Probabilistic Higher Order Differential Attack and Higher Order Bent Functions

Tetsu Iwata and Kaoru Kurosawa

Department of Electrical and Electronic Engineering,
Faculty of Engineering,
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152–8552, Japan
{tez, kurosawa}@ss.titech.ac.jp

Abstract. We first show that a Feistel type block cipher is broken if the round function is *approximated* by a low degree vectorial Boolean function. The proposed attack is a generalization of the higher order differential attack to a probabilistic one. We next introduce a notion of *higher order bent functions* in order to prevent our attack. We then show their explicit constructions.

1 Introduction

Consider a Feistel type block cipher with a round function G_K such that

$$(y_1, \ldots, y_n) = G_K(x_1, \ldots, x_n) \tag{1}$$

where K denotes a key. Then G_K can be viewed as a polynomial on $\mathrm{GF}(2^n)$ or a set of Boolean functions $\{f_1, \ldots, f_n\}$ such that

$$y_i = f_i(x_1, \ldots, x_n) \text{ for } i = 1, \ldots, n \ .$$

¿From a view point of polynomials, Jakobsen and Knudsen showed the interpolation attack which is effective if the degree of G_K is small [4]. Jakobsen further showed that the block cipher is broken even if G_K is *approximated* by a low degree polynomial [3].

On the other hand, from a view point of Boolean functions, Jakobsen and Knudsen showed the higher order differential attack [4]. It is effective if each of the degree of f_i is small, where the degree is defined as the degree of a Boolean function.

In this paper, we first show that the block cipher is broken even if each f_i is *approximated* by a low degree Boolean function. We call this attack a *probabilistic* higher order differential attack because our attack is a generalization of the higher order differential attack to a probabilistic one. (It can also be considered as a generalization of the differential attack [1] to a higher order one.)

K. Y. Lam, E. Okamoto and C. Xing (Eds.): ASIACRYPT'99, LNCS 1716, pp. 62–74, 1999.

We next introduce a notion of *higher order bent functions* in order to prevent our attack. Intuitively, an r-th order bent function is a Boolean function f such that $N_f^{(r)}$ is the maximum, where $N_f^{(r)}$ is defined as a distance from f to the set of Boolean functions with degree at most r. This means that an r-th order bent function is not approximated by any Boolean function with degree at most r if r is small.

We then present some explicit constructions of r-th order bent functions such that other cryptographic criteria are satisfied as well.

This paper is organized as follows. In Section 3, we review related works. In Section 4, we propose the probabilistic higher order differential attack. In Section 5, we introduce a notion of r-th order bent functions and show their explicit constructions.

2 Preliminaries

2.1 Notation

Consider a Feistel type block cipher with block size $2n$ and m rounds. Let $x = (x_L, x_R)$ denote the plaintext, where $x_L = (x_1, \ldots, x_n)$ and $x_R = (x_{n+1}, \ldots, x_{2n})$. Similarly, let $y = (y_L, y_R)$ denote the ciphertext. Let

$$C_0^L \stackrel{\triangle}{=} x_L \text{ and } C_0^R \stackrel{\triangle}{=} x_R \ .$$

The round function G operates as follows.

$$\begin{cases} C_i^L = C_{i-1}^R \ , \\ C_i^R = G(k_i, C_{i-1}^R) \oplus C_{i-1}^L \ , \end{cases}$$

where k_i is a key of the i-th round. The ciphertext is given by

$$y = (y_L, y_R) = (C_m^R, C_m^L) \ .$$

Further, we say that

$$(C_{m-1}^L, C_{m-1}^R) = E_K(x_L, x_R)$$

is the reduced cipher, where K is the key of the reduced cipher. Let $\tilde{y} = (\tilde{y}_L, \tilde{y}_R)$ denote the reduced ciphertext. That is,

$$\tilde{y} = (\tilde{y}_L, \tilde{y}_R) = (C_{m-1}^R, C_{m-1}^L) \ .$$

In this paper, we assume that m is not large.

2.2 Degree of Boolean Functions

The degree of a Boolean function f, $\deg(f)$, is defined as the degree of the highest degree term of the algebraic normal form:

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{1 \le i \le n} a_i x_i \oplus \bigoplus_{1 \le i < j \le n} a_{i,j} x_i x_j \oplus \cdots \oplus a_{1,2,\ldots,n} x_1 x_2 \cdots x_n \ .$$

The degree of a vectorial Boolean function $F(x_1, \ldots, x_n) = (f_1, \ldots, f_n)$ is defined as

$$\deg(F) \stackrel{\triangle}{=} \max_i \deg(f_i) \ .$$

3 Related Works

3.1 Higher Order Differential Attack

The higher order differential attack [4] is based on the following proposition shown by Lai [5]. Let L_r denote an r-dimensional subspace of $\mathrm{GF}(2)^n$.

Proposition 3.1. *[5] Let f be a Boolean function. Then for any $w \in \mathrm{GF}(2)^n$,*

$$\bigoplus_{x \in L_{r+1}} f(x \oplus w) = 0$$

if and only if $\deg(f) \leq r$.

In a Feistel type block cipher, let x_R be kept constant. Then

$$\tilde{y}_R = F(x_L) \ ,$$

for some vectorial Boolean function F, where $\tilde{y}_R$ is the right half of the reduced ciphertext. Suppose that $\deg(F) \leq r$ for any fixed x_R and any fixed key of the reduced cipher. Then the last round key k_m can successfully be recovered by using 2^{r+1} chosen plaintexts with average time complexity $2^r|K_m|$ by using Proposition 3.1, where K_m denotes the set of the last round keys.

3.2 Piling-Up Lemma

Matsui used the following lemma in the analysis of the linear attack [8].

Lemma 3.1 (Piling-up Lemma). *For $a_i \in \mathrm{GF}(2)$ with $i = 1, \ldots, l$, suppose that*

$$\bigoplus_{1 \leq i \leq l} a_i = 0 \ .$$

Let a'_i be an independent random element of $\mathrm{GF}(2)$ *such that* $\Pr(a_i = a'_i) \geq \mu$ *for $i = 1, \ldots, l$. Then*

$$\Pr(\textstyle\bigoplus_{1 \leq i \leq l} a'_i = 0) \geq 1/2 + 2^{l-1}(\mu - 1/2)^l \ .$$

4 Proposed Attack

In this section, we show that a Feistel type block cipher is broken even if the round function G is approximated by a low degree vectorial Boolean function. We call this attack the probabilistic higher order differential attack because our attack is a generalization of the higher order differential attack to a probabilistic one.

4.1 Algorithm of Our Attack

In a Feistel type block cipher with block size $2n$, let x_R be kept constant. Then

$$\tilde{y}_R = F(x_L) \tag{2}$$

for some vectorial Boolean function F, where $\tilde{y}_R$ is the right half of the reduced ciphertext. On the other hand, let G be the round function. Then

$$\tilde{y}_R = y_L \oplus G(k_m, y_R) \ ,$$

where $k_m \in K_m$ is the last round key and (y_L, y_R) is the ciphertext. Therefore,

$$\tilde{y}_R = F(x_L) = y_L \oplus G(k_m, y_R) \ . \tag{3}$$

Definition 4.1. *We say that a vectorial Boolean function $F(x)$ is (r, μ)-expressible if there exists a vectorial Boolean function $F'(x)$ such that* $\deg(F'(x)) \leq r$ *and*

$$\Pr_x(F(x) = F'(x)) \geq \mu \ .$$

Now suppose that $F(x_L)$ of eq.(2) is (r, μ)-expressible for any fixed x_R and any fixed key of the reduced cipher. Then the last round key $k_m \in K_m$ can be found by the proposed attack as shown below, where Algorithm 1 is used as a subroutine in Algorithm 2. Let K_m denote the set of the last round keys.

Step 1: Choose $x_R \in \mathrm{GF}(2)^n$ randomly. Choose $w \in \mathrm{GF}(2)^n$ and a full rank $(r+1) \times n$ matrix L over $\mathrm{GF}(2)$ randomly.
Step 2: For all $a \in \mathrm{GF}(2)^{r+1}$, compute the ciphertext $y(a) = (y_L(a), y_R(a))$ of a plaintext $(aL \oplus w, x_R)$.
Step 3: For each $k_i \in K_m$, compute

$$\sigma = \bigoplus_{a \in \mathrm{GF}(2)^{r+1}} y_L(a) \oplus G(k_i, y_R(a)) \ .$$

If $\sigma = (0, \ldots, 0)$, then let $u_i = 1$. Otherwise, let $u_i = 0$.

Fig.1. Algorithm 1

Step 1: Let $T_i = 0$ for $1 \leq i \leq |K_m|$.
Step 2: For $j = 1, \ldots, N$, do:
(a) Run Algorithm 1.
(b) For each $k_i \in K$, let $T_i = T_i + u_i$.
Step 3: Output k_c such that T_c is the maximum.

Fig.2. Algorithm 2

4.2 Analysis of Our Attack

The complexity of our attack is analyzed as follows.

Lemma 4.1. *For $a_i \in \mathrm{GF}(2)^n$ with $i = 1, \ldots, l$, suppose that*

$$\bigoplus_{1 \le i \le l} a_i = (0, \ldots, 0) \ .$$

Let a'_i be an independent random element of $\mathrm{GF}(2)^n$ such that $\Pr(a_i = a'_i) \ge \mu$ for $i = 1, \ldots, l$. Then

$$\Pr(\textstyle\bigoplus_{1 \le i \le l} a'_i = (0, \ldots, 0)) \ge \left(1/2 + 2^{l-1}(\mu - 1/2)^l\right)^n \ .$$

Proof. Denote the j-th bit of a_i as $a_{i,j}$ and the j-th bit of a'_i as $a'_{i,j}$ for $i = 1, \ldots, l$ and $j = 1, \ldots, n$. The equation $\bigoplus_{1 \le i \le l} a'_i = (0, \ldots, 0)$ holds if and only if

$$\bigoplus_{1 \le i \le l} a'_{i,j} = 0$$

holds for $j = 1, \ldots, n$. On the other hand, $\Pr(a_i = a'_i) \ge \mu$ implies that

$$\Pr(a_{i,j} = a'_{i,j}) \ge \mu$$

for $j = 1, \ldots, n$. Then from Lemma 3.1, the result follows. □

We assume that $\{F(aL \oplus w) \mid a = (0, \ldots, 0), \ldots, (1, \ldots, 1)\}$ behaves as independent random 2^{r+1} vectors if L and w are chosen randomly, where L is a full rank $(r+1) \times n$ matrix over $\mathrm{GF}(2)$.

Theorem 4.1. *Suppose that $F(x_L)$ of eq.(2) is (r, μ)-expressible for any fixed x_R and any fixed key of the reduced cipher. If μ is close to one, then the last round key can be found by using $N2^{r+1}$ chosen plaintexts with average time complexity $2^r N|K_m|$ and the success probability*

$$\sum_{1 \le i \le N} \binom{N}{i} p^i (1-p)^{N-i} \left(\sum_{0 \le j \le i-1} \binom{N}{j} 2^{-nj} (1 - 2^{-n})^{N-j} \right)^{|K_m|-1} ,$$

where

$$p = 1 - 2^{r+1} n (1 - \mu) \ .$$

Proof. Since $F(x_L)$ is (r, μ)-expressible, there exists a vectorial Boolean function $F'(x)$ such that $\deg(F'(x)) \le r$ and

$$\Pr_{L,w}(F(aL \oplus w) = F'(aL \oplus w)) \ge \mu \ . \tag{4}$$

First, from Proposition 3.1, it holds that

$$\bigoplus_{a} F'(aL \oplus w) = (0, \ldots, 0) \ . \tag{5}$$

On the other hand, at step 3 of Algorithm 1,

$$\sigma = \bigoplus_a F(aL \oplus w)$$

from eq.(3). Therefore, from eq.(4), eq.(5) and Lemma 4.1, we obtain that

$$\begin{aligned}\Pr_{L,w}(\sigma = (0,\ldots,0)) &= \Pr_{L,w}(\textstyle\bigoplus_a F(aL \oplus w) = (0,\ldots,0)) \\ &\geq \left(1/2 + 2^{2^{r+1}-1}(\mu - 1/2)^{2^{r+1}}\right)^n \quad . \end{aligned} \tag{6}$$

Let $\mu = 1 - \epsilon$, where ϵ is sufficiently small. Then the right hand side of eq.(6) can be approximated as

$$\begin{aligned}\left(1/2 + 2^{2^{r+1}-1}(\mu - 1/2)^{2^{r+1}}\right)^n &\approx \left(1/2 + 1/2(1 - 2 \times 2^{r+1}\epsilon)\right)^n \\ &\approx 1 - 2^{r+1}n\epsilon \\ &= p \quad .\end{aligned}$$

That is,

$$\Pr_{L,w}(\sigma = (0,\ldots,0)) \approx p \quad .$$

Hence, in Algorithm 2, if k_c is the correct key,

$$\Pr_{L,w}(T_c = i) \approx \binom{N}{i} p^i (1-p)^{N-i} \quad .$$

On the other hand, if k_w is a wrong key,

$$\Pr_{L,w}(T_w = j) = \binom{N}{j} 2^{-nj}(1 - 2^{-n})^{N-j}$$

because

$$\Pr_{L,w}(\sigma = (0,\ldots,0)) = 2^{-n} \quad .$$

Consequently,

$$\begin{aligned}&\Pr_{L,w}(T_c = i \text{ and } 0 \leq T_w \leq i-1 \text{ for all } w \neq c) \\ &\quad = \Pr_{L,w}(T_c = i) \Pr_{L,w}(0 \leq T_w \leq i-1 \text{ for all } w \neq c) \\ &\quad \approx \binom{N}{i} p^i (1-p)^{N-i} \left(\sum_{0 \leq j \leq i-1} \binom{N}{j} 2^{-nj}(1 - 2^{-n})^{N-j} \right)^{|K_m|-1} \quad .\end{aligned}$$

Since i ranges from 1 to N, the result follows. □

Our experiment shows that if $N = \lceil p^{-2} \rceil$, then the success probability is larger than 90 %.

4.3 Example

We show a block cipher such that it is broken by the proposed attack, but not broken by the higher order differential attack.

$\mathcal{KN}$ cipher developed by Knudsen and Nyberg is provably secure against the differential attack and the linear attack [6]. It is a 6 round Feistel cipher such that $n = 32$ and the round function G is given by

$$G(k, x) = d(f(e(x) \oplus k)) \ ,$$

where $f(x) = x^3$ over GF(2^{33}), $d : \{0,1\}^{33} \to \{0,1\}^{32}$ discards one bit from its argument and

$$e(x_1, \ldots, x_{32}) = (x_1, \ldots, x_{32}, a_1 x_1 \oplus \cdots \oplus a_{32} x_{32})$$

for some $a_1, \ldots, a_{32}$. Since $\deg(G) = 2$, $\mathcal{KN}$ cipher is broken with 512 chosen plaintext and 2^{41} complexity by the higher order differential attack [4].

Now consider a slight modification of $\mathcal{KN}$ cipher. Let the round function be

$$G'(k, x) = d(f(e'(x) \oplus k)) \ ,$$

where

$$e'(x_1, \ldots, x_{32}) = (x_1, \ldots, x_{32}, x_1 \cdots x_{32}) \ .$$

We call this cipher $\mathcal{KN}'$ cipher. Then $\mathcal{KN}'$ cipher cannot be broken by the higher order differential attack because $\deg(G') = 32$ which is very large.

However, it is broken by the proposed attack as follows. First, G' is $(2, 1 - 2^{-32})$-expressible. Therefore, F of eq.(2) is $(2^3, (1 - 2^{-32})^3)$-expressible. Now from Theorem 4.1, for $N = 2$, the last round key can be found with 2^{10} chosen plaintexts, 2^{42} complexity and the success probability almost 100%, where $p \approx 0.99$.

5 Higher Order Bent Function

In this section, we introduce a notion of higher order bent functions in order to prevent our attack. We then present their explicit constructions which satisfy some other cryptographic criteria as well.

5.1 Higher Order Nonlinearity

The truth table of a Boolean function $f(x)$ is defined as $(f(\alpha_0), \ldots, f(\alpha_{2^n-1}))$, where α_i is a vector of length n representing i in binary. For two Boolean functions $f(x)$ and $g(x)$, let $d(f(x), g(x))$ denote the Hamming distance between $(f(\alpha_0), \ldots, f(\alpha_{2^n-1}))$ and $(g(\alpha_0), \ldots, g(\alpha_{2^n-1}))$.

Let $B^{(r)}(x)$ denote the set of Boolean functions with degree at most r for $0 \le r \le n$. That is,

$$B^{(r)}(x) = \{a_0 \oplus \bigoplus_{1 \le i \le n} a_i x_i \oplus \cdots \oplus \bigoplus_{1 \le i_1 < \cdots < i_r \le n} a_{i_1, \ldots, i_r} x_{i_1} \cdots x_{i_r}\} \ .$$

Now we define the r-th order nonlinearity of a Boolean function $f(x)$ as follows.

Definition 5.1. *Let*

$$N_f^{(r)} \stackrel{\triangle}{=} \min_{g(x)\in B^{(r)}(x)} d(f(x), g(x))$$

for $0 \le r \le n$. *We say that* $N_f^{(r)}$ *is the* r*-th order nonlinearity of* $f(x)$.

Note that the well known nonlinearity of $f(x)$ is equivalent to $N_f^{(1)}$.

We next show that $N_f^{(r)}$ is closely related to the covering radius of the r-th order Reed-Muller code.

Definition 5.2. *[7] The* r*-th order Reed-Muller code* $\mathcal{R}(r,n)$ *of length* 2^n, *for* $0 \le r \le n$, *is the set of the truth table of a Boolean function* $f(x)$ *such that* $\deg(f) \le r$.

The covering radius of $\mathcal{R}(r,n)$ is defined as

$$\rho(r,n) \stackrel{\triangle}{=} \max_{v\in\{0,1\}^{2^n}} \min_{u\in\mathcal{R}(r,n)} d(v,u) \ .$$

Proposition 5.1. *[2] If* $0 \le r \le n-3$, *then*

$$\rho(r,n) \ge \begin{cases} 2^{n-r-3}(r+4) & \text{if } r \text{ is even} \ , \\ 2^{n-r-3}(r+5) & \text{if } r \text{ is odd} \ . \end{cases}$$

Theorem 5.1.

$$\max_{f(x)} N_f^{(r)} = \rho(r,n) \ .$$

Proof. From the definition of the r-th order nonlinearity $N_f^{(r)}$,

$$\max_{f(x)} N_f^{(r)} = \max_{f(x)} \min_{g(x)\in B^{(r)}(x)} d(f(x), g(x)) \ .$$

Since $B^{(r)} = \{u \mid u \in \mathcal{R}(r,n)\}$, we have

$$\begin{aligned} \max_{f(x)} \min_{g(x)\in B^{(r)}(x)} d(f(x), g(x)) &= \max_{v\in\{0,1\}^{2^n}} \min_{u\in\mathcal{R}(r,n)} d(v,u) \\ &= \rho(r,n) \ . \end{aligned}$$

□

5.2 Higher Order Bent Function

We then define r-th order bent functions based on Theorem 5.1 and Proposition 5.1 as follows.

Definition 5.3. *We say that $f(x)$ is an r-th order bent function if*

$$N_f^{(r)} \geq \begin{cases} 2^{n-r-3}(r+4) & \text{if } r \text{ is even} \\ 2^{n-r-3}(r+5) & \text{if } r \text{ is odd} \end{cases} .$$

for $0 \leq r \leq n-3$.

(A well known bent function is also a 1-st order bent function. However, the converse is not true.)

5.3 Basic Construction

In what follows, let $x = (x_1, \ldots, x_n)$ and $x' = (x_1, \ldots, x_{n-1})$. For a Boolean function $f(x)$, let

$$f_1(x') \stackrel{\triangle}{=} f(x', 0) \text{ and } f_2(x') \stackrel{\triangle}{=} f(x', 1) .$$

Lemma 5.1.

$$N_f^{(r)} \geq N_{f_1}^{(r)} + N_{f_2}^{(r)} .$$

Proof.

$$\begin{aligned} N_f^{(r)} &= \min_{g(x) \in B^{(r)}(x)} d(f(x), g(x)) \\ &= \min_{g(x) \in B^{(r)}(x)} d(f(x', 0), g(x', 0)) + d(f(x', 1), g(x', 1)) \\ &\geq \min_{g_1(x') \in B^{(r)}(x')} d(f_1(x'), g_1(x')) + \min_{g_2(x') \in B^{(r)}(x')} d(f_2(x'), g_2(x')) \\ &= N_{f_1}^{(r)} + N_{f_2}^{(r)} . \end{aligned}$$

□

Lemma 5.2. *If $f_1(x') = f_2(x')$, then*

$$N_f^{(r)} = 2N_{f_1}^{(r)} .$$

Proof. First $N_f^{(r)} \geq 2N_{f_1}^{(r)}$ from Lemma 5.1. Next choose $g'(x') \in B^{(r)}(x')$ such that

$$d(f_1(x'), g'(x')) = N_{f_1}^{(r)}$$

arbitrarily. Define $g(x)$ as $g(x) = g'(x')$. Then

$$\begin{aligned} 2N_{f_1}^{(r)} &= N_{f_1}^{(r)} + N_{f_2}^{(r)} \\ &= d(f_1(x'), g'(x')) + d(f_2(x'), g'(x')) \\ &= d(f(x', 0), g(x', 0)) + d(f(x', 1), g(x', 1)) \\ &= d(f(x), g(x)) \\ &\geq \min_{g(x) \in B^{(r)}(x)} d(f(x), g(x)) \\ &= N_f^{(r)} \end{aligned}$$

because $g(x) \in B^{(r)}(x)$. Therefore, $N_f^{(r)} = 2N_{f'}^{(r)}$. □

Let

$$\sigma^{(r)}(x) = \bigoplus_{1 \leq i_1 < \cdots < i_r \leq n} x_{i_1} \cdots x_{i_r} \ .$$

for $0 \leq r \leq n$. Then McLoughlin showed a lower bound on $\rho(n-3, 3)$ by using $\sigma^{(r)}(x)$ [9]. It can be restated as follows.

Proposition 5.2. *$\sigma^{(n-2)}(x)$ is an $(n-3)$-th order bent function for $n \geq 3$.*

Now we show our basic construction of r-th order bent functions.

Theorem 5.2. *Let*

$$f(x_1, \ldots, x_n) = \sigma^{(r+1)}(x_1, \ldots, x_{r+3}) \ .$$

Then $f(x)$ is an r-th order bent function for $0 \leq r \leq n-3$.

Proof. By using Lemma 5.2 repeatedly $n - r - 3$ times, we have

$$N_f^{(r)} = 2^{n-r-3} N_{\sigma^{(r+1)}}^{(r)} \ .$$

Then from Proposition 5.2, we see that

$$N_f^{(r)} \geq \begin{cases} 2^{n-r-3}(r+4) & \text{if } r \text{ is even} \ , \\ 2^{n-r-3}(r+5) & \text{if } r \text{ is odd} \ . \end{cases}$$

□

5.4 Improved Construction (I)

The r-th order bent function obtained from Theorem 5.2 is cryptographically weak since it is not balanced and $x_{r+4}, \ldots, x_n$ do not appear in $f(x)$. In what follows, we show some improved constructions.

Definition 5.4. *A Boolean function $f(x)$ is balanced if*

$$|\{x \mid f(x) = 0\}| = |\{x \mid f(x) = 1\}| \ .$$

Definition 5.5. *A Boolean function $f(x)$ satisfies SAC if*

$$f(x) \oplus f(x \oplus \alpha)$$

is balanced for any α such that the Hamming weight of α is equal to 1.

Lemma 5.3. *If $\deg(f(x)) > r$ and $\deg(h(x)) \leq r$, then*

$$N_f^{(r)} = N_{f \oplus h}^{(r)} \ .$$

Proof.

$$\begin{aligned} N_{f \oplus h}^{(r)} &= \min_{g(x) \in B^{(r)}(x)} d(f(x) \oplus h(x), g(x)) \\ &= \min_{g(x) \in B^{(r)}(x)} d(f(x), g(x) \oplus h(x)) \\ &= \min_{g(x) \in B^{(r)}(x)} d(f(x), g(x)) \\ &= N_f^{(r)} \ . \end{aligned}$$

□

By using Lemma 5.3, we can prove the following theorems. The proofs will be given in the final paper.

Theorem 5.3. *Suppose that $r + 3 < n$. Let*

$$f(x_1, \ldots, x_n) = \sigma^{(r+1)}(x_1, \ldots, x_{r+3}) \oplus x_{r+4} \oplus \cdots \oplus x_n \ .$$

Then $f(x)$ is a balanced r-th order bent function.

Theorem 5.4. *Suppose $2 \leq r \leq n - 3$. Let*

$$f(x_1, \ldots, x_n) = \sigma^{(r+1)}(x_1, \ldots, x_{r+3}) \oplus (x_1 \oplus \cdots \oplus x_{r+3})(x_{r+4} \oplus \cdots \oplus x_n) \ .$$

Then $f(x)$ is an r-th order bent function which satisfies SAC.

Theorem 5.5. *There exist r-th order bent functions which satisfy PC(l) of order k.*

5.5 Improved Construction (II)

Next we show r-th order bent functions such that each x_i is involved in a large degree term.

Lemma 5.4. *For any r, let*

$$\begin{cases} s_n(x_1, \ldots, x_n) \stackrel{\triangle}{=} \sigma^{(r+1)}(x_1, \ldots, x_n) \ , \\ s_{n-1}(x_1, \ldots, x_{n-1}) \stackrel{\triangle}{=} \sigma^{(r+1)}(x_1, \ldots, x_{n-1}) \ . \end{cases}$$

Then,

$$N_{s_n}^{(r)} \geq 2N_{s_{n-1}}^{(r)} \ .$$

Proof. Note that

$$\begin{aligned}\sigma^{(r+1)}(x',0) &= \sigma^{(r+1)}(x') \\ &= s_{n-1}(x') \ , \\ \sigma^{(r+1)}(x',1) &= \sigma^{(r+1)}(x') \oplus \sigma^{(r)}(x') \\ &= s_{n-1}(x') \oplus \sigma^{(r)}(x') \ .\end{aligned}$$

Then from Lemma 5.1 and Lemma 5.3,

$$\begin{aligned}N_{s_n}^{(r)} &\geq N_{s_{n-1}}^{(r)} + N_{s_{n-1}}^{(r)} \\ &= 2N_{s_{n-1}}^{(r)} \ .\end{aligned}$$

□

Theorem 5.6. *Let*

$$f(x_1,\ldots,x_n) \stackrel{\triangle}{=} \sigma^{(r+1)}(x_1,\ldots,x_n) \ .$$

Then $f(x)$ is an r-th order bent function for $0 \leq r \leq n-3$.

Proof. Let

$$s_{r+3}(x_1,\ldots,x_{r+3}) \stackrel{\triangle}{=} \sigma^{(r+1)}(x_1,\ldots,x_{r+3}) \ .$$

Then by using Lemma 5.4 repeatedly $n-r-3$ times, we have

$$N_f^{(r)} \geq 2^{n-r-3} N_{s_{r+3}}^{(r)} \ .$$

Finally from Proposition 5.2, we see that

$$N_f^{(r)} \geq \begin{cases} 2^{n-r-3}(r+4) & \text{if } r \text{ is even} \ , \\ 2^{n-r-3}(r+5) & \text{if } r \text{ is odd} \ . \end{cases}$$

Therefore, $f(x)$ is an r-th order bent function. □

Note that each x_i is involved in a term of degree $(r+1)$ in the above f.

References

1. E.Biham and A.Shamir. Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, 1993. 62
2. G.D.Cohen, M.G.Karpovsky, H.F.Mattson,Jr. and J.R.Schatz. Covering Radius — Survey and Recent Results. In *IEEE Transactions on Information Theory*, volume 31, Number 3, pages 328–343, 1985. 69
3. T.Jakobsen. Cryptanalysis of block ciphers with probabilistic non-linear relations of low degree. In *Advances in Cryptology — CRYPTO' 98 Proceedings*, volume 1462 of *Lecture Notes in Computer Science*, pages 212–222, Springer-Verlag, 1998. 62
4. T.Jakobsen and L.R.Knudsen. The interpolation attack on block ciphers. In *Fast Software Encryption*, volume 1267 of *Lecture Notes in Computer Science*, pages 28–40, Springer-Verlag, January 1997. 62, 64, 68

5. X. Lai. Higher order derivatives and differential cryptanalysis. In *Proceedings of Symposium on Communication, Coding and Cryptography, in honor of James L. Massey on the occasion of his 60'th birthday*, February 10–13, 1994, Monte-Verita, Ascona, Switzerland, 1994. 64
6. K.Nyberg and L.R.Knudsen. Provable security against a differential attack. In *Journal of Cryptology*, volume 8, number 1, pages 27–37, Winter 1995. 68
7. F.J.MacWilliams and N.J.A.Sloane. The theory of error-correcting codes. North-Holland, 1977. 69
8. M.Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology — EUROCRYPT' 93 Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397, Springer-Verlag, 1993. 64
9. A.M.McLoughlin. The covering radius of the $(m-3)$-rd order Reed-Muller codes and lower bounds on the $(m-4)$-th order Reed-Muller codes. In *SIAM Journal of Applied Mathematics*, volume 37, number 2, October 1979. 71
10. J.Pieprzyk and G.Finkelstein. Towards effective nonlinear cryptosystem design. In *IEE Proceedings Part E*, volume 35, number 6, pages 325–335, November 1988.