On the Second Order Nonlinearity of a Cubic Maiorana-McFarland Bent Function

Sumanta Sarkar [1] Sugata Gangopadhyay [2]

[1]INRIA Paris-Rocquencourt, FRANCE
[2]Indian Institute of Technology, Roorkee, INDIA

Finite Fields and their Applications 2009
July 13 - July 17, 2009

Outline

Outline

Motivation

- Second order nonlinearity is an important cryptographic property.
- However, the best known algorithm to measure the second order nonlinearity of an n-variable Boolean function works for $n \leq 13$.
- Therefore, given a Boolean function, it is important to find a lower bound of its second order nonlinearity.
- As we know that bent functions have the maximum first order nonlinearity, it is interesting to check their second order nonlinearity.

Outline

Our Contribution

- We study a new class of cubic Maiorana-McFarland bent functions which is based on a permutation constructed by Dobbertin (IEEE-IT 1999).
- First we show that this function can not have an affine derivative.
- Then we determine a lower bound of the second order nonlinearity of this function using Carlet's result (IEEE-IT 2008).

Outline

Boolean Function

- Boolean function f is a mapping :

$$f : \{0, 1\}^n \to \{0, 1\}.$$

- This is an n-variable Boolean function.
- A Boolean function f can also be defined over the finite field $\mathbb{F}_{2^n}$:

$$f : \mathbb{F}_{2^n} \to \mathbb{F}_2.$$

- Representing all $\alpha \in \mathbb{F}_{2^n}$ by the co-ordinates with respect to some basis of $\mathbb{F}_{2^n}$, the second representation gives the first one.

Reed-Muller Code

- The Reed-Muller code, $\mathcal{R}(r, n)$, of size 2^n and order r is the set of all n-variable Boolean functions of degree at most r.

r-th order nonlinearity

- Let f be an n-variable Boolean function.
- The r-th order nonlinearity ($nl_r(f)$) of f is the distance from f to the Reed-Muller code $\mathcal{R}(r, n)$.
- For $r = 1$, we simply denote it as nonlinearity.
- In this work, we are interested in $r = 2$, that is the second order nonlinearity.
- The r-th order nonlinearity is an important cryptographic property for block and stream ciphers.
- For example, there have been some notion of attack by using nonlinear approximations (r-degree Boolean function, $r > 1$) to f. To resist this attack the function needs to have high r-th order nonlinearity.

Maiorana McFarland Bent functions

- For even n, the maximum nonlinearity of an n-variable Boolean function is $2^{n-1} - 2^{\frac{n}{2}-1}$.
- For even n, the Boolean functions which possess this maximum nonlinearity are called bent functions.
- Maiorana McFarland is an important class of bent functions.
- Let $n = 2t$.
- The function $f : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_2$ given by

$$f(x, y) = Tr_1^t(x\pi(y))$$

is a Maiorana-McFarland bent function where $\pi : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ is a permutation and

$$Tr_1^t(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}.$$

Derivatives

- Let $f : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_2$.
- The derivative of f with respect to $a \in \mathbb{F}_{2^n}$, is denoted by $D_a f$ and is the Boolean function defined by

$$D_a f(x) = f(x) + f(x + a)$$

for all $x \in \mathbb{F}_{2^n}$.

Walsh Spectrum

- The Walsh transform of a Boolean function $f : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$ at $\lambda \in \mathbb{F}_{2^n}$ is defined as follows:

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr(\lambda x)}.$$

- Walsh spectrum is the set $\{W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}\}$.

Walsh Spectrum of quadratic Boolean functions

- The bilinear form associated to f is defined by

$$B(x,y) = f(0) + f(x) + f(y) + f(x+y).$$

- The kernel of $B(x,y)$ is the subspace defined by

$$\mathcal{E}_f = \{x \in \mathbb{F}_{2^n} : B(x,y) = 0 \text{ for all } y \in \mathbb{F}_{2^n}\}.$$

- For a quadratic Boolean function f, the kernel $\mathcal{E}_f$, is given by

$$\mathcal{E}_f = \{a \in \mathbb{F}_{2^n} | D_a f = constant\}.$$

Walsh Spectrum of quadratic Boolean functions (Continued)

- **Lemma 1:**(Macwilliams and Sloane; Canteaut, Charpin, Kyureghyan FFA 2008)
  If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a quadratic Boolean function and $B(x, y)$ is the quadratic form associated to it, then the Walsh Spectrum of f depends only on the dimension, k, of the kernel, $\mathcal{E}_f$, of $B(x, y)$. The weight distribution of the Walsh spectrum of f is:

$W_f(\lambda)$	number of λ
0	$2^n - 2^{n-k}$
$2^{(n+k)/2}$	$2^{n-k-1} + (-1)^{f(0)} 2^{(n-k-2)/2}$
$-2^{(n+k)/2}$	$2^{n-k-1} - (-1)^{f(0)} 2^{(n-k-2)/2}$

Outline

Known results on Higher order Nonlinearity

- **Proposition 1:** (Carlet IEEE-IT 2008)
  Let f be any n-variable Boolean function and r be a positive integer smaller than n, then

$$nl_r(f) \geq 2^{n-1} - \frac{1}{2}\sqrt{2^{2n} - 2\sum_{a \in \mathbb{F}_{2^n}} nl_{r-1}(D_a f)}.$$

- If exact values of $nl_{r-1}(D_a f)$ for all a are not known, but some lower bound is known, then we have the following corollary.
- **Corollary 1:** (Carlet IEEE-IT 2008)
  Let f be any n-variable function and r be a positive integer smaller than n. Assume that for some nonnegative integers M and m, we have $nl_{r-1}(D_a f) \geq 2^{n-1} - M2^m$ for every nonzero $a \in \mathbb{F}_{2^n}$. Then

$$\begin{aligned} nl_r(f) &\geq 2^{n-1} - \tfrac{1}{2}\sqrt{(2^n - 1)M2^{m+1} + 2^n} \\ &\approx 2^{n-1} - \sqrt{M}2^{\frac{n+m-1}{2}}. \end{aligned}$$

Outline

The Cubic Maiorana McFarland Function ϕ_n

- Let $n = 2t$, where $t = 2m + 1$ and $m \geq 2$.
- We define the cubic Maiorana-McFarland function $\phi_n : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_2$ as $\phi_n(x, y) = Tr_1^t(x(y^{2^{m+1}+1} + y^3 + y))$, where $y \mapsto y^{2^{m+1}+1} + y^3 + y$ is a permutation over $\mathbb{F}_{2^t}$ (Dobbertin IEEE-IT 1999).

Derivatives of ϕ_n

Theorem 1: The function ϕ_n does not possess any derivative in $\mathcal{R}(1, n)$.

Lower bound of second order nonlinearity of ϕ_n

Theorem 2: The lower bound of the second order nonlinearity of ϕ_n is given as

$$
\begin{aligned}
nl_2(\phi_n) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{\frac{n+t}{2}+3} + 2^n} \\
&\approx 2^{n-1} - 2^{\frac{7n+4}{8}}.
\end{aligned}
$$

Outline of the proof of Theorem 2

- Let $a, b \in \mathbb{F}_{2^t}$.
- Let $k(a, b)$ denote the dimension of the subspace

$$\mathcal{E}_{\phi_n} = \{(c, d) \in \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} | D_{(c,d)} D_{(a,b)}(\phi_n) = constant\}.$$

- $$k(a, b) = \begin{cases} t + i, \ 0 \leq i \leq 4 \text{ when } b = 0 \\ r + j, \ 0 \leq j \leq 2, 0 \leq r \leq 2 \text{ when } b \neq 0 \end{cases}$$

Outline of the proof of Theorem 2 (Continued)

- $D_{(a,b)}(\phi_n)$ is always quadratic (by Theorem 1) for $(a, b) \neq (0, 0)$.
- By Lemma 1,

$$nl(D_{a,b}(\phi_n)) = 2^{n-1} - 2^{\frac{n+k(a,b)}{2}}.$$

- since $i \leq 4$,

$$nl(D_{a,b}(\phi_n)) \geq 2^{n-1} - 2^{\frac{n+t+4}{2}}.$$

Outline of the proof of Theorem 2 (Continued)

- Comparing with Corollary 1, we get $M = 1$ and $m = \frac{n+t}{2} + 2$.
- This gives

$$\begin{aligned} nl_2(\phi_n) &\geq 2^{n-1} - \frac{1}{2}\sqrt{(2^n - 1)2^{\frac{n+t}{2}+3} + 2^n} \\ &\approx 2^{n-1} - 2^{\frac{7n+4}{8}}. \end{aligned}$$

Better lower bound than the general bound

- The general lower bound of the second order nonlinearity (Carlet IEEE-IT 2008) of an n-variable cubic Boolean function which does not have any derivative in $\mathcal{R}(1, n)$ is

$$2^{n-1} - 2^{n-\frac{3}{2}}.$$

- $2^{n-1} - 2^{\frac{7n+4}{8}} > 2^{n-1} - 2^{n-\frac{3}{2}}$, for all $n > 16$.

Conclusions and further research

- We have identified a class of Maiorana McFarland bent functions which do not have any affine derivative.
- We have studied the second order nonlinearity of these functions.
- Next step is to find a better lower bound of second order nonlinearity of this class of functions for which we need a new strategy.

Bibliography

- C. Bracken, E. Byrne, N. Markin and Gary McGuire.
  "Determining the Nonlinearity of a New Family of APN Functions". In *AAECC*, LNCS 4851, springer, pages 72–79, 2007.
- A. Canteaut and P. Charpin.
  "Decomposing Bent Functions". In *IEEE Transactions on Information Theory*, Vol. 49(8), pp. 2004-2019, 2003.
- CCK08 A. Canteaut, P. Charpin and G. M. Kyureghyan. "A new class of monomial bent functions". In *Finite Fields and their Applications*, Vol. 14, pp. 221-241, 2008.
- C. Carlet.
  "Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications". In *IEEE Transactions on Information Theory*, Vol. 54(3), pp. 1262–1272, March 2008.
- H. Dobbertin.
  "Almost Perfect Nonlinear Power Functions on $GF(2^n)$: The Welch Case". In *IEEE Transactions on Information Theory*, Vol. 45, No. 4, May 1999.
- X.-D. Hou.
  "Cubic bent functions". In *Discrete Mathematics*, Vol 189, pp 149–161.
- F. J. MacWilliams, N. J. A. Sloane,
  "The theory of Error Correcting Codes", North-Holland, Amsterdam, 1977.

THANK YOU