fast Software Encryption*, pp. 61-74, Springer Verlag, 1994.
5. R. Gold, "Maximal Recursive Sequences with 3-valued Cross Correlation Functions", *IEEE Trans. Inform. Theory* 14, pp. 154-156, 1968.
6. G. Gong, "Q-ary Cascaded GMW Sequences", *IEEE Trans. Inform. Theory*, vol.42 no.1, pp. 263-267, Jan 1996.
7. G. Gong and A.M. Youssef, "Cryptographic Properties of the Welch-Gong Transformation Sequence Generators", *IEEE Trans. Inform. Theory*, vol.48 no.11, pp. 2837-2846, Nov 2002.
8. T. Jacobsen, L. Knudsen, "The Interpolation Attack on Block Ciphers", LNCS 1267, *Fast Software Encryption*, pp.28-40, 1997.
9. K. Khoo and G. Gong,"Highly Nonlinear Sboxes with Reduced Bound on Maximum Correlation", in *Proceedings of IEEE International Symposium on Inform. Theory 2003*.
10. K. Kurosawa and T. Satoh, "Design of $SAC/PC(l)$ of Order k Boolean Functions and Three Other Cryptographic Poperties", pp. 434-449, LNCS 1233, *Eurocrypt'97*, Springer-Verlag, 1997.
11. T. Kasami, "The Weight Enumerators for several Classes of Subcodes of Second Order Binary Reed Muller Codes, *Information and Control*, vol. 18, pp. 369-394, 1971.
12. A. Klapper, A.H. Chan and M. Goresky, "Cascaded GMW sequence", *IEEE Transactions on Information Theory*, vol. 39 no. 1, pp. 177-183, 1993.
13. S. Leveiller, G. Zemor, P. Guillot,J. Boutros, "A New Cryptanalytic Attack for PN-Generators Filtered by a Boolean Function", *Proceedings of Selected Areas of Cryptography 2002*, 2002.
14. M. Matsui, "Linear cryptanalysis method for DES cipher", LNCS 765, *Eurocrypt'93*, pp. 386-397, 1994.
15. F.J. McWilliams and N.J.A. Sloane, *Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.
16. W. Millan, A. Clark and E. Dawson, "Heuristic Design of Cryptographically Strong Balanced Boolean Functions", LNCS 1403, *Eurocrypt'98*, Springer-Verlag, 1998.
17. Y. Niho, "Multi Valued Cross-Correlation Functions Between Two Maximal Linear Recursive Sequences, *Ph.D. dissert*, Univ. of Southern California, 1972.
18. E. Pasalic and T. Johansson, "Further Results on the Relationship between Nonlinearity and Resiliency of Boolean Functions", LNCS, *IMA Conference on Coding and Cryptography 1999*, Springer Verlag, 1999.
19. N.J Patterson and D.H. Wiedemann, "The Covering Radius of the $(2^{15}, 16)$ Reed-Muller Code is at least 16276", *IEEE Trans. Inform. Theory*, vol. 29 no. 3, pp. 354-356, May 1983.
20. N.J Patterson and D.H. Wiedemann, "Correction to - The Covering Radius of the $(2^{15}, 16)$ Reed-Muller Code is at least 16276", *IEEE Trans. Inform. Theory*, vol. 36 no. 2, pp. 443, Mar 1990.
21. P. Sarkar and S. Maitra, "Construction of Nonlinear Boolean Functions with Important Cryptographic Properties", LNCS 1807, *Eurocrypt'2000*, pp. 485-506, Springer-Verlag, 2000.
22. S. Maitra and P. Sarkar, "Modifications of Patterson-Wiedemann Functions for Cryptographic Applications", *IEEE Trans. on Inform. Theory*, vol. 48, pp. 278-284, 2002.
23. J. Seberry, X.M. Zhang, Y. Zheng, "Nonlinearly Balanced Boolean Functions and their Propagation Characteristics", LNCS 773, *Crypto'93*, pp. 49-60, Springer-Verlag, 1993.
24. J. Seberry, X.M. Zhang and Y. Zheng, "Structures of Cryptographic Functions with Strong Avalanche Characteristics", LNCS 917, *Asiacrypt'94*, pp. 119-132, Springer-Verlag, 1994.
25. T. Siegenthaler, "Decrypting a Class of Stream Ciphers using Ciphertexts only", *IEEE Trans. Computer*, vol. C34 no. 1, pp. 81-85, 1985.
26. M. Zhang and A. Chan, "Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers", LNCS 1880, *Crypto'2000*, pp. 501-514, Springer-Verlag, 2000.
27. Y. Zheng and X.M. Zhang, "Relationships between Bent Functions and Complementary Plateaued Functions", LNCS 1787, *ICISC'99*, pp. 60-75, Springer-Verlag, 1999.
28. Y. Zheng and X.M. Zhang, "On Relationship among Avalanche, Nonlinearity and Correlation Immunity", LNCS 1976, *Asiacrypt'2000*, pp. 470-482, Springer-Verlag, 2000.