On the Iterative Construction of Bent Functions[1]

JOAN-JOSEP CLIMENT[(a)], FRANCISCO J. GARCÍA[(b)], VERÓNICA REQUENA[(a)]
[(a)]Departament de Ciència de la Computació i Intel·ligència Artificial
[(b)]Departament de Fonaments de l'Anàlisi Econòmica
Universitat d'Alacant
Ap. 99 E-03080 Alacant
SPAIN

Abstract: In this paper we present two methods to construct iteratively bent functions of $n+2$ variables from bent functions of n variables. Our methods use bent functions expressed as sum of minterms.

Key-words: Boolean function, cryptography, nonlinearity, bent function, minterm, balanced sequence.

1 Introduction

Boolean functions are used for a wide variety of applications in engineering and computer science. They have been the subject of cryptography [4, 5, 11], coding theory [3, 7, 9], and digital communications [6, 8, 13], among others. The most important Boolean functions are bent functions since they are a very important tool in different kinds of cryptographic applications, like stream ciphers and block ciphers. That is why we need to find Boolean functions with a variety of criteria that reduce the effectiveness of advanced cryptanalytic attack, such as linear [10] and differential [2, 12]. Bent functions are the Boolean functions achieving the upper bound on nonlinearity, so that they offer the maximum possible resistance to these attacks [15]. Bent functions with 4 variables have been very studied, and therefore we know the number of bent functions that there are. However a general method to generate all the bent functions in n variables is unknown for $n \geq 6$ (see for example [1, 14, 16, 17]). So that, we want to contribute to the knowledge of that functions with the introduction of two methods to construct bent functions for any value of n. These methods are based on minterms.

2 Preliminaries

Let n be a positive integer and $B = \{0, 1\}$. A function $f : B^n \longrightarrow B$ is called a **Boolean function** of n variables. For $i = 0, 1, \ldots, 2^n - 1$, let $\boldsymbol{\beta}_i$ be the vector in B^n whose integer representation is i. For a Boolean function f, the $(0,1)$-sequence

$$\xi_f = (f(\boldsymbol{\beta_0}),\ f(\boldsymbol{\beta_1}),\ \ldots\ , f(\boldsymbol{\beta_{2^n-1}}))$$

is called the **truth table** of f.

We say that a Boolean function f is an **affine function** if it takes the form

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{i=1}^{n} a_i x_i \oplus b,$$

where $a_i, b \in B$ for $i = 1, 2, \ldots, n$ and $\oplus$ is the binary addition. In addition, f is called a **linear function** if $b = 0$.

The **Hamming weight** of a $(0,1)$-sequence $\boldsymbol{\alpha}$, denoted by $\mathrm{w}(\boldsymbol{\alpha})$, is the number of 1s in $\boldsymbol{\alpha}$. A $(0,1)$-sequence is **balanced** if it contains an equal number of 0s and 1s; a Boolean function f is **balanced** if its truth table is balanced. The **Hamming distance** between two $(0,1)$-sequences $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, denoted by $\mathrm{d}(\boldsymbol{\alpha}, \boldsymbol{\beta})$, is the number of positions where the two sequences differ, that is $\mathrm{d}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \mathrm{w}(\boldsymbol{\alpha} \oplus \boldsymbol{\beta})$. For two Boolean functions f and g we have that $\mathrm{w}(f) = \mathrm{w}(\xi_f)$ and $\mathrm{d}(f, g) = \mathrm{d}(\xi_f, \xi_g)$.

The **nonlinearity** NL of a Boolean function f is given by

$$\mathrm{NL}(f) = \min\{\mathrm{d}(f, \varphi) \mid \varphi \in \mathcal{A}_n\}$$

where $\mathcal{A}_n$ is the set of all affine functions; it is well known (see [18]) that

$$\mathrm{NL}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

The Boolean functions that attains the maximum nonlinearity are called **bent functions** (see [18]), in this case, n must be even. It follows then that $f(\boldsymbol{x})$ is a bent function if and only $1 \oplus f(\boldsymbol{x})$ is a bent function.

A **minterm** on n variables $x_1, x_2, \ldots, x_n$ is a Boolean function

$$m_{e_1 e_2 \cdots e_n}(x_1, x_2, \ldots, x_n) = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$$

where

$$x^e = \begin{cases} x, & \text{if } e = 1, \\ 1 \oplus x, & \text{if } e = 0. \end{cases}$$

[1]This work was partially supported by Spanish grant MTM2005-05759

We write $m_i(\boldsymbol{x})$ instead of $m_{\boldsymbol{\beta}_i}(\boldsymbol{x})$, and therefore $m_i(\boldsymbol{x}) = 1$ if only if $\boldsymbol{x} = \boldsymbol{\beta}_i$. So, the truth table of $m_i(\boldsymbol{x})$ has a 1 in the ith position and 0 elsewhere. Consequently,

$$\bigoplus_{i=0}^{2^n-1} m_i(\boldsymbol{x}) = 1. \tag{1}$$

It is well known that any Boolean function f can be expressed as

$$f(\boldsymbol{x}) = \bigoplus_{i\in I} m_i(\boldsymbol{x})$$

for a subset I of $\{1, 2, \ldots, n\}$.

According with the above comments, f is a bent function if and only if $f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})$ is a balanced function [18]; in addition, $g_\alpha(\boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{\alpha})$ is also a bent function. In addition if f is a bent function, then it has exactly $2^{n-1} \pm 2^{\frac{n}{2}-1}$ minterms; so that f is not balanced.

3 Main results

We consider that $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, y_2)$, also (i_0, i_1, i_2, i_3) and (j_0, j_1, j_2, j_3) will be permutations of $(0, 1, 2, 3)$.

The two following two lemmas, whose proofs can be obtained directly from the definition of minterm, are the key of our main results.

Lemma 1: *For each minterm in n variables, it is possible to construct 4 different minterms in $n + 2$ variables.*

Minterms have the following property that make them operative from the algebraic point of view.

Lemma 2: $m_{\boldsymbol{\alpha}}(\boldsymbol{\beta} \oplus \boldsymbol{x}) = m_{\boldsymbol{\alpha}\oplus\boldsymbol{\beta}}(\boldsymbol{x})$ *for* $\boldsymbol{\alpha}, \boldsymbol{\beta} \in B^n$.

In the following two theorems, that are the main results of this paper, we introduce two methods to construct bent functions.

Theorem 1: *If $f(\boldsymbol{x})$ is a bent function with n variables, then*

$$F(\boldsymbol{y}, \boldsymbol{x}) = \left(\bigoplus_{t=0}^{2} m_{i_t}(y)\right) f(\boldsymbol{x}) \oplus m_{i_3}(\boldsymbol{y}) \left(1 \oplus f(\boldsymbol{x})\right)$$

is a bent function with $n + 2$ variables.

PROOF: We need to prove that

$$F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x}) = F(\boldsymbol{y}, \boldsymbol{x}) \oplus F((\boldsymbol{\beta}, \boldsymbol{\alpha}) \oplus (\boldsymbol{y}, \boldsymbol{x}))$$

is balanced for all nonzero $(\boldsymbol{\beta}, \boldsymbol{\alpha}) \in B^2 \times B^n$

Now, by Lemma 2, by expression (1), and after some tedious algebraic manipulations, it follows then that

$$F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x}) = f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{\alpha}) \oplus m_{i_3}(\boldsymbol{y}) \oplus m_{i_3\oplus\boldsymbol{\beta}}(\boldsymbol{y}). \tag{2}$$

So, if $\mathbf{0}$ and $\mathbf{1}$ are the $2^n \times 1$ arrays with all entries equal to 0 and 1 respectively, $\boldsymbol{\tau}$ is the $2^n \times n$ array whose ith row is $\boldsymbol{\beta}_i$, and $\boldsymbol{\xi}_{\boldsymbol{\alpha}}$ is the truth table of $f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})$, then, according with expression (2), Table 1 show the truth table of $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ for $i_3 = 3$ and $\boldsymbol{\beta} = 2$.

To obtain the last column of the truth table for the different values of i_3 and $\boldsymbol{\beta}$ is not difficult.

We consider the following cases:

- $\boldsymbol{\beta} \neq \mathbf{0}_2$ and $\boldsymbol{\alpha} \neq \mathbf{0}_n$. In this case, the truth table of $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ has, according with the above comments, four blocs

  $$\boldsymbol{\xi}_{\boldsymbol{\alpha}} \quad \boldsymbol{\xi}_{\boldsymbol{\alpha}} \quad \boldsymbol{\xi}_{\boldsymbol{\alpha}} \oplus \mathbf{1} \quad \boldsymbol{\xi}_{\boldsymbol{\alpha}} \oplus \mathbf{1}$$

  not necessarily in that order. The exact position of each bloc depends on the values of i_3 and $\boldsymbol{\beta}$. Now, taking into account that the number of 1s (and also the number of 0s) in $\boldsymbol{\xi}_{\boldsymbol{\alpha}}$ is 2^{n-1}, we can ensure that the number of 1s in the truth table of $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ is $4 \cdot 2^{n-1} = 2^{n+1}$ and, consequently, $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ is balanced.

- $\boldsymbol{\beta} = \mathbf{0}_2$ and $\boldsymbol{\alpha} \neq \mathbf{0}_n$. In this case, the truth table of $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ has, four blocs

  $$\boldsymbol{\xi}_{\boldsymbol{\alpha}} \quad \boldsymbol{\xi}_{\boldsymbol{\alpha}} \quad \boldsymbol{\xi}_{\boldsymbol{\alpha}} \quad \boldsymbol{\xi}_{\boldsymbol{\alpha}}$$

  which correspond to a balanced sequence.

- $\boldsymbol{\beta} \neq \mathbf{0}_2$ and $\boldsymbol{\alpha} = \mathbf{0}_n$. In this case, $\boldsymbol{\xi}_{\boldsymbol{\alpha}} = \boldsymbol{\xi}_{\mathbf{0}} = \mathbf{0}$, and the truth table of $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ has four blocs

  $$\mathbf{0} \quad \mathbf{0} \quad \mathbf{1} \quad \mathbf{1}$$

  not necessarily in that order. So, it is balanced.

Consequently, $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y}, \boldsymbol{x})$ is balanced and, therefore, $F(\boldsymbol{y}, \boldsymbol{x})$ is a bent function. ■

For a given bent function $f(\boldsymbol{x})$ in n variables, we can construct, according with Theorem 1, $4!/3! = 4$ different bent functions in $n + 2$ variables.

Now, in a similar way as in the previous theorem, we have the following result.

y_1	y_2	$\boldsymbol{x}$	$m_0(\boldsymbol{y})$	$m_1(\boldsymbol{y})$	$m_2(\boldsymbol{y})$	$m_3(\boldsymbol{y})$	$f(\boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{x})$	$F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$
$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi_\alpha}$	$\boldsymbol{\xi_\alpha}$
$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$	$\boldsymbol{\xi_\alpha}$	$\boldsymbol{\xi_\alpha} \oplus \mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$	$\boldsymbol{\xi_\alpha}$	$\boldsymbol{\xi_\alpha}$
$\mathbf{1}$	$\mathbf{1}$	$\boldsymbol{\tau}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$	$\boldsymbol{\xi_\alpha}$	$\boldsymbol{\xi_\alpha} \oplus \mathbf{1}$

Table 1: Truth table of $F_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$

Theorem 2: *If $f(\boldsymbol{x})$ is a bent function with n variables, and we consider a nonzero $\boldsymbol{\lambda} \in B^n$, then*

$$\begin{aligned} G(\boldsymbol{y},\boldsymbol{x}) = & \left(m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y})\right) f(\boldsymbol{x}) \\ & \oplus m_{i_2}(\boldsymbol{y}) f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ & \oplus m_{i_3}(\boldsymbol{y}) \left(1 \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x})\right) \end{aligned}$$

is a bent function with $n+2$ variables.

PROOF: As in Theorem 1, considerer a nonzero $(\boldsymbol{\beta},\boldsymbol{\alpha}) \in B^2 \times B^n$ and let

$$\begin{aligned} G_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x}) &= G(\boldsymbol{y},\boldsymbol{x}) \oplus G((\boldsymbol{\beta},\boldsymbol{\alpha}) \oplus (\boldsymbol{y},\boldsymbol{x})) \\ &= \left(m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y})\right) f(\boldsymbol{x}) \\ &\quad \oplus \left(m_{i_2}(\boldsymbol{y}) \oplus m_{i_3}(\boldsymbol{y})\right) f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ &\quad \oplus \left(m_{i_0 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \oplus m_{i_1 \oplus \boldsymbol{\beta}}(\boldsymbol{y})\right) f(\boldsymbol{\alpha} \oplus \boldsymbol{x}) \\ &\quad \oplus \left(m_{i_2 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \oplus m_{i_3 \oplus \boldsymbol{\beta}}(\boldsymbol{y})\right) f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ &\quad \oplus m_{i_3}(\boldsymbol{y}) \oplus m_{i_3 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \end{aligned}$$

- Assume that $\boldsymbol{\alpha} = \mathbf{0}_n$ and $\boldsymbol{\beta} \neq \mathbf{0}_2$. Then,

  $$\begin{aligned} & G_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x}) \\ & = \left(\bigoplus_{t=0}^{1} m_{i_t}(\boldsymbol{y}) \oplus m_{i_t \oplus \boldsymbol{\beta}}(\boldsymbol{y})\right) f(\boldsymbol{x}) \\ & \oplus \left(\bigoplus_{t=2}^{3} m_{i_t}(\boldsymbol{y}) \oplus m_{i_t \oplus \boldsymbol{\beta}}(\boldsymbol{y})\right) f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ & \oplus m_{i_3}(\boldsymbol{y}) \oplus m_{i_3 \oplus \boldsymbol{\beta}}(\boldsymbol{y}) \end{aligned}$$

  and taking into account that

  $$\begin{aligned} & (i_0 \oplus \boldsymbol{\beta}, i_1 \oplus \boldsymbol{\beta}, i_2 \oplus \boldsymbol{\beta}, i_3 \oplus \boldsymbol{\beta}) \\ & = \begin{cases} (i_1, i_0, i_3, i_2) & \text{if } \boldsymbol{\beta} = 1 \\ (i_2, i_3, i_0, i_1) & \text{if } \boldsymbol{\beta} = 2 \\ (i_3, i_2, i_1, i_0) & \text{if } \boldsymbol{\beta} = 3 \end{cases} \end{aligned}$$

  we can consider the following cases:

  - If $\boldsymbol{\beta} = 1$, then

    $$G_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x}) = m_{i_3}(\boldsymbol{y}) \oplus m_{i_2}(\boldsymbol{y})$$

    which is balanced, because its truth table has four blocs

    $$\mathbf{0} \quad \mathbf{0} \quad \mathbf{1} \quad \mathbf{1}$$

    not necessarily in that order, each one of length 2^n.

  - If $\boldsymbol{\beta} = 2$, in a similar way we have that

    $$\begin{aligned} G_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x}) = & f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \\ & \oplus m_{i_1}(\boldsymbol{y}) \oplus m_{i_3}(\boldsymbol{y}) \end{aligned}$$

    whose truth table has four blocs

    $$\boldsymbol{\xi_\lambda} \quad \boldsymbol{\xi_\lambda} \quad \boldsymbol{\xi_\lambda} \oplus \mathbf{1} \quad \boldsymbol{\xi_\lambda} \oplus \mathbf{1}$$

    This truth table is balanced because $\boldsymbol{\xi_\lambda}$, the truth table of $f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x})$, is balanced.

  - The case $\boldsymbol{\beta} = 3$ is analogous to the case $\boldsymbol{\beta} = 2$.

- Assume that $\boldsymbol{\alpha} \neq \mathbf{0}_n$ and $\boldsymbol{\beta} = \mathbf{0}_2$. Then,

  $$\begin{aligned} & G_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x}) \\ & = \left(m_{i_0}(\boldsymbol{y}) \oplus m_{i_1}(\boldsymbol{y})\right) \left(f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x})\right) \\ & \quad \oplus \left(m_{i_2}(\boldsymbol{y}) \oplus m_{i_3}(\boldsymbol{y})\right) \left(f(\boldsymbol{\lambda} \oplus \boldsymbol{x})\right. \\ & \quad \left. \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})\right). \end{aligned}$$

  So, the truth table of this function has four blocs

  $$\boldsymbol{\xi}_1 \quad \boldsymbol{\xi}_1 \quad \boldsymbol{\xi}_2 \quad \boldsymbol{\xi}_2$$

  where $\boldsymbol{\xi}_1$ and $\boldsymbol{\xi}_2$ are the truth tables of $f(\boldsymbol{x}) \oplus f(\boldsymbol{\lambda} \oplus \boldsymbol{x})$ and $f(\boldsymbol{\lambda} \oplus \boldsymbol{x}) \oplus f(\boldsymbol{\alpha} \oplus \boldsymbol{\lambda} \oplus \boldsymbol{x})$ respectively. Now, since $\boldsymbol{\xi}_1$ and $\boldsymbol{\xi}_2$ are balanced, because $f(\boldsymbol{x})$ and $f(\boldsymbol{\lambda} \oplus \boldsymbol{x})$ are bent functions, we can ensure that the above truth table is also balanced.

- Assume that $\boldsymbol{\alpha} \neq \mathbf{0}_n$ and $\boldsymbol{\beta} \neq \mathbf{0}_2$. By proceeding as in the first part, we obtain that the truth table of $G_{(1,\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$ has four blocs

  $$\boldsymbol{\xi}_1 \quad \boldsymbol{\xi}_1 \quad \boldsymbol{\xi}_2 \oplus \mathbf{1} \quad \boldsymbol{\xi}_2 \oplus \mathbf{1}$$

  not necessarily in that order; so, it is a balanced sequence.

  Similarly for $G_{(2,\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$ and $G_{(3,\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$.

So, the function $G_{(\boldsymbol{\beta},\boldsymbol{\alpha})}(\boldsymbol{y},\boldsymbol{x})$ is balanced and, consequently, $G(\boldsymbol{y},\boldsymbol{x})$ is a bent function. ■

For a given bent function $f(\boldsymbol{x})$ in n variables, we can construct, according with Theorem 2, $(4!/2!)(2^n-1) = 12(2^n-1)$ different bent functions in $n+2$ variables.

4 Conclusion

We have presented two methods to obtain iteratively new bent functions of $n+2$ variables from bent functions of n variables. These methods are based in the expression of Boolean functions as sum of minterms. With these methods we can construct, starting with a bent function of n variables, $4+12(2^n-1)$ bent functions. So, taking into account that if F is a bent function, then $F \oplus 1$ is also a bent functions, really we have $8+24(2^n-1)$ bent functions. The results of this paper are valuable in both theory and practical applications.

References:

[1] C. M. Adams and S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, 35(5):1170–1173, 1990.

[2] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology – CRYPTO '90*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer-Verlag, Berlin, 1991.

[3] Y. Borissov, A. Braeken, S. Nikova, and B. Preneel. On the covering radii of binary reed-muller codes in the set of resilient boolean functions. *IEEE Transactions on Information Theory*, 51(3):1182–1189, 2005.

[4] A. Braeken, V. Nikov, S. Nikova, and B. Preneel. On Boolean functions with generalized cryptographic properties. In Anne Canteaut and Kapaleeswaran Viswanathan, editors, *Progress in Cryptology – INDOCRYPT 2004*, volume 3348 of *Lecture Notes in Computer Science*, pages 120–135. Springer-Verlag, Berlin, 2004.

[5] C. Charnes and T. Yu. Covering sequences of boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, 25:263–279, 2002.

[6] P. V. Kumar and R. A. Scholtz. Bounds on the linear span of bent sequences. *IEEE Transactions on Information Theory*, 29(6):854–862, 1983.

[7] K. Kurosawa, T. Iwata, and T. Yoshiwara. New covering radius of reed-muller codes for t-resilient functions. *IEEE Transactions on Information Theory*, 50(3):468–475, 2004.

[8] A. Lempel and M. Cohn. Maximal families of bent sequences. *IEEE Transactions on Information Theory*, 28(6):865–868, 1982.

[9] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 6 edition, 1988.

[10] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, Berlin, 1994.

[11] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In J.J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology – EUROCRYPT'89*, volume 434 of *Lecture Notes in Computer Science*, pages 549–562. Springer-Verlag, Berlin, 1998.

[12] S. Murphy and M. J. B. Robshow. Key-dependent s-boxes and differential cryptanalysis. *Designs, Codes and Cryptography*, 27:229–255, 2002.

[13] J. D. Olsen, R. A. Scholtz, and L. R. Welch. Bent-function sequences. *IEEE Transactions on Information Theory*, 28(6):858–864, 1982.

[14] K. Ren, J. Park, and K. Kim. On the construction of cryptographycally strong boolean functions with desirable trade-off. *Journal of Zhejiang University SCIENCE*, 6A(5):358–364, 2005.

[15] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, 20:300–305, 1976.

[16] P. Sarkar and S. Maitra. Construction of nonlinear boolean functions with important cryptographyc properties. In B. Prenee, editor, *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 485–506. Springer-Verlag, Berlin, 2000.

[17] P. Sarkar and S. Maitra. Efficient implementation of cryptographically useful "large" boolean functions. *IEEE Transactions on Computers*, 52(4):410–417, 2003.

[18] J. Seberry, X.-M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119:1–13, 1995.