Boolean Functions with Large Distance to all Bijective Monomials: N odd case

Amr Youssef [1] and Guang Gong [2]

Center for Applied Cryptographic Research
[1]Department of Combinatorics & Optimization
[2]Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
{a2youssef,ggong}@cacr.math.uwaterloo.ca

Abstract. Cryptographic Boolean functions should have large distance to functions with simple algebraic description to avoid cryptanalytic attacks based on successive approximation of the round function such as the interpolation attack. Hyper-bent functions achieve the maximal minimum distance to all the coordinate functions of all bijective monomials. However, this class of functions exists only for functions with even number of inputs. In this paper we provide some constructions for Boolean functions with odd number of inputs that achieve large distance to all the coordinate functions of all bijective monomials.

Key words. Boolean functions, hyper-bent functions, extended Hadamard transform, Legendre sequences, nonlinearity.

1 Introduction

Several cryptanalytic attacks on block ciphers are based on approximating the round function (or S-box) with a simpler one. For example, linear cryptanalysis [13] is based on approximating the round function with an affine function. Another example is the interpolation attack [10] on block ciphers using simple algebraic functions as S-boxes and the extended attack in [11] on block ciphers with probabilistic nonlinear relation of low degree.

Thus, cryptographic functions used in the construction of the round function should have a large distance to functions with simple algebraic description. Along this line of research , Gong and Golomb [9] introduced a new S-box design criterion. By showing that many block ciphers can be viewed as a non linear feedback shift register with input, Gong and Golomb proposed that S-boxes should not be approximated by a bijective monomial. The reason is that, for $gcd(c, 2^N - 1) = 1$, the trace functions $Tr(\zeta x^c)$ and $Tr(\lambda x)$, $x \in GF(2^N)$, are both m-sequences with the same linear span.
For Boolean functions with even number of input variables, bent functions achieve the maximal minimum distance to the set of affine functions. In other

words, they achieve the maximal minimum distance to all the coordinate functions of affine monomials (i.e., functions in the form $Tr(\lambda x)+e)$). However, this doesn't guarantee that such bent functions cannot be approximated by the coordinate functions of bijective monomials (i.e., functions in the form $Tr(\lambda x^c)+e, gcd(c, 2^N-1)=1$). At Eurocrypt' 2001, Youssef and Gong [19] introduced a new class of bent functions which they called hyper-bent functions. Functions within this class achieve the maximal minimum distance to all the coordinate functions of all bijective monomials.

In this paper we provide some constructions for Boolean functions with odd number of inputs that achieve large distance to all the coordinate functions of all bijective monomials. Unlike the N even case, bounding the nonlinearity (NL) for functions with odd number of inputs, N, is still an open problem. For $N=1,3,5$ and 7, it is known that max $NL=2^{N-1}-2^{(N-1)/2}$. However, Patterson and Wiedemann [15], [16] showed that for $N=15$, $\max NL \geq 16276 = 16384-\frac{27}{32}2^{\frac{15-1}{2}}$. It should be noted that our task, i.e., finding functions with large distance to all the coordinate functions of all bijective monomials, is far more difficult than finding functions with large nonlinearity. For example, while the (experimental) average nonlinearity for functions with $N=11$ and 13 is about 941 and 3917 respectively, the (experimental) average minimum distance to the coordinate functions of all bijective monomials is about 916 and 3857 respectively.

We conclude this section with the notation and concepts which will be used throughout the paper.

- $\mathbb{F}=GF(2)$.
- $\mathbb{E}=GF(2^N)$.
- $Tr_M^N(x)$, $M|N$, represents the trace function from $\mathbb{F}_{2^N}$ to $\mathbb{F}_{2^M}$, i.e., $Tr_M^N(x)=x+x^q+\cdots+x^{q^{l-1}}$ where $q=2^M$ and $l=N/M$. If $M=1$ and the context is clear, we write it as $Tr(x)$.
- $\underline{\mathbf{a}}=\{a_i\}$, a binary sequence with period $s|2^N-1$. Sometimes, we also use a vector of dimension s to represent a sequence with period s. I.e., we also write $\underline{\mathbf{a}}=(a_0,a_1,\cdots,a_{s-1})$.
- $Per(\underline{\mathbf{b}})$, the period of a sequence $\underline{\mathbf{b}}$.
- $\underline{\mathbf{a}}^{(t)}$ denotes the sequence obtained by decimating the sequence $\underline{\mathbf{a}}$ by t,i.e., $\underline{\mathbf{a}}^{(t)}=\{a_{tj}\}_{j\geq 0}=a_0,a_t,a_{2t},\cdots$.
- $w(s)$: the number of 1's in one period of the sequence s or the number of 1's in the set of images of the function $s(x): GF(2^N)\rightarrow GF(2)$. This is the so-called *the Hamming weight* of s whether s is a periodic binary sequence or a function from $GF(2^N)$ to $GF(2)$.
- $\mathcal{S}$ denotes the set of all binary sequences with period $r|2^N-1$.
- $\mathcal{F}$ denotes the set of all (polynomial) functions from $GF(2^N)$ to $GF(2)$.

2 Preliminaries

The trace representation of any binary sequence with period dividing 2^N-1 is a polynomial function from $GF(2^N)$ to $GF(2)$. Any such polynomial function corresponds to a Boolean function in N variables. This leads to a connection among sequences, polynomial functions and Boolean functions. Using this connection, pseudo-random sequences are rich resources for constructing functions with good cryptographic properties.

Any non-zero function $f(x) \in \mathcal{F}$ can be represented as

$$f(x) = \sum_{i=1}^{s} Tr_1^{m_{t_i}}(\beta_i x^{t_i}), \beta_i \in GF(2^{m_{t_i}})^*, \qquad (1)$$

where $1 \leq s \leq |\Omega(2^N-1)|$, $\Omega(2^N-1)$ is the set of coset leaders modulo 2^N-1, t_i is a coset leader of a cyclotomic coset modulo 2^N-1, and $m_{t_i}|N$ is the size of the cyclotomic coset containing t_i. For any sequence $\underline{\mathbf{a}} = \{a_i\} \in \mathcal{S}$, there exists $f(x) \in \mathcal{F}$ such that

$$a_i = f(\alpha^i), i = 0, 1, \cdots,$$

where α is a primitive element of $\mathbb{E}$. $f(x)$ is called *the trace representation* of $\underline{\mathbf{a}}$. ($\underline{\mathbf{a}}$ is also referred to as an s-term sequence.) If $f(x)$ is any function from $\mathbb{E}$ to $\mathbb{F}$, by evaluating $f(\alpha^i)$, we get a sequence over $\mathbb{F}$ with period dividing 2^N-1. Thus

$$\delta : \underline{\mathbf{a}} \leftrightarrow f(x) \qquad (2)$$

is a one-to-one correspondence between $\mathcal{F}$ and $\mathcal{S}$ through the trace representation in (1). We say that $f(x)$ is the *trace representation* of $\underline{\mathbf{a}}$ and $\underline{\mathbf{a}}$ is the *evaluation* of $f(x)$ at α. In this paper, we also use the notation $\underline{\mathbf{a}} \leftrightarrow f(x)$ to represent the fact that $f(x)$ is the trace representation of $\underline{\mathbf{a}}$. The set consisting of the exponents that appear in the trace terms of $f(x)$ is said to be the *null spectrum set* of $f(x)$ or $\underline{\mathbf{a}}$.

If $s = 1$, i.e.,

$$a_i = Tr_1^N(\beta\alpha^i), i = 0, 1, \cdots, \beta \in \mathbb{E}^*,$$

then $\underline{\mathbf{a}}$ is an m-sequence over $\mathbb{F}$ of period 2^N-1 of degree N. (For a detailed treatment of the trace representation of sequences, see [14]).

3 Extended Transform Domain Analysis for Boolean Functions

The Hadamard transform of $f : \mathbb{E} \to \mathbb{F}$ is defined by [1]

$$\hat{f}(\lambda) = \sum_{x \in \mathbb{E}} (-1)^{f(x)+Tr(\lambda x)}, \lambda \in \mathbb{E}. \qquad (3)$$

The Hadamard transform spectrum of f exhibits the nonlinearity of f. More precisely, the nonlinearity of f is given by

$$NL(f) = 2^{N-1} - \frac{1}{2} \max_{\lambda \in \mathbb{E}} |\hat{f}(\lambda)|,$$

which indicates that the absolute value of $\hat{f}(\lambda)$ reflects the difference between agreements and disagreements of $f(x)$ and the linear function $Tr(\lambda x)$. Only bent functions [17] have a constant spectrum of their Hadamard transform. Gong and Golomb [9] showed that many block ciphers can be viewed as a non linear feedback shift register with input. In the analysis of shift register sequences [4], all m-sequences are equivalent under the decimation operation on elements in a sequence. The same idea can be used to approximate Boolean functions, i.e., we can use monomial functions instead of linear functions to approximate Boolean functions. Gong and Golomb [9] introduced the concept of extended Hadamard transform (*EHT*) for a function from $\mathbb{E}$ to $\mathbb{F}$. The extended Hadamard transform is defined as follows.

Definition 1. *Let f(x) be a function from $\mathbb{E}$ to $\mathbb{F}$. Let*

$$\hat{f}(\lambda, c) = \sum_{x \in \mathbb{E}} (-1)^{f(x)+Tr(\lambda x^c)} \tag{4}$$

where $\lambda \in \mathbb{E}$ and c is a coset leader modulo $2^N - 1$ co-prime to $2^N - 1$. Then we call $\hat{f}(\lambda, c)$ an extended Hadamard transform of the function f.

Notice that the Hadamard transform of f, defined by (3), is $\hat{f}(\lambda, 1)$. The numerical results in [9] show that, for all the coordinate functions $f_i, i = 1, \cdots, 32$ of the DES s-boxes, the distribution of $\hat{f}_i(\lambda, c)$ in λ is invariant for all c.

Thus a new generalized nonlinearity measure can be defined as

$$NLG(f) = 2^{N-1} - \frac{1}{2} \max_{\substack{\lambda \in \mathbb{E}, \\ c : gcd(c, 2^N - 1) = 1}} |\hat{f}(\lambda, c)|.$$

This leads to a new criterion for the design of Boolean functions used in conventional cryptosystems. The *EHT* of Boolean functions should not have any large component.

In what follows we will provide constructions for Boolean functions with large distance to all the coordinate functions of bijective monomials. The construction method depends on whether N is a composite number or not.

4 Case 1: N is a composite number

Let $N = nm$ where $n, m > 1$. Let $\underline{\mathbf{b}} = \{b_j\}_{j \geq 0}$ be a binary sequence with $per(\underline{\mathbf{b}}) = d = \frac{q^n - 1}{q - 1}$, $q = 2^m$, and $w(\underline{\mathbf{b}}) = v$. Let $g(x) \leftrightarrow \underline{\mathbf{b}}$. In the following, we derive some bounds on $NLG(g)$ in terms of v.

Write $a_i = Tr_1^{nm}(\alpha^i)$, $i = 0, 1, \cdots$. Thus $\underline{\mathbf{a}} = \{a_i\}$ is an m-sequence of period $2^N - 1$. Let

$$\delta(\tau) = |\{0 \leq i < d | b_i = 1, Tr_m^N(\alpha^{i+\tau}) = 0\}|.$$

Lemma 1. *With the above notation, we have*

$$w(Tr(\alpha^\tau x^r) + g(x)) = 2^{nm-1} - v + q\delta(\tau). \tag{5}$$

Proof. Throughout the proof, we will write $\delta(\tau)$ as δ for simplicity. The sequence $\underline{\mathbf{a}}$ can be arranged into a $(q-1,d)$-interleaved sequence [8]. Thus $\underline{\mathbf{a}}$ can be arranged into the following array

$$A = \begin{bmatrix} a_0 & a_1 & \cdots & a_{d-1} \\ a_d & a_{d+1} & \cdots & a_{2d-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{d(q-2)} & v_{d(q-2)+1} & \cdots & v_{(q-1)d-1} \end{bmatrix} = [A_0, A_1, \cdots, A_{d-1}],$$

where A_i's are columns of the matrix. Similarly we can arrange the sequence $\underline{\mathbf{b}}$ in the following array

$$B = \begin{bmatrix} b_0 & b_1 & \cdots & b_{d-1} \\ b_d & b_{d+1} & \cdots & b_{2d-1} \\ \vdots & \vdots & \vdots & \vdots \\ b_{d(q-2)} & b_{d(q-2)+1} & \cdots & b_{(q-1)d-1} \end{bmatrix}.$$

Note that $w(A) = |\{(i,j)|a_{ij} = 1\}, 0 \leq i < q-1, 0 \leq j < d\}|$. Thus

$$w(A+B) = \sum_{b_i=0} w(A_i) + \sum_{b_i=1} w(A_i+1)$$

$$= \sum_{b_i=0} w(A_i) + \sum_{b_i=1} (q-1-w(A_i)).$$

In the array A, there are

$$r = \frac{q^{n-1}-1}{q-1} \tag{6}$$

zero columns (See Lemma 1 in [18]). If there are δ zero columns corresponding to the indices of the 1's in $\{b_i\}$, then they contribute $\delta(q-1)$ 1's. Thus we have

$$w(A+B) =$$

$$\sum_{b_i=0, A_i\neq 0} w(A_i) + \sum_{b_i=0, A_i=0} w(A_i) + \sum_{b_i=1, A_i\neq 0} (d-w(A_i)) + \sum_{b_i=1, A_i=0} (q-1-w(A_i)).$$

Since A_i's are m-sequences, then for all the non-zero A_i's we have $w(A_i) = 2^{m-1}$. Let

$$N_{ij} = |\{b_k = i, char(A_k) = j, 0 \leq k < d\}|,$$

where $i, j \in \{0,1\}$ and

$$char(A_i) = \begin{cases} 0 \text{ if } A_i = 0, \\ 1 \text{ if } A_i \neq 0. \end{cases}$$

Note that

$$\begin{aligned} &N_{1,0} = \delta, \\ &N_{1,0} + N_{0,0} = r, \\ &N_{0,0} = r - \delta. \end{aligned} \tag{7}$$

Hence we have

$$N_{1,0} + N_{1,1} = v \Rightarrow N_{1,1} = v - N_{1,0} = v - \delta,$$

$$N_{0,1} + N_{1,1} = d - r \Rightarrow N_{0,1} = d - r - N_{1,1} = d - r - (v - \delta) = d - r - v - \delta.$$

Thus

$$\begin{aligned} w(A+B) &= 2^{m-1}N_{0,1} + 0N_{0,0} + (2^{m-1}N_{1,1} + (2^m - 1)N_{1,0} \\ &= 2^{m-1}(d-r-v) + \delta 2^{m-1} + v(2^{m-1} - 1) - \delta 2^{m-1} + \delta + 2^m\delta - \delta \\ &= 2^{m-1}(d-r) - v2^{m-1} + v2^{m-1} - v + 2^m\delta \\ &= 2^{m-1}(d-r) - v + 2^m\delta = 2^{m-1}(d-r) - v + 2^m\delta. \end{aligned} \tag{8}$$

By noting that $d - r = q^{n-1}$ then we have

$$w(A+B) = 2^{nm-1} - v + 2^m\delta,$$

which proves the lemma.

Theorem 1. *With the notation above, if* $v = \frac{d-1}{2}$ *then*

$$NLG(g) \geq 2^{nm-1} - \frac{d-1}{2}.$$

Proof.

$$\begin{aligned} \widehat{g}(0,c) &= \sum_{x \in \mathbb{E}} (-1)^{g(x)} = 1 + \sum_{x \in E^*} (-1)^{g(x)} = 1 + (q-1)\sum_{k=0}^{d-1} (-1)^{b_k} \\ &= 1 + (q-1)(d - 2wt(\underline{\mathbf{b}})) = q. \end{aligned}$$

For $\lambda \neq 0$,

$$\begin{aligned} \widehat{g}(\lambda, c) &= \textstyle\sum_{x \in \mathbb{E}} (-1)^{Tr(\lambda x^c) + g(x)} = 1 + \sum_{i=0}^{2^{nm}-1} (-1)^{a_i + b_i} \\ &= 2^{nm} - 2wt(A+B). \end{aligned} \tag{9}$$

Note that $\delta \leq r = \frac{q^{n-1}-1}{q-1}$. Thus

$$w(A+B) \leq 2^{nm-1} - \frac{d-1}{2},$$

and

$$w(A+B) \geq -2^{nm-1} - \frac{d-1}{2} + q\frac{q^{n-1}-1}{q-1} = -2^{nm-1} + \frac{d-1}{2}.$$

By noting that $n > 1$ then $d - 1 > q$ and hence

$$|\widehat{g}(\lambda, c)| \leq (d-1)$$

which proves the theorem.

Using the construction above for $N = 9$, $m = n = 3$ we get $NLG = 220$. It is clear that, in order to maximize NLG, we should minimize $d = \frac{2^{nm}-1}{2^m-1}$. Thus we should choose m to be the large factor of $N = n \times m$. For example, let $N = 15 = 3 \times 5$. If we choose $m = 5$, then we have $NLG = 15856$. However, if we picked $m = 3$, then we get $NLG = 14044$.

5 Case 2: N is a prime number

If N is a prime number then the above sub-field construction is not applicable. This case is further divided into two cases depending on whether $2^N - 1$ is a prime number or not.

5.1 Case 2.1: $2^N - 1$ is a prime number

In this case, we base our construction on the Legendre sequence. Let γ be a primitive root of a prime p, then the Legendre sequence (also called quadratic residue sequence) of period p, $p \equiv 3 \pmod 4$,is defined by

$$a_i = \begin{cases} 1 \text{ or } 0, \text{if } i = 0 \\ 1, \qquad \text{i is a residue } (i \equiv \gamma^{2s} \bmod p \\ 0, \qquad \text{i is a non-residue } (i \not\equiv \gamma^{2s} \bmod p) \end{cases}$$

Note that for $N \geq 2$ we always have $2^N - 1 \equiv 3 \bmod 4$. The properties of Legendre sequences have been extensively studied (e.g., [2], [5], [6], [12]). In here we are concerned with the following fact:

Fact 1 *If a Legendre sequence of period $p \equiv 3$ mod 4 is decimated with d then the original sequence is obtained if d is a quadratic residue mod p, and the reverse sequence is obtained if d is non-quadratic residue mod p.*

This fact can be easily explained by noting that the Boolean function corresponding to Legendre sequence has the following trace representation [12]

$$f(x) = \sum_{c \in QR} Tr(x^c),$$

where QR denotes the set of quadratic residue mod $2^N - 1$.

Example 1. Let p=7, then $\underline{\mathbf{a}} = \{1110100\}$ The sequences $\underline{\mathbf{a}}^{(d)}$ obtained by decimating $\underline{\mathbf{a}}$ with d are given by

$$\begin{aligned} \underline{\mathbf{a}}^{(1)} &= \{1110100\}, \\ \underline{\mathbf{a}}^{(2)} &= \{1110100\}, \\ \underline{\mathbf{a}}^{(3)} &= \{1001011\}, \\ \underline{\mathbf{a}}^{(4)} &= \{1110100\}, \\ \underline{\mathbf{a}}^{(5)} &= \{1001011\}, \\ \underline{\mathbf{a}}^{(6)} &= \{1001011\}. \end{aligned} \tag{10}$$

Note that $\underline{\mathbf{a}}^{(1)} = \underline{\mathbf{a}}^{(2)} = \underline{\mathbf{a}}^{(3)}$ since $1, 2, 4$ are quadratic residue mod 7. Also $\underline{\mathbf{a}}^{(3)} = \underline{\mathbf{a}}^{(5)} = \underline{\mathbf{a}}^{(6)}$ are the same since since $3, 5, 6$ are quadratic non-residue mod 7.

The following property follows directly from Fact 1.

Property 1. Let $f \leftrightarrow \underline{\mathbf{a}}$ where $\underline{\mathbf{a}}$ is a Legendre sequence. Then we have

$$NLG(f) = \min \{NL(f), NL(g)\}, \tag{11}$$

where $g \leftrightarrow \underline{\mathbf{a}}^{(c)}$ and c is any quadratic non-residue modulo $2^N - 1$.

Example 2. For $N = 5$, $\underline{\mathbf{b}} = \{1110110111110001010111000001001 00\}$. If we let $f \leftrightarrow \underline{\mathbf{b}}$ with $f(0) = 1$ then we have $\hat{f}(\lambda, c) \in \{-2, -6, -10, 2, 6, 10\}$ for $c \in$ set of quadratic residue mod 31. $\hat{f}(\lambda, c) \in \{-2, -6, 2, 10\}$ for $c \notin$ set of quadratic residue mod 31. Thus we have $NLG(f) = 11$.

Table 1 shows NLG of the functions obtained from this construction. In this case, we set $f(0) = 1$. If we set $f(0) = 0$ then we obtain balanced functions for which NLG is 1 less than the values shown in the table.

N	3	5	7	13	17	19
NLG	1	11	55	3964	64816	259882

Table 1.

Table 2 shows NLG versus NL distribution for $N = 5$. It is clear that our Legendre sequence construction achieves the maximum possible NLG. Table 3 shows the same distribution for balanced functions. For $N = 7$ we searched all functions in the form [7]

$$f(x) = \sum_{c \in \Omega(2^N - 1)} Tr_1^{n_c}(x^c),$$

where $\Omega(2^N - 1)$ is the set of coset leaders mod $2^N - 1$ and n_c is the size of the coset containing c. Table 4 shows NLG versus NL distribution for this case. Table 5 shows the same distribution for the balanced functions of the same form. Again, it's clear that the construction above achieves the best possible NLG. For larger values of N, our construction is no longer optimum. For example, for $N = 13$, $g(x) \leftrightarrow \underline{\mathbf{b}} = \{i \bmod 2 \ , i = 0, 1, \cdots\}$ have $NLG = 3972$.

5.2 Case 2.2: N is a prime number and $2^N - 1$ is a composite number

Let $2^N - 1 = dr$, $d > r > 1$. In this case we a use construction similar to case 1, i.e., we let $f \leftrightarrow \underline{\mathbf{b}}$ where $per(\underline{\mathbf{b}}) = d$ and $w(\underline{\mathbf{b}}) = \frac{d-1}{2}$. However, unlike case 1, there is no easy way to determine the weight distribution of A_i's because they are no longer m-sequences. Using this approach for $N = 11$, $d = 89$ we obtained several functions with $NLG(f) = 980 = 2^{N-1} - \frac{d-1}{2}$.

6 Conclusions and open problems

In this paper we presented some methods to construct functions with odd number of inputs which achieve large minimum distance to the set of all bijective monomials. However, since a a general upper bound on NLG is not known, it is interesting to search for other functions that outperform the constructions presented in this paper. Finding NLG of functions corresponding to the Legendre sequences is another interesting open problem.

References

1. R.E. Blahut, *Theory and practice of error control codes*, Addison-Wesley Publishing Company, 1983.
2. I. B. Damgard, *On the randomness of Legendre and Jacobi sequences*, Advances in Cryptology - CRYPTO '88, pp. 163-172.
3. J. F. Dillon, *Elementary Hadamard difference sets*, Ph.D. Dissertation, University of Maryland, 1974.
4. S.W. Golomb, *Shift register sequences*, Aegean Park Press, Laguna Hills, California, 1982.
5. C. Ding, T. Helleseth and W. Shan, *On the linear complexity of Legendre sequences*, IEEE Trans. Inf. Theory, vol. IT-44, no.3, pp. 1276-1278, May 1998.
6. P. Fan and M. Darnell, *Sequence design for communications applications*, John Wiley and Sons Inc., 1996.
7. C. Fontaine, *The Nonlinearity of a class of Boolean functions with short representation*, Proc. of Pragocrypt ' 96, pp. 129-144, 1996.
8. G. Gong, Theory and applications of q-ary interleaved sequences, *IEEE Trans. on Inform. Theory*, vol. 41, No. 2, 1995, pp. 400-411.
9. G. Gong and S. W. Golomb, *Transform domain analysis of DES*, IEEE transactions on Information Theory. Vol. IT-45, no. 6, pp. 2065-2073, September, 1999.
10. T. Jakobsen and L. Knudsen, *The interpolation attack on block ciphers, LNCS 1267*, Fast Software Encryption, pp. 28-40. 1997.
11. T. Jakobsen, *Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree*, Proceedings of Crypto'99, LNCS 1462, pp. 213-222, 1999.
12. J. No; H. Lee; H. Chung; H. Song, *Trace representation of Legendre sequences of Mersenne prime period*, IEEE Trans. Inf. Theory, vol. IT-42, no.6, pt.2, pp.2254-2255.
13. M. Matsui, *Linear cryptanalysis method for DES cipher* Advances in Cryptology, Proceedings of Eurocrypt'93, LNCS 765, pp. 386-397, Springer-Verlag, 1994.
14. R. J. McEliece, *Finite fields for computer scientists and engineers* , Kluwer Academic Publishers, Dordrecht, 1987.
15. N.J. Patterson, D.H. and Wiedemann, *The covering radius of the* $(2^{15}, 16)$ *Reed-Muller code is at least 16276*, IEEE Trans. Inf. Theory, vol.IT-29, no.3, pp. 354-356, May 1983.
16. N.J. Patterson, D.H. and Wiedemann, *Correction to: The covering radius of the* $(2^{15}, 16)$ *Reed-Muller code is at least 16276*, IEEE Trans. Inf. Theory, vol.IT-36, no.2, pp. 343, March 1990.
17. O.S. Rothaus , On bent functions, *J. Combinatorial Theory*, vol. 20(A), 1976, pp.300-305.

18. R.A. Scholtz and L.R. Welch, *GMW sequences*, IEEE Trans. Inf. Theory, vol.IT-30, no.3, pp. 548-553, May 1984.
19. A. Youssef and G. Gong, Hyper-bent functions, *Advances in Cryptology, Proc. of Eurocrypt'2001*, LNCS 2045, pp. 406-419, Springer-Verlag, 2001.

NLG	0	1	2	3	4	5	6	7	8	9	10	11
NL												
0	64	0	0	0	0	0	0	0	0	0	0	0
1	0	2048	0	0	0	0	0	0	0	0	0	0
2	0	0	31744	0	0	0	0	0	0	0	0	0
3	0	0	0	317440	0	0	0	0	0	0	0	0
4	0	0	0	0	2301440	0	0	0	0	0	0	0
5	0	0	0	0	0	12888064	0	0	0	0	0	0
6	0	0	0	0	13020	0	57983268	0	0	0	0	0
7	0	0	0	7440	0	3919392	0	211487952	0	0	0	0
8	0	0	2790	0	2396610	0	74021180	0	571246300	0	0	0
9	0	620	0	923180	0	39040780	0	544800200	0	777687700	0	0
10	62	0	149668	0	8474160	0	189406218	0	1022379070	0	191690918	0
11	0	9300	0	606980	0	19419516	0	232492250	0	302968890	0	911896
12	248	0	1302	0	263810	0	3803018	0	20035610	0	3283148	0

Table 2. $N = 5$

NLG	0	2	4	6	8	10
NL						
0	62	0	0	0	0	0
2	0	15872	0	0	0	0
4	0	0	892800	0	0	0
6	0	0	6200	19437000	0	0
8	0	1550	1074150	27705010	167500130	0
10	62	77128	3274220	62085560	276057170	34259588
12	248	682	109430	1536050	6312220	735258

Table 3. $N = 5$ balanced case

NLG	0	2	8	14	16	22	28	30	36	42	44	46	48	50	52	54
NL																
2	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	72	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	306	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	306	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	3264	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	90	0	6030	0	0	0	0	0	0	0	0	0
30	0	0	0	90	0	0	1269	4761	0	0	0	0	0	0	0	0
36	0	0	72	0	0	3156	4032	2916	23088	0	0	0	0	0	0	0
42	0	6	0	280	460	2448	4715	4408	12927	7012	0	0	0	0	0	0
44	6	0	0	460	280	2448	6696	2427	12927	6248	764	0	0	0	0	0
46	0	0	0	4	1	121	157	174	326	119	0	8	0	0	0	0
48	0	0	1	25	46	578	1232	757	2486	1052	3	0	50	0	0	0
50	0	0	326	918	948	10187	16267	9632	32340	16288	33	90	401	742	0	0
52	0	1	120	549	504	4746	6409	4236	12167	5781	15	25	170	272	5	0
54	2	10	46	228	164	1281	2557	1295	4548	1727	1	21	5	84	1	1
56	10	0	47	47	108	619	1270	570	2241	926	15	0	13	27	0	1

Table 4. $N = 7$

NLG	0	2	14	16	28	30	42	44	52	54
NL										
0	1	0	0	0	0	0	0	0	0	0
2	0	1	0	0	0	0	0	0	0	0
14	0	0	81	0	0	0	0	0	0	0
16	0	0	0	81	0	0	0	0	0	0
28	0	0	0	54	1242	0	0	0	0	0
30	0	0	54	0	561	681	0	0	0	0
42	0	6	160	232	2144	1997	2517	0	0	0
44	6	0	232	160	3067	1074	2510	7	0	0
46	0	0	4	1	66	76	28	0	0	0
48	0	0	21	39	904	561	747	3	0	0
50	0	0	82	115	1220	544	908	1	0	0
52	0	1	549	504	6409	4236	5781	15	5	0
54	2	10	228	164	2557	1295	1727	1	1	1
56	10	0	47	108	1270	570	926	15	0	1

Table 5. $N = 7$ balanced case