ISSN:0975-9646

Secondary Construction of Non-normal Boolean Functions

Deepmala Sharma[1], Rashmeet Kaur[2]

Department of Mathematics
National Institute of Technology
Raipur, Chhattisgarh

***Abstract*— Normality of a Boolean function is an important cryptographic property. It gives information about the structure of a Boolean function. If an n-variable Boolean function is normal then it is constant on a $n/2$-dimensional affine subspace. Although almost all Boolean functions are non-normal but very few examples are known. In this paper, we proposed a secondary construction of non-weakly $(k+2)$-normal Boolean function on $(n+4)$ variables from two non-weakly k-normal Boolean functions on n variables.**

Keywords— Boolean functions, Non-linearity, Normality

INTRODUCTION

Boolean functions play a significant role in Cryptography. They are the main building blocks for the design of various ciphers. Boolean functions which are to be used in ciphers must possess high non-linearity. Bent functions belong to the family of Boolean functions which possess maximum non-linearity, but they cannot be used directly in a cryptosystem as they are not balanced. The notion of normality was first introduced by Dobbertin [5] to construct highly non-linear balanced Boolean functions. Since Dobbertin's work is mainly concerned with the construction of Bent functions, normality was first introduced with the even number of variables. Later on, the notion of normality was extended to odd variables by Charpin [8]. In the same paper the notion of k-normality was introduced. Several results on non-normal and k-normal Boolean functions have been found in the literature [1], [2], [6], [7], [10].

Dobbertin [5] by using counting principle proved that although almost all Boolean functions are non-normal but very few examples are known. We have extended the result presented in [10]. We prove our result by using the technique as given in [10], [2].

PRELIMINARIES

A Boolean function is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2$ denotes the finite field of characteristic 2. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. The support of $f \in \mathcal{B}_n$ is defined by the set

$$\mathrm{Supp}(f) = \{x \in \mathbb{F}_2^n | f(x) \neq 0\}$$

and the weight of f denoted by $wt(f) = |\mathrm{Supp}(f)|$. The Hamming distance between two Boolean functions $f, g \in \mathcal{B}_n$ is defined by the number of positions in which the functions differ and is denoted by $d(f, g)$.

Let $f: \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables. The Walsh transform of f is defined by

$$f^w(\lambda) = \Sigma_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\lambda.x}$$

Non-linearity of a Boolean function $f \in \mathcal{B}_n$ is defined as minimum Hamming distance of f from set of all affine functions and is denoted by $nl(f)$.
Non-linearity can also be calculated from Walsh transform by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^n} |f^w(\lambda)|$$

The family of Boolean functions with maximum non-linearity is called Bent functions. They exists only for even n.

A Boolean function $f \in \mathcal{B}_n$ is called normal or weakly normal, if restriction of f to a $\lceil n/2 \rceil$-dimensional flat is constant or affine respectively.

A Boolean function $f \in \mathcal{B}_n$ is said to be k-normal or weakly k-normal, if there exists a flat U of dimension k such that f is constant or affine on U respectively.

MAIN RESULT

In this section we have proved our main result:

Theorem 1 : Let $f_1, f_2: \mathbb{F}_2^n \to \mathbb{F}_2$ be two Boolean functions on n variables. Then f_1 or f_2 is weakly k-normal if and only if the function

$$g(x, y_1, y_2, y_3, y_4): \mathbb{F}_2^n \times \mathbb{F}_2^4 \to \mathbb{F}_2,$$

where

$$\mathbb{F}_2^4 = \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2,$$

defined by

$$g(x, y_1, y_2, y_3, y_4) = f_1(x) + y_1y_2 + y_1y_3 + y_1y_4 + y_2y_3 + y_2y_4 + y_3y_4 + (y_1 + y_2 + y_3 + y_4)(f_1(x) + f_2(x))$$

is weakly $(k+2)$-normal.

Proof: In order to prove our result first we assume g is weakly $(k+2)$ -normal. Then there exists a $(k+2)$-dimensional flat H, $\zeta \in \mathbb{F}_2^n$ and $\alpha, \beta, \gamma, \delta \in \mathbb{F}_2$ such that
$h(x, y_1, y_2, y_3, y_4) = g(x, y_1, y_2, y_3, y_4) + \alpha y_1 + \beta y_2 + \gamma y_3 + \delta y_4 + \langle \zeta, x \rangle$

takes the same value, e, on H. We claim that either $f_1(x)$ or $f_2(x)$ is weakly k-normal. For $a, b, c, d \in \mathbb{F}_2$, we define

$$H_{abcd} = \{x \in \mathbb{F}_2^n | (x, a, b, c, d) \in H\}.$$

Now there exists an element $u \in \mathbb{F}_2^n \times \mathbb{F}_2^4$ and a $(k+2)$-dimensional subspace H_1 of $\mathbb{F}_2^n \times \mathbb{F}_2^4$ (Since H is a $(k+2)$- dimensional flat) such that $H = u + H_1$.

We define a map
$$\varphi: \mathbb{F}_2^n \times \mathbb{F}_2^4 \to \mathbb{F}_2^n$$
defined by
$\varphi(x, a, b, c, d) = x$ for all $(x, a, b, c, d) \in \mathbb{F}_2^n \times \mathbb{F}_2^4$.

Clearly
$H_{abcd} = \varphi(\mathbb{F}_2^n \times \{a\} \times \{b\} \times \{c\} \times \{d\}) \cap H)$.

Suppose $(\mathbb{F}_2^n \times \{a\} \times \{b\} \times \{c\} \times \{d\}) \cap H \neq \phi$ and let $(x, a, b, c, d), (y, a, b, c, d) \in (\mathbb{F}_2^n \times \{a\} \times \{b\} \times \{c\} \times \{d\}) \cap H$.
since $H = u + H_1$,
$(x, a, b, c, d) - (y, a, b, c, d) = (x - y, 0,0,0,0) \in (\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1)$.

Again if $(x, a, b, c, d) \in (\mathbb{F}_2^n \times \{a\} \times \{b\} \times \{c\} \times \{d\}) \cap H$ and $(z, 0,0,0,0) \in (\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1$ then $(x, a, b, c, d) + (z, 0,0,0,0) = (x + z, a, b, c, d) \in (\mathbb{F}_2^n \times \{a\} \times \{b\} \times \{c\} \times \{d\}) \cap H$.
Therefore $(\mathbb{F}_2^n \times \{a\} \times \{b\} \times \{c\} \times \{d\}) \cap H$ is a flat of subspace $(\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1$ for any $a, b, c, d \in \mathbb{F}_2$.
Hence, all the non-empty H_{abcd}'s are flats of the same subspace $\varphi((\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1)$ and therefore have the same dimension.

Let $\psi: \mathbb{F}_2^n \times \mathbb{F}_2^4 \to \mathbb{F}_2^4$ be a map defined by

$$\psi(x, a, b, c, d) = (a, b, c, d),$$
then $(\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1$ is the kernel of ψ restricted to H_1. Thus

$\dim((\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1) = (k+2) - \dim(\psi(H_1))$

The $\dim(\psi(H_1)) \in \{0,1,2,3,4\}$. Because φ is restricted to $(\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\})$ is bijective.

$\dim(\varphi(\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1)) = \dim((\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1)$

Therefore
$$\varphi(\mathbb{F}_2^n \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cap H_1)$$
has dimension either $k+2,\ k+1,\ k,\ k-1,\ k-2$.

Suppose $x \in H_{abcd}$, then

$e = h(x, a, b, c, d) = f_1(x) + ab + ac + ad + bc + bd + cd + (a + b + c + d)(f_1(x) + f_2(x)) + \alpha a + \beta b + \gamma c + \delta d + \langle \zeta, x \rangle$
i.e.,

$$f_1(x) + (a + b + c + d)(f_1(x) + f_2(x)) = \begin{cases} f_1(x), & \text{if } a + b + c + d = 0 \\ f_2(x), & \text{if } a + b + c + d = 1 \end{cases}$$

Therefore if $H_{abcd} \neq \phi$ then either $f_1(x)$ or $f_2(x)$ is affine on H_{abcd}.

We need to check whether one of the flats H_{abcd} has dimension $\geq k$ or not. If this is so then we are done. If this is not true, then for any $a, b, c, d \in \mathbb{F}_2^n$ the number of elements in H_{abcd}, $|H_{abcd}| \in \{0, 2^{k-2}\}$.
Since $|H_{abcd}| = |\{(x, a, b, c, d): x \in H\}|$

we have

$$|H| = \Sigma_{d \in \mathbb{F}_2} \Sigma_{c \in \mathbb{F}_2} \Sigma_{b \in \mathbb{F}_2} \Sigma_{a \in \mathbb{F}_2} |H_{abcd}| = 2^{k+2}$$

This is possible iff $|H_{abcd}| = 2^{k-2}$. Now consider the flats $H_{\bar{\alpha}\beta\gamma\delta}$, $H_{\alpha\bar{\beta}\gamma\delta}$, $H_{\alpha\beta\bar{\gamma}\delta}$, $H_{\alpha\beta\gamma\bar{\delta}}$. Since any two flats of a subspace are disjoint or identical. We shall show that all these four flats are pairwise distinct. Suppose if possible let $H_{\bar{\alpha}\beta\gamma\delta} = H_{\alpha\bar{\beta}\gamma\delta}$ so that for any element $(x, \bar{\alpha}, \beta, \gamma, \delta) \in H$ the element $(x, \alpha, \bar{\beta}, \gamma, \delta) \in H$ where for any $\varepsilon \in \mathbb{F}_2$, if $\varepsilon = 0$ then $\bar{\varepsilon} = 1$ or vice versa. If we consider two elements $(x, \bar{\alpha}, \beta, \gamma, \delta)$ and $(x', \alpha, \beta, \gamma, \delta)$ in H we obtain that,

$$(x, \bar{\alpha}, \beta, \gamma, \delta) + (x, \alpha, \bar{\beta}, \gamma, \delta) + (x', \alpha, \beta, \gamma, \delta) = (x', \bar{\alpha}, \bar{\beta}, \gamma, \delta)$$
belongs to H implying that

$$h(x', \alpha, \beta, \gamma, \delta) = h(x', \bar{\alpha}, \bar{\beta}, \gamma, \delta).$$
But,

$$h(x', \bar{\alpha}, \bar{\beta}, \gamma, \delta) = h(x', \alpha, \beta, \gamma, \delta) + 1$$

which leads to a contradiction that h is constant on H.
Therefore $H_{\bar{\alpha}\beta\gamma\delta}$ and $H_{\alpha\bar{\beta}\gamma\delta}$ are distinct parallel flats. Similarly we can show that the other flats are also pairwise distinct.

Since $H_{\bar{\alpha}\beta\gamma\delta}$, $H_{\alpha\bar{\beta}\gamma\delta}$, $H_{\alpha\beta\bar{\gamma}\delta}$, $H_{\alpha\beta\gamma\bar{\delta}}$ are distinct parallel flats of dimension $k-2$, the set

$$\mathcal{H} = H_{\bar{\alpha}\beta\gamma\delta} \cup H_{\alpha\bar{\beta}\gamma\delta} \cup H_{\alpha\beta\bar{\gamma}\delta} \cup H_{\alpha\beta\gamma\bar{\delta}}$$
is a flat of dimension k.

Moreover we deduce that for all $x \in H_{\bar{\alpha}\beta\gamma\delta}$

$$e = h(x, \bar{\alpha}, \beta, \gamma, \delta)$$
i.e. $f_1(x) + (1 + \alpha + \beta + \gamma + \delta)\big(f_1(x) + f_2(x)\big) = e + \alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta + \langle\zeta, x\rangle$,

for all $x \in H_{\alpha\bar{\beta}\gamma\delta}$

$$e = h\big(x, \alpha, \bar{\beta}, \gamma, \delta\big)$$
i.e. $f_1(x) + (1 + \alpha + \beta + \gamma + \delta)\big(f_1(x) + f_2(x)\big) = e + \alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta + \langle\zeta, x\rangle$,
for all $x \in H_{\alpha\beta\bar{\gamma}\delta}$

$$e = h(x, \alpha, \beta, \bar{\gamma}, \delta)$$
i.e. $f_1(x) + (1 + \alpha + \beta + \gamma + \delta)\big(f_1(x) + f_2(x)\big) = e + \alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta + \langle\zeta, x\rangle$.
for all $x \in H_{(\alpha\,\beta\gamma\bar{\delta})}$

$$e = h\big(x, \alpha, \beta, \gamma, \bar{\delta}\big)$$
i.e. $f_1(x) + (1 + \alpha + \beta + \gamma + \delta)\big(f_1(x) + f_2(x)\big) = e + \alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta + \langle\zeta, x\rangle$.

Therefore when $x \in \mathcal{H}$

$$f_1(x) + (1 + \alpha + \beta + \gamma + \delta)\big(f_1(x) + f_2(x)\big) = e + \alpha\beta + \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta + \gamma\delta + \langle\zeta, x\rangle.$$

If $(1 + \alpha + \beta + \gamma + \delta) = 1$ then $f_2(x)$ is affine on $\mathcal{H}$ otherwise $f_1(x)$ is affine on $\mathcal{H}$. Therefore either $f_1(x)$ or $f_2(x)$ is weakly k- normal.

Conversely suppose $f_1(x)$ or $f_2(x)$ is weakly k-normal. First suppose $f_1(x)$ is weakly normal which implies that there exists a k-dimensional flat H on which $f_1(x)$ is affine. Suppose $f_1(x) = \langle\zeta, x\rangle + e$ on H. Consider the $(k + 2)$- dimensional flat

$H' = (H \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cup (H \times \{1\} \times \{1\} \times \{1\} \times \{1\}) \cup (H \times \{1\} \times \{1\} \times \{0\} \times \{0\}) \cup (H \times \{0\} \times \{0\} \times \{1\} \times \{1\})$.

If H is a flat of the subspace H_1 then H' is a flat of the subspace

$H_1' = (H_1 \times \{0\} \times \{0\} \times \{0\} \times \{0\}) \cup (H_1 \times \{1\} \times \{1\} \times \{1\} \times \{1\}) \cup (H_1 \times \{1\} \times \{1\} \times \{0\} \times \{0\}) \cup (H_1 \times \{0\} \times \{0\} \times \{1\} \times \{1\})$

It can be checked that

$$g(x, 0,0,0,0) = f_1(x) = \langle\zeta, x\rangle + e$$
and
$$g(x, 1,1,1,1) = f_1(x) = \langle\zeta, x\rangle + e.$$

$$g(x, 1,1,0,0) = f_1(x) + 1 = \langle\zeta, x\rangle + e + 1.$$

$$g(x, 0,0,1,1) = f_1(x) + 1 = \langle\zeta, x\rangle + e + 1.$$

Therefore
$$g(x, y_1, y_2, y_3, y_4) = \langle\zeta, x\rangle + e + y_1 + y_3$$

for all $(x, y_1, y_2, y_3, y_4) \in H'$.

Suppose that $f_2(x)$ is weakly k-normal which implies that there exists a k-dimensional flat H on which $f_2(x)$ is affine. Suppose $f_2(x) = \langle\zeta, x\rangle + e$ on H. Consider the $(k + 2)$ dimensional flat

$H' = (H \times \{1\} \times \{0\} \times \{0\} \times \{0\}) \cup (H \times \{0\} \times \{1\} \times \{1\} \times \{1\}) \cup (H \times \{0\} \times \{1\} \times \{0\} \times \{0\}) \cup (H \times \{1\} \times \{0\} \times \{1\} \times \{1\})$.

The flat H' constructed as above is a coset of subspace $H_1' = (H_1 \times \{1\} \times \{0\} \times \{0\} \times \{0\}) \cup (H_1 \times \{0\} \times \{1\} \times \{1\} \times \{1\}) \cup (H_1 \times \{0\} \times \{1\} \times \{0\} \times \{0\}) \cup (H_1 \times \{1\} \times \{0\} \times \{1\} \times \{1\})$.

As above we check that

$$g(x, 1,0,0,0) = f_2(x) = \langle\zeta, x\rangle + e.$$

$$g(x, 0,1,1,1) = f_2(x) + 1 = \langle\zeta, x\rangle + e + 1.$$

$$g(x, 0,1,0,0) = f_2(x) = \langle\zeta, x\rangle + e.$$

$$g(x, 1,0,1,1) = f_2(x) + 1 = \langle\zeta, x\rangle + e + 1.$$

Therefore
$$g(x, y_1, y_2, y_3, y_4) = \langle\zeta, x\rangle + e + y_3$$

for all $(x, y_1, y_2, y_3, y_4) \in H'$.

Thus g is weakly $(k + 2)$-normal.

CONCLUSION

In this paper we present a secondary construction of non-nomal Boolean functions. This result is extension of the result presented in [10]. We demonstrate the technique used in [10] to construct secondary construction of non-weakly $(k + 2)$- normal Boolean function on $(n + 4)$ variables.

REFERENCES

[1] A. Braeken, C. Wolf, and B. Preneel, *"A randomised algorithm for checking the normality of cryptographic Boolean functions,"* in 3rd IFIP International Conference on Theoretical Computer, pp. 51–66, 2004.

[2] A. Canteaut, M. Daum, H. Dobbertin and G. Leander, "*Normal and Non Normal Bent Functions,*" Workshop on Coding and Cryptography '03, pp. 91 - 100.

[3] C. Carlet, H. Dobbertin and G. Leander, "*Normal Extensions of Bent Functions*," IEEE Trans. on Information Theory, number 11 pp. 2880 - 2885, 2004.

[4] C. Carlet, *"On secondary constructions of resilient and bent functions"*, Coding, Cryptography and Combinatorics, Progress in

computer science and applied logic, Birkhauser Verlag, Basel, vol. 23, pp.3 - 28, 2004.

[5] H. Dobbertin, "*Construction of bent functions and balanced Boolean functions with high nonlinearity*," in: Fast Software Encryption—FSE'94, Lecture Notes in Computer Science, Springer, Berlin, vol. 1008, pp. 61–74,1995.

[6] M. Daum, H. Dobbertin, and G. Leander, "*An algorithm for checking normality of Boolean functions*," in 2003 Workshop on Coding and Cryptography (WCC), pp. 133–142, 2003.

[7] N. Kolokotronis and K. Limniotis, "*A Greedy Algorithm for Checking Normality of Cryptographic Boolean* Functions," ISITA, Honolulu, Hawaii, USA, 2012.

[8] P. Charpin, "*Normal Boolean functions*," J. Complexity, vol. 20, pp. 245–265, 2004.

[9] R. Lidl and H. Niederreiter, "*Introduction to finite fields and their applications*," Cambridge University Press, 1994.

[10] S. Gangopadhyay and D. Sharma, "*On construction of non-normal Boolean functions*," Australasian journal of combinatorics, vol. 38, 2007.