On Cryptographically Secure Vectorial Boolean Functions

Takashi Satoh[1], Tetsu Iwata[2], and Kaoru Kurosawa[2]

[1] Faculty of International Environmental Engineering
Promotion and Development Office,
Kitakyushu University
4–2–1 Kitagata, Kokuraminami-ku, Kitakyushu 802–8577, Japan
tsatoh@kitakyu-u.ac.jp

[2] Department of Electrical and Electronic Engineering,
Faculty of Engineering,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152–8552, Japan
{tez,kurosawa}@ss.titech.ac.jp

Abstract. In this paper, we show the first method to construct vectorial bent functions which satisfy both the largest degree and the largest number of output bits simultaneously. We next apply this method to construct balanced vectorial Boolean functions which have larger nonlinearities than previously known constructions.

1 Introduction

Boolean functions play an important role in block ciphers (for example, see [3,7,8,10,11]) and stream ciphers [12,2]. The nonlinearity N_f of a Boolean function $f(x_1, \ldots, x_n)$ is defined as a distance between f and the set of affine functions $\{a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n\}$. N_f should be large to resist the linear attack [2,6].

$f(x_1, \ldots, x_n)$ is said to be a bent function if it has the maximum nonlinearity [5,9]. More generally, we say that a vectorial Boolean function $F(x_1, \ldots, x_n) = (f_1, \ldots, f_m)$ is a (n, m)-bent function if any nonzero linear combination of $f_1, \ldots, f_m$ is a bent function. For (n, m)-bent functions, it is known that [7]

$$m \le n/2 \ . \tag{1}$$

On the other hand, the degree of f, $\deg(f)$, is defined as the degree of the highest degree term of the algebraic normal form:

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{1\le i\le n} a_ix_i \oplus \bigoplus_{1\le i<j\le n} a_{i,j}x_ix_j \oplus \cdots \oplus a_{1,2,\ldots,n}x_1x_2\cdots x_n \ .$$

The degree of a vectorial Boolean function $F(x_1, \ldots, x_n) = (f_1, \ldots, f_m)$ is defined as

$$\deg(F) \overset{\triangle}{=} \min_{(c_1,\ldots,c_m)\ne(0,\ldots,0)} \deg(c_1f_1 \oplus \cdots \oplus c_mf_m) \ .$$

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 20–28, 1999.

In block ciphers, $\deg(F)$ should be large to resist the higher order differential attack [4]. For (n,m)-bent functions, it is known that [5,9]

$$\deg(F) \leq n/2 \ . \tag{2}$$

However, no construction method has been known so far which achieves both equalities of eq.(1) and eq.(2) simultaneously. In this paper, we show the first method to construct (n,m)-bent functions which satisfy the both equalities of eq.(1) and eq.(2) simultaneously.

It is known that bent functions are not balanced. For $m = 1$, Seberry, Zhang and Zheng [10] and Dobbertin [3] showed balanced functions which have large nonlinearity. For $m = n$, Nyberg showed balanced *vectorial* Boolean functions with high nonlinearity [8].

We next apply our method to construct balanced vectorial Boolean functions with high nonlinearity. For $2 \leq m \leq n/2$, our balanced vectorial Boolean functions have larger nonlinearity than that of [8].

2 Bent Functions

For a Boolean function $f(x_1, \dots, x_n)$, define

$$\|f(x_1, \dots, x_n)\| \overset{\triangle}{=} |\{(x_1, \dots, x_n) \mid f(x_1, \dots, x_n) = 1\}| \ .$$

$$N_f \overset{\triangle}{=} \min_{a_0, \dots, a_n} \|f(x_1, \dots, x_n) \oplus (a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n)\| \ .$$

N_f is called the nonlinearity of f and it denotes a distance between f and the set of affine functions $\{a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n\}$. For a vectorial Boolean function $F(x_1, \dots, x_n) = (f_1, \dots, f_m)$, the nonlinearity N_F is defined as

$$N_F \overset{\triangle}{=} \min_{(c_1, \dots, c_m) \neq (0, \dots, 0)} N_{c_1 f_1 \oplus \cdots \oplus c_m f_m} \ . \tag{3}$$

N_F should be large to resist the linear attack [2,6]. It is known that

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1} \text{ and } N_F \leq 2^{n-1} - 2^{\frac{n}{2}-1} \ . \tag{4}$$

Definition 2.1. *$f(x_1, \dots, x_n)$ is called a bent function if $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. $F(x_1, \dots, x_n) = (f_1, \dots, f_m)$ is called a (n,m)-bent function if $N_F = 2^{n-1} - 2^{\frac{n}{2}-1}$.*

Proposition 2.1. *[5,9] If $f(x_1, \dots, x_n)$ is a bent function, then n is even and*

$$\deg(f) \leq n/2 \ .$$

Proposition 2.2. *[7] If $F(x_1, \dots, x_n) = (f_1, \dots, f_m)$ is a (n,m)-bent function, then n is even,*

$$m \leq n/2 \text{ and } \deg(F) \leq n/2 \ .$$

For even n, let $\mathcal{X} \stackrel{\triangle}{=} (x_1, \ldots, x_{n/2})$ and $\mathcal{Y} \stackrel{\triangle}{=} (y_1, \ldots, y_{n/2})$. Then it is known that

$$f(\mathcal{Y}, \mathcal{X}) = \pi(\mathcal{Y}) \cdot \mathcal{X}^T \oplus g(\mathcal{Y})$$

is a bent function if π is a permutation on $\{0,1\}^{n/2}$, where $g(\mathcal{Y})$ is any Boolean function [1]. This is called a Maiorana-McFarland type bent function [1]. From the definition of (n,m)-bent functions, we have the following proposition immediately.

Proposition 2.3. *[7] $F(\mathcal{Y}, \mathcal{X}) = (f_1, \ldots, f_m)$ is a (n,m)-bent function if*

$$f_i(\mathcal{Y}, \mathcal{X}) = \pi_i(\mathcal{Y}) \cdot \mathcal{X}^T \oplus g_i(\mathcal{Y})$$

and every nonzero linear combination of $\{\pi_i\}$ is a permutation on $\{0,1\}^{n/2}$, where $g_i(\mathcal{Y})$ is any Boolean function.

Nyberg gave several constructions of such $\{\pi_i\}$ [7].

3 Proposed Vectorial Bent Function

3.1 Notation

For a binary vector $(y_1, \ldots, y_m)$, define

$$dec(y_1, \ldots, y_m) \stackrel{\triangle}{=} 2^{m-1}y_1 + 2^{m-2}y_2 + \cdots + y_m \ .$$

For an element α of GF(2^m), let $[\alpha]$ denote a vector representation of α.

3.2 Proposed Construction

We now present a method to construct (n,m)-bent functions which satisfy both equalities of Proposition 2.2.

Proposition 3.1. *[5, page 372] Any Boolean function f can be expanded as*

$$f(x_1, \ldots, x_n) = \bigoplus_{a_1, \ldots, a_n} h(a_1, \ldots, a_n) x_1^{a_1} \cdots x_n^{a_n} \ ,$$

where

$$h(a_1, \ldots, a_n) = \bigoplus_{b \subset a} f(b_1, \ldots, b_n) \ ,$$

and $b \subset a$ means that the 1's in $(b_1, \ldots, b_n)$ are a subset of the 1's in $(a_1, \ldots, a_n)$.

Lemma 3.1. *Let α be a primitive element of* GF(2^m)*. Then*

$$1 + \alpha + \alpha^2 + \cdots + \alpha^l \begin{cases} \neq 0 & \text{if } \ 0 < l+1 < 2^m - 1 \ , \\ = 0 & \text{if } \ l+1 = 2^m - 1 \ . \end{cases}$$

Proof. Since α is a primitive element, we have

$$(1+\alpha)(1+\alpha+\alpha^2+\cdots+\alpha^l) = 1+\alpha^{l+1}\begin{cases}\neq 0 & \text{if } 0<l+1<2^m-1\ ,\\ =0 & \text{if } l+1=2^m-1\ .\end{cases}$$

Therefore, this lemma holds. □

For even n, let $m = n/2$, $\mathcal{X} = (x_1, \ldots, x_m)$ and $\mathcal{Y} = (y_1, \ldots, y_m)$. Let α be a primitive element of $\mathrm{GF}(2^{n/2})$. Consider $F(\mathcal{Y}, \mathcal{X}) = (f_1, \ldots, f_{n/2})$ such that

$$f_i(\mathcal{Y}, \mathcal{X}) = [\varphi_i(\mathcal{Y})] \cdot \mathcal{X}^T \oplus g_i(\mathcal{Y})\ ,$$

where

$$\varphi_i(\mathcal{Y}) \triangleq \begin{cases}0 & \text{if } \mathcal{Y} = (0, \ldots, 0)\ ,\\ \alpha^{dec(\mathcal{Y})+i-1} & \text{otherwise}\end{cases}$$

and g_i is any Boolean function.

Theorem 3.1. *The above F is a (n, m)-bent function such that $m = n/2$ and* $\deg(F) = n/2$*.*

Proof. For any $c = (c_1, \ldots, c_m) \neq (0, \ldots, 0)$, let

$$\varPhi_c(\mathcal{Y}) \triangleq c_1\varphi_1(\mathcal{Y}) + \cdots + c_m\varphi_m(\mathcal{Y})\ . \tag{5}$$

Then it is easy to see that

$$\varPhi_c(\mathcal{Y}) = \begin{cases}0 & \text{if } \mathcal{Y} = (0, \ldots, 0)\ ,\\ \alpha^{dec(\mathcal{Y})}\gamma & \text{otherwise}\quad ,\end{cases} \tag{6}$$

where

$$\gamma \triangleq (c_1 + c_2\alpha + \cdots + c_m\alpha^{m-1}) \neq 0 \tag{7}$$

because α is a primitive element of $\mathrm{GF}(2^m)$. This implies that $[\varPhi_c(\mathcal{Y})]$ is a permutation on $\{0, 1\}^m$. Therefore, F is a $(n, n/2)$-bent function from Proposition 2.3.

Next suppose that $[\varPhi_c(\mathcal{Y})]$ is written as

$$\begin{aligned}[\varPhi_c(\mathcal{Y})] = {} & h(1, \ldots, 1)y_1 \cdots y_m\\ & \oplus h(1, \ldots, 1, 0)y_1 \cdots y_{m-1}\\ & \oplus \cdots \oplus h(0, 1, \ldots, 1)y_2 \cdots y_m\\ & \oplus \cdots \oplus h(0, \ldots, 0)\ .\end{aligned}$$

Let $\beta \triangleq 1 + \alpha + \alpha^2 + \cdots + \alpha^{2^{m-1}-1}$. Then

$$\beta = 1 + \alpha + \alpha^2 + \cdots + \alpha^{2^{m-1}-1} = \sum_{(i_2, \ldots, i_m)} \alpha^{dec(0, i_2, \ldots, i_m)}\ .$$

From eq.(6)

$$\gamma\beta = \gamma\left(\sum_{(i_2,\ldots,i_m)} \alpha^{dec(0,i_2,\ldots,i_m)}\right) = \sum_{(i_2,\ldots,i_m)} \Phi_c(0,i_2,\ldots,i_m) \ .$$

Finally, from Proposition 3.1, we have

$$h(0,1,\ldots,1) = \bigoplus_{(i_2,\ldots,i_m)} [\Phi_c(0,i_2,\ldots,i_m)] = [\gamma\beta] \ . \tag{8}$$

Hence, we have

$$[\Phi_c(\mathcal{Y})]\cdot\mathcal{X}^T = [\gamma\beta]\cdot\mathcal{X}^T y_2\cdots y_m \oplus \cdots \ , \tag{9}$$

where $\gamma\beta \neq 0$ from Lemma 3.1 and eq.(7). Therefore,

$$\deg([\Phi_c(\mathcal{Y})]\cdot\mathcal{X}^T) \geq \deg([\gamma\beta]\cdot\mathcal{X}^T y_2\cdots y_m) = m = n/2 \ .$$

This means that $\deg(F) = n/2$ since $\deg(F) \leq n/2$ from Proposition 2.2. □

3.3 Maximum Degree for Each Variable

Definition 3.1. *We say that a (n,m)-bent function $F(x_1,\ldots,x_n) = (f_1,\ldots,f_m)$ has the maximum degree for each variable if each variable x_i appears in some term of degree $n/2$.*

Definition 3.2. *[5, page 120] A normal basis of* $\mathrm{GF}(p^k)$ *is a basis of the form* $\beta, \beta^p, \ldots, \beta^{p^k-1}$.

Proposition 3.2. *[5, page 122] A normal basis exists in any field* $\mathrm{GF}(p^k)$.

Theorem 3.2. *In the proposed construction, let $m = n/2$ and let*

$$\beta = 1 + \alpha + \alpha^2 + \cdots + \alpha^{2^{m-1}-1} \ . \tag{10}$$

Then our (n,m)-bent function F has the maximum degree for each variable if $\{\beta, \beta^2, \ldots, \beta^{2^{m-1}}\}$ *is a normal basis of* $\mathrm{GF}(2^m)$.

Proof. In eq.(8), we have proved that

$$h(0,1,\ldots,1) = [\gamma\beta] \ .$$

Similarly, we can prove that

$$\begin{gathered} h(1,\ldots,1,0) = [\gamma\beta^2] \ , \\ h(1,\ldots,1,0,1) = [\gamma\beta^{2^2}] \ , \\ \vdots \end{gathered}$$

Then eq.(9) becomes as follows.

$$[\Phi_c(\mathcal{Y})] \cdot \mathcal{X}^T = [\gamma\beta^2] \cdot \mathcal{X}^T y_1 \cdots y_{m-1} \oplus \cdots \oplus [\gamma\beta] \cdot \mathcal{X}^T y_2 \cdots y_m \oplus \cdots \ .$$

Now $[\gamma\beta^2], [\gamma\beta^{2^2}], \ldots, [\gamma\beta]$ are linearly independent since $\{\beta, \beta^2, \ldots, \beta^{2^{m-1}}\}$ is a normal basis and $\gamma \neq 0$. This means that each x_i is included in some term of degree $m = n/2$. It is clear that each y_i is included in some term of degree $n/2$. □

Corollary 3.1. *Our $(n, n/2)$-bent function F has the maximum degree for each variable if $2^{n/2} - 1$ is a prime.*

Proof. There exists a normal basis $\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n/2-1}}$ in $\mathrm{GF}(2^{n/2})$ from Proposition 3.2. On the other hand, if eq.(10) holds, then from lemma 3.1,

$$(1 + \alpha^{2^{m-1}})\beta = 1 + \alpha + \alpha^2 + \cdots + \alpha^{2^m-1} = \alpha^{2^m-1} = 1$$

and

$$\begin{aligned} (1 + \alpha^{2^m})\beta^2 &= 1 \\ (1 + \alpha)\beta^2 &= 1 \\ \alpha &= \beta^{-2} + 1 \ . \end{aligned}$$

Now any nonzero element is a primitive element of $\mathrm{GF}(2^{n/2})$ if $2^{n/2} - 1$ is a prime. Therefore, $\alpha = \beta^{-2} + 1$ is a primitive element. This implies that the condition of Theorem 3.2 is satisfied. □

4 Application to Balanced Boolean Functions

We say that $f(x_1, \ldots, x_n)$ is balanced if

$$\|f(x_1, \ldots, x_n)\| = 2^{n-1} \ .$$

We also say that $F(x_1, \ldots, x_n) = (f_1, \ldots, f_m)$ is balanced if any nonzero linear combination of $f_1, \ldots, f_m$ is balanced.

For $m = 1$, Seberry, Zhang and Zheng [10] and Dobbertin [3] showed balanced functions which have large nonlinearity. For $m = n$, Nyberg showed balanced *vectorial* Boolean functions with high nonlinearity such as follows.

Proposition 4.1. *[8] For $m = n$, there exists a balanced vectorial Boolean function such that*

$$N_F \begin{cases} \geq 2^{n-1} - 2^{\frac{n}{2}} & \text{if } n \text{ is even} \ , \\ = 2^{n-1} - 2^{\frac{n-1}{2}} & \text{if } n \text{ is odd} \ . \end{cases}$$

This section shows that we can obtain balanced *vectorial* Boolean functions which have larger nonlinearity than Proposition 4.1 for $2 \leq m \leq n/2$ by applying our technique of Sec.3.2.

Theorem 4.1. *Suppose that there exists a balanced vectorial Boolean function* $F(x_1,\ldots,x_h)=(f_1,\ldots,f_m)$ *with nonlinearity* N_F *for* $m\le h$. *Then there exists a balanced vectorial Boolean function* $\widetilde{F}=(\tilde{f}_1,\ldots,\tilde{f}_m)$ *with* $2h$ *input variables such that*

$$N_{\widetilde{F}} \ge N_F + 2^{h-1}(2^h-2) \ .$$

Proof. Let $\mathcal{X}=(x_1,\ldots,x_h)$ and $\mathcal{Y}=(y_1,\ldots,y_h)$. Let α be a primitive element of GF(2^h). Define

$$\widetilde{f}_i(\mathcal{Y},\mathcal{X}) \overset{\triangle}{=} \begin{cases} f_i(\mathcal{X}) & \text{if } \mathcal{Y}=(0,\ldots,0) \ , \\ \left[\alpha^{dec(\mathcal{Y})+i-1}\right]\cdot\mathcal{X}^T \oplus g_i(\mathcal{Y}) & \text{otherwise} \quad . \end{cases}$$

where $g_i(\mathcal{Y})$ is any Boolean function. Let $\widetilde{F}(\mathcal{Y},\mathcal{X}) \overset{\triangle}{=} (\widetilde{f}_1,\ldots,\widetilde{f}_m)$. For any $\mathbf{c}=(c_1,\ldots,c_m)\ne(0,\ldots,0)$, let

$$\begin{aligned} \widetilde{f}_{\mathbf{c}}(\mathcal{X},\mathcal{Y}) &\overset{\triangle}{=} c_1 f_1(\mathcal{X},\mathcal{Y}) \oplus\cdots\oplus c_m f_m(\mathcal{X},\mathcal{Y}) \\ &= \begin{cases} c_1 f_1(\mathcal{X}) \oplus\cdots\oplus c_m f_m(\mathcal{X}) & \text{if } \mathcal{Y}=(0,\ldots,0) \ , \\ \Big(c_1[\varphi_1(\mathcal{Y})]\oplus\cdots\oplus c_m[\varphi_m(\mathcal{Y})]\Big)\cdot\mathcal{X}^T & \text{otherwise} \quad , \\ \qquad\qquad \oplus c_1 g_1(\mathcal{Y})\oplus\cdots c_m g_i(\mathcal{Y}) & \end{cases} \end{aligned}$$

where $\varphi_i(\mathcal{Y})=\alpha^{dec(\mathcal{Y})+i-1}$.

We first prove that $\widetilde{f}_{\mathbf{c}}(\mathcal{Y},\mathcal{X})$ is balanced. For $\mathcal{Y}=(0,\ldots,0)$, $\widetilde{f}_{\mathbf{c}}(\mathcal{X},0,\ldots,0)=c_1f_1\oplus\cdots\oplus c_mf_m$ is balanced since F is balanced. For $\mathcal{Y}\ne(0,\ldots,0)$,

$$\begin{aligned} c_1[\varphi_1(\mathcal{Y})]\oplus\cdots\oplus c_m[\varphi_m(\mathcal{Y})] &= [\alpha^{dec(\mathcal{Y})}(c_1+c_2\alpha+\cdots+c_m\alpha^{m-1})] \\ &= [\alpha^{dec(\mathcal{Y})}\gamma]\ne(0,\ldots,0) \end{aligned} \tag{11}$$

where $\gamma=c_1+c_2\alpha+\cdots+c_m\alpha^{m-1}$. Note that $\gamma\ne0$ since α is a primitive element of GF(2^h). Therefore $(c_1[\varphi_1(\mathcal{Y})]\oplus\cdots\oplus c_m[\varphi_m(\mathcal{Y})])\cdot\mathcal{X}^T=[\alpha^{dec(\mathcal{Y})}\gamma]\cdot\mathcal{X}^T$ is balanced for each fixed $\mathcal{Y}\ne(0,\ldots,0)$. This implies that $\widetilde{f}_{\mathbf{c}}(\mathcal{Y},\mathcal{X})$ is balanced.

We next compute the nonlinearity of $\widetilde{f}_{\mathbf{c}}(\mathcal{Y},\mathcal{X})$. Let

$$L(\mathcal{Y},\mathcal{X})=\mathbf{a}\cdot\mathcal{Y}^T\oplus\mathbf{b}\cdot\mathcal{X}^T\oplus c_0 \ .$$

Then

$$\begin{aligned} N_{\widetilde{F}} &= \min_L ||\widetilde{f}_{\mathbf{c}}(\mathcal{Y},\mathcal{X})\oplus L(\mathcal{Y},\mathcal{X})|| \\ &\ge \min_L ||\widetilde{f}_{\mathbf{c}}(0,\ldots,0,\mathcal{X})\oplus L(0,\ldots,0,\mathcal{X})|| \\ &\quad + \min_L \sum_{\mathcal{Y}\ne(0,\ldots,0)} ||\widetilde{f}_c(\mathcal{Y},\mathcal{X})\oplus L(\mathcal{Y},\mathcal{X})|| \\ &= \min_{\mathbf{b},c_0} ||c_1f_1(\mathcal{X})\oplus\cdots\oplus c_mf_m(\mathcal{X})\oplus\mathbf{b}\cdot\mathcal{X}^T\oplus c_0|| \\ &\quad + \min_{\mathbf{b},c_0} \sum_{\mathcal{Y}\ne(0,\ldots,0)} ||(c_1[\varphi_1(\mathcal{Y})]\oplus\cdots\oplus c_m[\varphi_m(\mathcal{Y})]\oplus\mathbf{b})\cdot\mathcal{X}^T\oplus\widetilde{c}_{\mathcal{Y}}|| \\ &\ge N_F + \min_{\mathbf{b},c_0} \sum_{\mathcal{Y}\ne(0,\ldots,0)} ||([\alpha^{dec(\mathcal{Y})}\gamma]\oplus\mathbf{b})\cdot\mathcal{X}^T\oplus\widetilde{c}_{\mathcal{Y}}|| \end{aligned}$$

for some $\widetilde{c}_{\mathcal{Y}}$ (= 0 or 1) from eq.(11). For any $\mathbf{b}$, there exists at most one $\mathcal{Y}$ such that

$$[\alpha^{dec(\mathcal{Y})}\gamma] \oplus \mathbf{b} = (0, \ldots, 0) \ . \tag{12}$$

If $[\alpha^{dec(\mathcal{Y})}\gamma] \oplus \mathbf{b} \neq (0, \ldots, 0)$, then

$$||([\alpha^{dec(\mathcal{Y})}\gamma] \oplus \mathbf{b}) \cdot \mathcal{X}^T \oplus \widetilde{c}_{\mathcal{Y}}|| = 2^{h-1} \ .$$

Hence,

$$N_{\widetilde{F}} \geq N_F + 2^{h-1}\left((2^h - 1) - 1\right) \ .$$

□

Corollary 4.1. *Suppose that there exists a balanced vectorial Boolean function $F(x_1, \ldots, x_h) = (f_1, \ldots, f_m)$ with nonlinearity N_F for $m \leq h$. Then there exists a balanced vectorial Boolean function $\widetilde{F}$ with $2^s h$ input variables such that*

$$N_{\widetilde{F}} \geq N_F + 2^{2^s h - 1} - \frac{1}{2}(2^{2^{s-1}h} + 2^{2^{s-2}h} + \cdots + 2^{2h} + 2 \cdot 2^h) \ .$$

Finally, we can obtain the following corollary from Corollary 4.1 and Proposition 4.1.

Corollary 4.2. *If $n = 2^s h$, then there exists a balanced vectorial Boolean function $F(x_1, \ldots, x_n) = (f_1, \ldots, f_m)$ such that $m \leq h$ and*

$$N_F \geq \begin{cases} 2^{2^s h - 1} - \frac{1}{2}(2^{2^{s-1}h} + 2^{2^{s-2}h} + \cdots + 2^h + 2^{\frac{h}{2}+1}) & \textit{if } h \textit{ is even} \quad , \\ 2^{2^s h - 1} - \frac{1}{2}(2^{2^{s-1}h} + 2^{2^{s-2}h} + \cdots + 2^h + 2^{\frac{h+1}{2}}) & \textit{if } h \textit{ is odd} \quad . \end{cases}$$

(Remark) Corollary 4.2 gives larger nonlinearity than Proposition 4.1 for $s \geq 1$ which corresponds to $2 \leq m \leq n/2$.

References

1. J.F. Dillon. Elementary Hadamard difference sets. In *The Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing*, pages 237–249, 1975. 22
2. C.Ding, G.Xiao and W.Shan. The stability theory of stream ciphers. Lecture Notes in Computer Science 561, Springer-Verlag, 1991. 20, 21
3. H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. In *Fast Software Encryption*, volume 1008 of *Lecture Notes in Computer Science*, pages 61–74, Springer-Verlag, 1995. 20, 21, 25
4. T. Jakobsen and L. R. Knudsen. The interpolation attack on block ciphers. In *Fast Software Encryption*, volume 1267 of *Lecture Notes in Computer Science*, pages 28–40, Springer-Verlag, 1997. 21
5. F.J. MacWilliams and N.J.A. Sloane. The theory of error-correcting codes. North-Holland Publishing Company, 1977. 20, 21, 22, 24

6. M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology —EUROCRYPT '93 Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386-397, Springer-Verlag, 1994. 20, 21
7. K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology —EUROCRYPT '91 Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386, Springer-Verlag, 1991. 20, 21, 22
8. K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology —EUROCRYPT '92 Proceedings*, volume 658 of *Lecture Notes in Computer Science*, pages 92–98, Springer-Verlag, 1993. 20, 21, 25
9. O. S. Rothaus. On bent functions. In *Journal of Combinatorial Theory (A)*, 20:300–305, 1976. 20, 21
10. J. Seberry, X.M. Zhang and Y. Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. In *Information and Computation*, 119(1):1–13, May 1995. 20, 21, 25
11. X.M. Zhang and Y. Zheng. Cryptographically resilient functions. In *IEEE Transactions on Information Theory*, 43(5):1740–1747, September 1997. 20
12. T.Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. In *IEEE Transactions on Information Theory*, 30(5):776–780, 1984. 20