FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 31, N° 2, June 2018, pp. 207 - 222
https://doi.org/10.2298/FUEE1802207R

CONSTRUCTION OF SUBSETS OF BENT FUNCTIONS SATISFYING RESTRICTIONS IN THE REED-MULLER DOMAIN*

Miloš Radmanović, Radomir S. Stanković

Faculty of Electronic Engineering, University of Niš, Niš, Serbia

Abstract. *Bent functions are Boolean functions with highest nonlinearity which makes them interesting for cryptography. Determination of bent functions is an importantbut hard problem, since the general structure of bent functions is still unknown. Various constructions methods for bent functions are based on certain deterministic procedures, which might result in some regularitythat is a feature undesired for applications in cryptography. Random generation of bent functions is an alternative, however, the search space is very large and the related procedures are time consuming. A solution is to restrict the search space by imposing some conditions that should be satisfied by the produced bent functions. In this paper, we propose three ways of imposing such restrictions to construct subsets of Boolean functions within which the bent functions are searched. We estimate experimentally the number of bent functions in the corresponding subsets of Boolean functions.*

Key words: *Cryptography, Boolean functions, Bent, Reed-Muller domain, Subsets.*

1 Introduction

Bent functions are by definition the most nonlinear Boolean functions, i.e., at the maximum distance of $2^{n-1}-2^{n/2-1}$, n-number of variables, from affine functions. Due to that property, bent functions are useful for cryptographic purposes, such as block ciphers, stream ciphers, and hash functions in many areas [1], [2]. They have been attracted a lot of attention in cryptography, but have also studied in many other areas such as combinatorics, coding theory, logic synthesis, and signal processing [3], [4]. The problem is that they are not balanced. Therefore, constructing bent functions followed by a procedure to make them balanced is in foundations of many cryptographic procedures.

Received October 21, 2017; received in revised form January 31, 2018
Corresponding author: Miloš Radmanović
Faculty of Electronic Engineering, University of Niš, Medevedeva 14, 18000 Niš, Serbia
(E-mail: milos.radmanovic@elfak.ni.ac.rs)
*An earlier version of this paper was presented as an invited address at the Reed-Muller 2017 Workshop, Novi Sad, Serbia, May 24-25, 2017

There are many procedures to construct bent functions, but most of them are exhaustive in the sense that can produce all bent functions for a given n. Another problem is that being based on some deterministic procedures, there is a no negligible possibility that the produced bent function might express some degree of regularity. Random generation of bent functions is often used as an alternative. The problem is however that the number of bent functions is very small compared to the total number of 2^{2n} Boolean functions. Expressed in percentages, it is $1,36\%$, $2,94\times10^{-8}\%$, and $8,57\times10^{-44}\%$ for $n=4,6,8$, out of 65.536, 18.446.744.073.709.551.616, and $1,157920892373161954235709850086 9\times10^{+77}$ functions.

Therefore, random finding of bent functions necessarily requires reduction of the search space by using properties of bent functions. In this paper, we explore how large is the number of bent functions in certain restricted subsets of Boolean functions with restrictions derived from properties of bent functions. The aim is to provide specifications how to restrict the search space for bent functions according to the probability of finding them in predefined subsets of Boolean functions. The restrictions are formulated in the Reed-Muller (RM) domain [5].

This paper is organized as follows: Section 2 shortly introduces the theoretical background and necessary concepts to be discussed. In Section 3, three approaches to the restriction of the search space in finding bent functions in RM domain are presented. The experimental results are shown and discussed in Section 4. The closing Section 5 summarizes the results of the research reported in this paper.

2 Background Theory

2.1 Reed-Muller Transform

The algebraic normal form (ANF) is one of the most used representations in cryptography. Every Boolean function has a unique representation in the ANF as the binary coefficient vector, known as the positive polarity Reed-Muller spectrum. Therefore in switching theory, logic design, signal processing and related areas, the ANF is also called positive polarity Reed-Muller normal form.

Any Boolean function of n variables can be expressed in the positive polarity Reed-Muller form or algebraic normal form as [6]:

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{i=1} s_i \phi_i, \tag{1}$$

where,

$$\phi_i = \prod_{k=0}^{n-1} (x_k)^{i_k}, \tag{2}$$

where x_k is a variable that may assume either 0 or 1. The values $s_i \in \{0, 1\}$, also known as the RM spectral coefficients, short RM-coefficients, determine whether a product term is present or not in (1). In addition, coordinates $i_k \in \{0, 1\}$ in binary representation of i indicate the presence or absence of a variable x_k in the product term ϕ_i, $(x_k^1 = x_k, x_k^0 = 1)$. The symbol $\oplus$ denotes the EXOR operation, and multiplication is assumed to be the AND operation.

The algebraic degree or the order of nonlinearity of f is the maximum number of variables in a product term related with a non-zero coefficient s_i. The positive polarity RM coefficients are divided into groups according to the number of ones in the binary representation of their indices. For example, coefficients of the first order are $s_1, s_2, s_4, s_8 \ldots$. Coefficients of the second order are assigned to product terms consisting of two variables. The third order coefficients correspond to product of three variables and so forth, until the coefficient of order n related to the last product term $x_1 x_2 \ldots x_n$.

Definition 1 *In matrix notation, if a function f and its RM spectrum S_f are represented by vectors $F = [f_0, f_1, \ldots, f_{2^n-1}]^T$ and $S_f = [s_0, s_1, \ldots, s_{2^n-1}]^T$ respectively, the positive polarity RM transform is defined by the positive polarity RM matrix $RM(n)$ [6]:*

$$S_f = R(n)F, \tag{3}$$

where,

$$R(n) = \bigotimes_{i=1}^{n} R(1), \tag{4}$$

and

$$R(1) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{5}$$

is the basic positive Reed-Muller transform matrix. Note that $RM(1)$ and, therefore, also $RM(n)$ is a self-inverse matrix.

The Kornecker product used in (4) determines the so-called Hadamard order of the RM-coefficients which will be used in the following considerations. When the order of coefficients is specified, then the position of each coefficient in the RM-spectrum is uniquely determined. This property will be used to define restrictions reducing the search space for bent functions.

Definition 2 *The function f is reconstructed from its RM spectrum as:*

$$f(x_1, x_2, \ldots, x_n) = X(n)S_f, \tag{6}$$

where

$$X(n) = \bigotimes_{i=1}^{n} \left[\begin{array}{cc} 1 & x_i \end{array} \right]. \tag{7}$$

2.2 Walsh transform

Definition 3 *For a Boolean function f in $(1, -1)$ encoding defined by the truth-vector $F = [f_0, f_1, \ldots, f_{2^n-1}]^T$, the Walsh spectrum $S_{f,W} = [r_0, r_1, \ldots, r_{2^n-1}]^T$ is defined as [?]:*

$$S_{f,W} = W(n)F, \tag{8}$$

where,

$$W(n) = \bigotimes_{i=1}^{n} W(1), \tag{9}$$

where,

$$W(1) = \left[\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array} \right] \tag{10}$$

is the basic Walsh transform matrix.

2.3 Bent functions

For the case of even number of variables, there is a class of Boolean functions introduced by O. Rothaus achieving maximum nonlinearity, the so-called bent functions, figurative meaning is opposite to linear. The exact number of n-variable bent functions is known only for small number of variables, for $n < 10$. The general number of bent functions is an open problem and it is known the upper bounds in respect to n. The following theorems and definition determine some basic properties of bent functions that will be used in the present considerations.

Theorem 1 *[3] There are defined some "naive" lower and upper bounds on the number of bent functions. The lower bound is* $(2^{n/2})!2^{2^{n/2}}$*, and upper bound is* $2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$.

Note that, the number of bent functions increases rapidly due to exponential increasing of lower bound.

Theorem 2 *[2] If* f *is a bent function,* $\overline{f}$ *is also bent.*

Theorem 3 *[1] Every bent function has a Hamming weight (number of ones in the truth vector) of* $2^{n-1} \pm 2^{n/2-1}$.

The following definition of a bent function is formulated in terms of the Walsh transform coefficients:

Definition 4 *[4] A Boolean function* $f(x_1, x_2, \ldots, x_n)$ *in* $(1, -1)$ *encoding is called bent if all Walsh coefficients in vector* $S_{f,W}$ *have the same absolute value* $2^{n/2}$.

Theorem 4 *[4] The algebraic degree of bent functions* $f(x_1, x_2, \ldots, x_n)$ *is at most* $n/2$ *for* $n > 2$.

Positions of the non-zero RM coefficients in the S_f of a bent function are related with the order of coefficients. For example, the bent functions of four variables can have non-zero RM coefficients of order 0,1,2 and the number of ones in the binary representation of their vector index is ≤ 2.

In relation to that, the maximal number of non-zero coefficients in the RM spectrum of bent functions is:

$$\sum_{i=0}^{n/2} \binom{n}{i} = 2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}. \tag{11}$$

These both features will be used in the present paper.

Example 1 *Consider for a bent function of four variables* $f(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4$*, given by* $F = [0,0,0,1,0,0,0,1,0,0,0,1,1,1,1,0]^T$*. The RM spectrum is* $S_f = [0,0,0,1,0,0,0,0,0,0,0,0,1,0,0,0]^T$*, from where the number of non-zero RM coefficients is* 2 *and algebraic degree is* $2 \leq 4/2$*. The Walsh spectrum with* $(1, -1)$ *encoding is* $S_{f,W} = [4,4,4,-4,4,4,4,-4,4,4,4,$ $-4,-4,-4,-4,4]^T$*, where all coefficients have the same absolute value* $2^2 = 4$.

2.4 Construction of bent functions

Finding the complete set of bent functions for a given number of inputs is an open problem. There are no formal methods for generalization, construction, or classification of all bent functions for a given number of inputs. Thus, it has been developed a variety of approaches for construction and classification of bent functions with particular properties [2]. However, bent functions that have some predefined specific properties are very rare and they constitute a rather small subset of the total of all bent functions. Therefore, it is important to define different approaches for determination of bent functions.

Different classes of bent functions are focused on bent functions satisfying certain additional conditions. For example, quadratic bent functions have an important place in bent function construction. All bent functions from this class are known and they can be obtained by applying the affine transformations to the variables of the function [7].

Two most known approaches for construction classification of bent functions are based on a combinatorial construction and an algebraic construction of functions [2]. The well-known combinatorial constructions are Maiorana-McFarland [8], partial spreads [9], Dobbertin [10], iterative constructions [11], minterm constructions [12], Maiorana-McFarland super class [13], etc. The most widely known algebraic constructions are monomial bent functions in the Kasami, Gold, Dillon and Canteaut-Leander case [14], hyper bent functions [15], Niho bent functions [16], etc.

3 Subsets of Bent Functions in the RM Domain

In this paper, we propose to split the set of all Boolean functions with respect to three different criteria related to the properties of RM-spectra of bent functions:

1. The number of non-zero RM-coefficients. We call it the vertical subset.
2. The orders of nonlinearity defined as the maximum number of variables in a product term corresponding to a non-zero RM-coefficient. We call it the horizontal subset.
3. Both, the number of non-zero RM-coefficients and the order of nonlinearity. We call it the grid subset.

The main objective is to investigate the number of bent functions in each of these subsets. In order to study the proposed subsets of functions in the spectral RM domain, we developed in C++ three independent implementations of the algorithms for vertical, horizontal, and grid RM subset classifications. These implementations are used to investigate considered subsets of bent functions with 4, 6, and 8 variables.

3.1 Vertical subset

Since the order of nonlinearity of n-variable bent functions is less or equal to $n/2$, in their RM-spectra there cannot be non-zero RM-coefficients assigned to product terms with more than $n/2$ variables. The values of coefficients of larger order are 0. Therefore, the number of possible non-zero coefficients is smaller than 2^n.

Functions that do not satisfy this requirement can be eliminated from checking for bentness. In this way, the search space for bent functions is considerably reduced which permits for finding bent functions in a reasonably short time.

Since the RM-expression for a bent function cannot contain product terms with more than $n/2$ variables, the maximal number of non-zero coefficients of k-th order is $\binom{n}{k}$, $k = 0, 1, \ldots, n/2$. Therefore, the total number of non-zero coefficients in the RM spectrum of bent functions is: $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n/2} = 2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}$.

Vertical (V) subset consists of n-variable Boolean functions with no more than $2^{n-1} + \frac{1}{2}\binom{n}{\frac{n}{2}}$ RM-coefficients.

Definition 5 *A bent function belongs to the Vertical k-subset $V(k)$ iff it has k non-zero RM-coefficients.*

Clearly, the number of possible V subsets depends of the number of variables.

Example 2 *The maximal number of non-zero spectral RM coefficients of bent functions with 4 variables is 11 out of 16 coefficients. Hence, there are 11 possible V subsets for bent function with 4 variables. The $V(1)$ subset is the subset of bent functions having the RM spectrum with 1 non-zero RM coefficient, the $V(2)$ subset is the subset having 2 non-zero RM coefficients, and etc.*

There are 42 possible V subsets for bent functions with 6 variables, and 163 possible V subsets for bent functions with 8 variables.

Example 3 *Two bent functions of 4 variables* $f_1(x_1, x_2, x_3, x_4) = 1 \oplus x_1x_2 \oplus x_3x_4$, *and* $f_2(x_1, x_2, x_3, x_4) = x_4 \oplus x_1x_2 \oplus x_3x_4$ *have 3 non-zero RM-coefficients and belong to the same subset* $V(3)$.

3.2 Horizontal subset

In definition of this subset, we take into account the order of the RM coefficients.

If we fix the order of RM coefficients, then we know the positions of coefficients that have to be 0 in the RM spectrum of a bent function, due to this restriction related to the order of nonlinearity. All other coefficients can be either 0 or 1.

As noticed above, in this paper, we use the so-called Hadamard ordering of RM coefficients originating in the Kronecker product structure of the Reed-Muller matrix in (4). In this ordering, for a given n, we can determine positions of coefficients which cannot be 1 by referring to (7).

Example 4 *For a bent function of four variables, the RM spectrum can be represented by* $S_f = [-, -, -, -, -, -, -, \times, -, -, -, \times, -, \times, \times, \times]^T$, *where the possible positions of the non-zero coefficients are denoted by dash lines and the restricted positions are denoted with* $\times$.

Definition 6 *A bent function belongs to the Horizontal* (k_{min}, k_{max})*-subset* $H(k_{min}, k_{max})$ *iff it has the minimum* k_{min} *and the maximum* k_{max} *order of RM coefficients.*

H subsets involve the application of ranges of possible non-zero RM spectrum coefficients orders. The number of H subsets also depends of the number of variables of the bent functions.

Example 5 *The maximal order of non-zero spectral coefficients of bent functions with 4 variables is 2. Hence, there are 3 possible* H *subsets* $H(0, 2)$, $H(1, 2)$, *and* $H(2, 2)$. *There are* H *subsets* $H(0, 0)$, $H(0, 1)$, *and* $H(1, 1)$, *that do not contain any of the bent functions.*

Example 6 *For bent functions with 6 variables, there are 10 possible H subsets:* $H(0,0)$, $H(0,1)$, $H(0,2)$, $H(0,3)$, $H(1,1)$, $H(1,2)$, $H(1,3)$, $H(2,2)$, $H(2,3)$, *and* $H(3,3)$. *Some of subsets also do not contain any of the bent functions.*

Example 7 *Two bent functions of 4 variables* $f_1(x_1,x_2,x_3,x_4) = x_1x_2 \oplus x_2x_4 \oplus x_3x_4$, *and* $f_2(x_1,x_2,x_3,x_4) = x_1x_3 \oplus x_2x_4$ *have only second order non-zero RM-coefficients and belong to the same subset* $H(2,2)$.

3.3 Grid subset

In definition of this subset, we take into account both, the orders and the number of the coefficients.

Definition 7 *A bent function belongs to the Grid* (k, k_{min}, k_{max}) *- subset* $G(k, k_{min}, k_{max})$ *iff it has k non-zero RM-coefficients and minimum order of RM coefficients* k_{min} *and maximum order* k_{max}.

The G subsets of bent functions are the intersection of V and H subsets. Number of G subsets also depends of the number of variables of the bent functions. For example, there are many G subsets for bent functions with 4 variables: $V(1,0,0)$, $H(1,0,1)$, ..., $H(6,2,2)$. There are also many subsets that do not contain any of the bent functions.

Example 8 *Two bent functions of 4 variables* $f_1(x_1,x_2,x_3,x_4) = x_1x_2 \oplus x_3x_4$, *and* $f_2(x_1,x_2,x_3,x_4) = x_1x_3 \oplus x_2x_4$ *have only 2 and second order non-zero RM-coefficients and belong to the same subset* $G(2,2,2)$.

It should be noticed that there are bent functions that do not belongs to any of G subsets.

4 Experimental Results

In this section, we made enumeration of bent functions in some vertical, horizontal and grid subsets for functions with 4, 6, and 8 variables.

There are two types of methods for enumerations of bent functions, primary and secondary. The primary methods are based on the direct enumeration in the Boolean domain. The secondary methods are based on

enumeration in the Reed-Muller domain. The most known secondary methods use property that all bent functions of n variables have algebraic degree at most $n/2$ [17]. The secondary method for complete enumeration of bent functions of 8 variables has been used approximately 50 PCs running for 3 months [18]. It is known that, there are 8 bent functions in two variables, 896 bent functions in four variables, 5.425.430.528 bent functions in 6 variables, and 99.270.589.265.934.370.305.785.861.242.880 bent functions in 8 variables [2].

The efficiency of using parallel multi-core CPU technique for random generation of bent function in the RM domain is analyzed in [19]. To improve execution performance, the algorithm for efficient parallel generation of bent function in the RM domain using GPU platform have been defined in [20].

For experimental purposes, we developed a C++ implementations of the algorithm for creating subsets of bent functions in the RM domain. The algorithm for creation of subsets in RM domain is similar to the techniques for hardware enumeration of bent functions [21] and generation of bent function in the RM domain [19], except that the search space of further reduced. Note that, for some functions of 6 and 8 variables, experiments were not shown, since the computation time was limited to 30 minutes.

Table 1 shows the number of bent functions in the subsets $V(k)$ for $n = 4$ variables. There exists no bent function that can be represented by a single product term. Note that majority of the bent functions requires 4 to 7 coefficients. Precisely, more that 756 of the total of 896 bent functions for $n = 4$ require 4 to 7 non-zero coefficients. This makes $84,375\%$ of the total of bent functions. From data in Table 1, it can be seen that vertical subsets $V(5)$ and $V(6)$ contain more than a half of the total number of bent functions. Note that vertical subsets $V(2)$, $V(10)$, and $V(11)$ contain small number of the bent functions.

Table 2 shows the number of bent functions in the most of RM vertical subsets for functions with 6 variables. From data in Table 2, it can be seen again that central vertical subsets contains large number of the bent functions. For example, the RM vertical subsets $V(18)$ and $V(19)$ contain about 20% of the bent functions. Again, note that vertical subsets $V(3)$, $V(4)$, $V(36)$ and $V(37)$ contain small number of the bent functions. The numbers of bent functions for the subsets from $V(20)$ to $V(27)$ are not included due to very long computation time.

Table 3 shows the number of bent functions with 4 and 5 non-zero RM coefficients for functions with 8 variables. It is again confirmed that vertical subsets with small and large number of coefficients do not contain many bent

Table 1: The number of bent functions in the subsets $V(k)$ for $n = 4$ variables

k	$\#f$ of $V(k)$
2	3
3	27
4	102
5	210
6	256
7	188
8	82
9	22
10	5
11	1

functions. For example, experiments show that there are no bent functions with 1,2, and 3 as well as with 157, 158, 159, 160, 161, 162, and 163 non-zero RM-coefficients. Note that the number of "empty" vertical subsets with small number of coefficients is linearly increases in the number of variables of bent functions. Moreover, "empty" vertical subsets with great number of coefficients exponentially increase in respect to number of variables of bent functions.

Table 4 shows the number of bent functions in some RM horizontal subsets for functions with 4, 6, and 8 variables. It is evident that subsets with only third order non-zero RM coefficients contain very small number of bent functions.

Table 5, 6, and 7 shows the number of bent functions in some RM grid subsets for functions with 4, 6, and 8 variables, respectively. It is evident that subsets with only second order non-zero RM coefficients contain large number of functions, especially in central grid subsets with respect to the total number of coefficients of only second order. It is interesting that there are only two non-"empty" grid subsets for functions with 6 variables with only third order non-zero RM coefficients. It is evident that most of bent functions are with mixture of first, second, and third order of non-zero RM coefficients. Experiments with mixture of different orders of coefficients are not included in this paper.

Table 2: The number of bent functions in the subsets $V(k)$ for $n = 6$ variables

k	$\#f$ of $V(k)$
3	15
4	405
5	4575
6	30885
7	147630
8	548190
9	1657950
10	4239474
11	9512343
12	19341969
13	36536505
14	65365185
15	112296016
16	185615422
17	290719416
18	420742250
19	551175695
28	57338355
29	25754775
30	9869427
31	3098124
32	770562
33	153060
34	26070
35	3882
36	504
37	72

Table 3: The number of bent functions in the subsets $V(k)$ for $n = 8$ variables

k	$\#f$ of $V(k)$
4	105
5	8505

Table 4: The number of bent functions in some subsets $H(k_{min}, k_{max})$ for n =4,6, and, 8 variables

n	k_{min}, k_{max}	$\#f$ of $H(k_{min}, k_{max})$
4	2,2	24
6	2,2	13440
6	3,3	12
8	2,2	111992832

Table 5: The number of bent functions in some subsets $G(k, k_{min}, k_{max})$ for $n = 4$ variables

k, k_{min}, k_{max}	$\#f$ of $G(k, k_{min}, k_{max})$
2,2,2	2
3,2,2	8
4,2,2	10
5,2,2	4

Table 6: The number of bent functions in some subsets $G(k, k_{min}, k_{max})$ for $n = 6$ variables

k, k_{min}, k_{max}	$\#f$ of $G(k, k_{min}, k_{max})$
3,2,2	12
4,2,2	144
5,2,2	732
6,2,2	1968
7,2,2	3008
8,2,2	3040
9,2,2	2360
10,2,2	1384
11,2,2	564
12,2,2	176
13,2,2	44
14,2,2	8
16,3,3	6
17,3,3	6

5 Conclusion

For practical cryptographic applications, it is often necessary to generate random bent functions. The runtime of an exhaustive search method for generation of bent function is exponential in terms of the number of variables. In this paper, we propose an approach to the restriction of the search space based on the restriction of the number and order of RM-coefficients for bent functions.

Table 7: The number of bent functions in some subsets $G(k, k_{min}, k_{max})$ for $n = 8$ variables

k, k_{min}, k_{max}	$\#f$ of $G(k, k_{min}, k_{max})$
2,2,2	2
3,2,2	8
4,2,2	90
5,2,2	2160
6,2,2	23850
7,2,2	157860
8,2,2	687030
9,2,2	2081400
10,2,2	4753710
11,2,2	8640684
12,2,2	12897908
13,2,2	16181264
14,2,2	17405460
15,2,2	16291480
16,2,2	13230940
17,2,2	9215136
18,2,2	5554956
19,2,2	2907720
20,2,2	1277010
21,2,2	476288
22,2,2	157730
23,2,2	41412
24,2,2	7630
25,2,2	1000
26,2,2	102
27,2,2	12

Using properties of bent function in RM domain, we define RM vertical, horizontal, and grid subsets of Boolean functions that might contain bent functions. The proposed approach is experimentally verified through enumeration of bent functions in some RM vertical, horizontal, and grid subsets for functions with 4, 6, and 8 variables. Experimental results showed some interesting properties of different subsets in the spectral Reed-Muller domain. It is shown that some vertical, horizontal and grid subsets contain large and small number of the bent functions, or they are "empty". This information can be helpful in designing search method for generation of bent function.

It can be concluded from these experimental results that besides the Walsh and the Reed-Muller domain, exploring bent functions in some other representation domains can be interesting.

References

[1] S. Mesnager, *Bent Functions: Fundamentals and Results*. Springer International Publishing, 2016.

[2] N. Tokareva, *Bent Functions, Results and Applications to Cryptography*. Academic Press, 2015.

[3] T. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications (Second edition)*. Academic Press, 2017.

[4] T. Sasao and J. T. Butler, *Boolean functions for cryptography*. Morgan and Claypool Publishers, 2010.

[5] M. Thornton, R. Drechsler, and D. Miller, *Spectral Techniques in VLSI CAD*. Springer US, 2012.

[6] M. G. Karpovsky, R. S. Stanković, and J. T. Astola, *Spectral Logic and Its Applications for the Design of Digital Devices*. Wiley, 2008.

[7] C. Carlet and P. Guillot, *Bent, resilient functions and the numerical normal form*. American Mathematical Society, 2001, vol. 56.

[8] R. McFarland, "A family of noncyclic difference sets," *Journal of Combinatorial Theory*, vol. 15A, pp. 541–542, 1965.

[9] J. F. Dillon, "Elementary hadamard difference sets," Ph.D. dissertation, University of Maryland, 1974.

[10] H. Dobbertin, *Construction of bent functions and balanced Boolean functions with high nonlinearity*, ser. Lecture Notes in Computer Science, B. Preneel, Ed. Springer, Berlin, Germany, 1995, vol. 1008.

[11] J. Climent, F. Garcia, and V. Requena, "On the iterative construction of bent functions," in *Proc. of the 5th WSEAS Int. Conf. on Inf. Security and Privacy (ISP06)*, N. Mastorakis and A. Cecchi, Eds. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2006, pp. 15–18.

[12] J. Climent, F. Garca, and V. Requena, "On the construction of bent functions of n+2 variables from bent functions of n variables," *Advances in Mathematics of Communications*, vol. 2, pp. 421–431, 2008.

[13] C. Carlet, *A larger class of cryptographic Boolean functions via a study of the MaioranaMcFarland construction*, ser. Lecture Notes in Computer Science, B. Preneel, Ed. Springer, 2002, vol. 2442.

[14] P. Langevin and G. Leander, "Monomial bent functions and stickelberger's theorem," *Finite Fields and Their Applications*, vol. 14, no. 3, pp. 727–742, 2008.

[15] A. M. Youssef and G. Gong, *Hyper-bent functions*, ser. Lecture Notes in Computer Science, B. Preneel, Ed. Springer, 2001, vol. 2045.

[16] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, "Construction of bent functions via niho power functions," *Journal of Combinatorial Theory*, vol. 113, no. 5, pp. 779–798, 2006.

[17] J. L. Shafer, S. W. Schneider, J. T. Butler, and P. Stanica, "Enumeration of bent boolean functions by reconfigurable computer," in *Proc. of 18th IEEE Annual Int. Symposium on Field-Programmable Custom Computing Machines*, vol. 2, Charlotte, NC, USA, 2010, pp. 265–272.

[18] P. Langevin and G. Leander, "Counting all bent functions in dimension eight," *Designs, Codes and Cryptography*, vol. 59, pp. 193–201, 2011.

[19] M. Radmanović and R. S. Stanković, "Random generation of bent functions on multicore cpu platform," in *Proc. of 51st Int. Sci. Conf. on Inf., Communication and Energy Systems and Technologies (ICEST 2016)*, Ohrid, Macedonia, 2016, pp. 239–242.

[20] M. Radmanović, "Efficient random generation of bent functions using gpu platform," in *Proc. 12th Int. Workshop on Boolean Problems (IWSBP2016)*, Freiberg, Germany, 2016, pp. 167–173.

[21] S. W. Schneider and J. T. Butler, *Bent function enumeration by a circular pipeline implemented on FPGA*, B. Steinbach, Ed. Cambridge Scholars Publishing, 2017.