New Covering Radius of Reed-Muller Codes for t-Resilient Functions

Tetsu Iwata[1], Takayuki Yoshiwara[1], and Kaoru Kurosawa[2]

[1] Department of Communications and Integrated Systems,
Tokyo Institute of Technology,
2-12-1 O-okayama, Meguro-ku, Tokyo 152-8552, Japan
tez@ss.titech.ac.jp
[2] Department of Computer and Information Sciences,
Ibaraki University,
4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan
kurosawa@cis.ibaraki.ac.jp

Abstract. In stream ciphers, we should use a t-resilient Boolean function $f(X)$ with large nonlinearity to resist fast correlation attacks and linear attacks. Further, in order to be secure against an *extension* of linear attacks, we wish to find a t-resilient function $f(X)$ which has a large distance even from low degree Boolean functions. From this point of view, we define a new covering radius $\hat{\rho}(t, r, n)$ as the maximum distance between a *t-resilient* function $f(X)$ and the r-th order Reed-Muller code $RM(r, n)$. We next derive its lower and upper bounds. Finally, we present a table of numerical bounds for $\hat{\rho}(t, r, n)$.

Keywords: Nonlinearity, t-resilient function, Reed-Muller code, covering radius, stream cipher.

1 Introduction

Nonlinearity and resiliency are two of the most important cryptographic criteria of Boolean functions which are used in stream ciphers and block ciphers. The nonlinearity of a Boolean function $f(X)$, denoted by $nl(f)$, is the distance between $f(X)$ and the set of affine (linear) functions. It must be large to avoid linear attacks.

$f(X)$ is said to be balanced if $\#\{X \mid f(X) = 0\} = \#\{X \mid f(X) = 1\} = 2^{n-1}$, where $X = (x_1, \ldots, x_n)$. Suppose that $f(X)$ is balanced even if any t variables $x_{i_1}, \ldots, x_{i_t}$ are fixed to any t values $b_{i_1}, \ldots, b_{i_t}$. Then $f(X)$ is called a t-resilient function. $f(X)$ should be t-resilient for large t to resist fast correlation attacks in stream ciphers such as combination generators and nonlinear filter generators.

Therefore, $f(X)$ should satisfy both large nonlinearity $nl(f)$ and large resiliency. Recently, Sarkar and Maitra derived an upper bound on $nl(f)$ of t-resilient functions [5].

We further observe that $f(X)$ should not be approximated even by low degree Boolean functions $g(X)$ in order to be secure against an *extension* of linear

S. Vaudenay and A. Youssef (Eds.): SAC 2001, LNCS 2259, pp. 75–86, 2001.

attacks [3]. Note that the set of n variable Boolean functions $g(X)$ such that $\deg(g) \leq r$ is identical to an error correcting code known as the r-th order Reed-Muller code $RM(r, n)$.

Consequently, we wish to find a t-resilient function $f(X)$ which has a large distance even from $RM(r, n)$ for small r. On the other hand, the covering radius of $RM(r, n)$, denoted by $\rho(r, n)$, is defined as the maximum distance between $f(X)$ and $RM(r, n)$, where the maximum is taken over *all* n variable Boolean functions $f(X)$. That is,

$$\rho(r, n) \stackrel{\text{def}}{=} \max_{f(X)} d(f(X), RM(r, n)).$$

In this paper, we introduce a new definition of covering radius of $RM(r, n)$ from this point of view. We define *t-resilient covering radius* of $RM(r, n)$, denoted by $\hat{\rho}(t, r, n)$, as the maximum distance between a t-resilient function $f(X)$ and $RM(r, n)$, where the maximum is taken over all *t-resilient functions* $f(X)$. That is,

$$\hat{\rho}(t, r, n) \stackrel{\text{def}}{=} \max_{t\text{-resilient } f(X)} d(f(X), RM(r, n)).$$

We then derive lower bounds and upper bounds on $\hat{\rho}(t, r, n)$. The result of Sarkar and Maitra [5] is obtained as a special case of one of our upper bounds. Finally, we present a table of numerical bounds for $\hat{\rho}(t, r, n)$ which are derived from our bounds.

2 Preliminaries

Let $X = (x_1, \ldots, x_n)$.

2.1 Nonlinearity of Boolean Functions

Define the distance between two Boolean functions $f(X)$ and $g(X)$ as

$$d(f(X), g(X)) \stackrel{\text{def}}{=} \#\{X \mid f(X) \neq g(X)\} \ .$$

Define the weight of $f(X)$ as

$$w(f) \stackrel{\text{def}}{=} \#\{X \mid f(X) = 1\} \ .$$

A Boolean function such that $a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n$ is called an affine function. Let A_n denote the set of n variable affine functions. That is,

$$A_n \stackrel{\text{def}}{=} \{a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n\} \ .$$

The nonlinearity of $f(X)$, denoted by $nl(f)$, is defined as the distance between $f(X)$ and A_n. That is,

$$nl(f) \stackrel{\text{def}}{=} \min_{g(X) \in A_n} d(f(X), g(X)) \ .$$

Cryptographically secure Boolean functions should have large nonlinearity to resist linear attacks. Then the following upper bound is known.

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1} \ .$$

It is tight if $n = even$. $f(X)$ which satisfies the above equality is called a bent function.

2.2 t-Resilient Function and its Nonlinearity

$f(X)$ is said to be balanced if

$$\#\{X \mid f(X) = 1\} = \#\{X \mid f(X) = 0\} = 2^{n-1} \ .$$

Suppose that $f(X)$ is balanced even if any t variables $x_{i_1}, \ldots, x_{i_t}$ are fixed to any values $b_{i_1}, \ldots, b_{i_t}$. Then $f(X)$ is called a t-resilient function. Boolean functions used in stream ciphers should be t-resilient for large t to resist fast correlation attacks.

Therefore, $f(X)$ should satisfy both large nonlinearity $nl(f)$ and large resiliency. Sarkar and Maitra derived an upper bound on $nl(f)$ of t-resilient functions [5].

Proposition 2.1. *Let $f(X)$ be a t-resilient function and $l(X)$ be an affine function. Then*

$$d(f(X), l(X)) \equiv 0 \bmod 2^{t+1}.$$

Proposition 2.2. *Suppose that $f(X)$ is a t-resilient function. If $n = even$, then*

$$nl(f) \leq \begin{cases} 2^{n-1} - 2^{t+1} & \text{if } t+1 > n/2-1 \\ 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{t+1} & \text{if } t+1 \leq n/2-1 \end{cases}$$

They derived a similar bound for $n = odd$.

3 Reed-Muller Code and Its Covering Radius

Any Boolean function is written as the algebraic normal form such that

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

The degree of $g(X)$, denoted by $\deg(g)$, is the degree of the highest degree term in the algebraic normal form. The r-th order Reed-Muller code $RM(r, n)$ is identical to the set of n-variable Boolean function $g(X)$ such that $\deg(g) \leq r$.

The covering radius of $RM(r, n)$, denoted by $\rho(r, n)$, is defined as the maximum distance between $f(X)$ and $RM(r, n)$, where the maximum is taken over all n variable Boolean functions $f(X)$. That is,

$$\rho(r, n) \stackrel{\text{def}}{=} \max_{f(X)} d(f(X), RM(r, n)),$$

where

$$d(f(X), RM(r,n)) \stackrel{\text{def}}{=} \min_{\deg(g) \le r} d(f(X), g(X)).$$

Note that $\rho(1,n)$ is equal to the maximum nonlinearity of n-variable Boolean functions.

In the following table, the best known numerical bounds for $\rho(r,n)$ with $n \le 7$ are presented.

n	1	2	3	4	5	6	7
$r=1$	0	1	2	$6^{[4]}$	12	28	56
$r=2$		0	1	2	$6^{[4]}$	$18^{[6]}$	$40^{[1]}$-$44^{[2]}$
$r=3$			0	1	2	$8^{[4]}$	$20^{[1]}$-$23^{[1]}$
$r=4$				0	1	2	$8^{[4]}$
$r=5$					0	1	2
$r=6$						0	1
$r=7$							0

It is easy to see the following propositions.

Proposition 3.1. *Any Boolean function* $f(x_1, \ldots, x_n)$ *such that* $\deg(f) \le r$ *is written as*

$$f(X) = f_1(x_1, \ldots, x_{n-1}) \oplus x_n \cdot f_2(x_1, \ldots, x_{n-1}) \ ,$$

where $\deg(f_1) \le r$ *and* $\deg(f_2) \le r-1$.

Proposition 3.2. $d(f, g \oplus h) \ge d(f,g) - w(h)$.

Proof.

$$\begin{aligned} d(f, g \oplus h) &= w(f \oplus g \oplus h) \\ &\ge w(f \oplus g) - w(h) \\ &= d(f,g) - w(h) \end{aligned}$$

□

4 New Covering Radius for t-Resilient Functions

4.1 New Covering Radius

Boolean functions $f(X)$ used in stream ciphers and block ciphers should not be approximated by affine (linear) functions to resist linear attacks. This leads to the notion of the nonlinearity $nl(f)$ which is defined as the distance between $f(X)$ and the set of affine (linear) functions.

We also observe that $f(X)$ should not be approximated even by low degree Boolean functions to resist an extension of linear attacks [3]. Remember that

$RM(r,n)$ is identical to the set of $g(X)$ such that $\deg(g) \leq r$, and the covering radius of $RM(r,n)$ is the maximum distance between $f(X)$ and $RM(r,n)$. That is,

$$\rho(r,n) = \max_{f(X)} d(f(X), RM(r,n)).$$

Further, $f(X)$ should be t-resilient to be secure against fast correlation attacks in stream ciphers.

In this section, we introduce a new definition of covering radius of $RM(r,n)$ from this point of view. We define *t-resilient covering radius* of $RM(r,n)$, denoted by $\hat{\rho}(t,r,n)$, as the maximum distance between a t-resilient function $f(X)$ and $RM(r,n)$, where the maximum is taken over all *t-resilient functions* $f(X)$. That is,

$$\hat{\rho}(t,r,n) \stackrel{\text{def}}{=} \max_{t\text{-resilient } f(X)} d(f(X), RM(r,n)).$$

Note that $\hat{\rho}(t,r,n) = 0$ if $n - t - 1 \leq r$. This follows immediately from Siegenthalar's inequality on resilient functions [7].

We then derive lower bounds and upper bounds on $\hat{\rho}(t,r,n)$.

4.2 Lower Bounds on $\hat{\rho}(t,r,n)$

In this subsection, we derive lower bounds on $\hat{\rho}(t,r,n)$.

Theorem 4.1.

$$\hat{\rho}(t,r,n) \geq \begin{cases} 2\rho(r,n-1) & \text{if } t = 0 \\ 2\hat{\rho}(t-1,r,n-1) & \text{if } t \geq 1 \end{cases}$$

Proof. **(1)** $t = 0$**.** Suppose that $\rho(r,n-1)$ is achieved by $f'(x_1,\ldots,x_{n-1})$. That is,

$$d(f', RM(r,n-1)) = \rho(r,n-1) \ .$$

Let $f(x_1,\ldots,x_n) = f'(x_1,\ldots,x_{n-1}) \oplus x_n$. Then it is easy to see that $f(x_1,\ldots,x_n)$ is balanced. Therefore, $f(X)$ is a 0-resilient function. Further,

$$\begin{aligned} \hat{\rho}(t,r,n) &\geq d(f, RM(r,n)) \\ &= d(f', RM(r,n-1)) + d(f', RM(r,n-1)) \\ &= 2\rho(r,n-1) \end{aligned}$$

(2) $t \geq 1$**.** Suppose that $\hat{\rho}(t-1,r,n-1)$ is achieved by a $(t-1)$-resilient function $f'(x_1,\ldots,x_{n-1})$. That is,

$$d(f', RM(r,n-1)) = \hat{\rho}(t-1,r,n-1) \ .$$

Let $f(x_1,\ldots,x_n) = f'(x_1,\ldots,x_{n-1}) \oplus x_n$. Then it is easy to see that $f(x_1,\ldots,x_n)$ is a t-resilient function. The rest of the proof is similar to the above.

□

Corollary 4.1. $\hat{\rho}(t, r, n) \geq 2^{t+1}\rho(r, n-t-1)$.

Theorem 4.2. *Suppose that there exists* $f(x_1, \ldots, x_n)$ *such that*

$$d(f, RM(r, n)) \geq k$$

and

$$f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_m) \oplus f_2(x_l, \ldots, x_n)$$

for some f_1 *and* f_2*, where* $1 \leq m \leq n-1$*,* $2 \leq l \leq n-1$*. Let*

$$t = \min(n-m-1, l-2).$$

Then

$$\hat{\rho}(t, r+1, n+1) \geq k.$$

Proof. Let

$$\begin{cases} h_1(x_1, \ldots, x_n) \stackrel{\text{def}}{=} f_1(x_1, \ldots, x_m) \oplus x_{m+1} \oplus \cdots \oplus x_n \\ h_2(x_1, \ldots, x_n) \stackrel{\text{def}}{=} x_1 \oplus \cdots \oplus x_{l-1} \oplus f_2(x_l, \ldots, x_n) \end{cases}$$

It is easy to see that $h_1(X)$ is $(n-m-1)$-resilient and $h_2(X)$ is $(l-2)$-resilient. Then define

$$h(X, x_{n+1}) \stackrel{\text{def}}{=} h_1(X) \oplus x_{n+1} \cdot (h_1(X) \oplus h_2(X)) \ ,$$

where $X = (x_1, \ldots, x_n)$.

We first show that h is t-resilient. For $x_{n+1} = 0$,

$$h(X, 0) = h_1(X)$$

which is $(n-m-1)$-resilient. For $x_{n+1} = 1$,

$$h(X, 1) = h_2(X)$$

which is $(l-2)$-resilient. Therefore, $h(X, x_{n+1})$ is t-resilient, where $t = \min(n-m-1, l-2)$.

We next prove that $d(h, RM(r+1, n+1)) \geq k$. Choose $g(X, x_{n+1})$ such that $\deg(g) \leq r+1$ and

$$d(h, g) = d(h, RM(r+1, n+1)) \ .$$

From Proposition 3.1, g is written as

$$g(X, x_{n+1}) = g_1(X) \oplus x_{n+1} \cdot g_2(X)$$

for some $g_1 \in RM(r+1, n)$ and $g_2 \in RM(r, n)$. Then from Proposition 3.2,

$$\begin{aligned} d(h, g) &= d(h, g)|_{x_{n+1}=0} + d(h, g)|_{x_{n+1}=1} \\ &= d(h_1, g_1) + d(h_2, g_1 \oplus g_2) \\ &= d(h_1, g_1) + d(h_1 \oplus h_2, h_1 \oplus g_1 \oplus g_2) \\ &\geq d(h_1, g_1) + d(h_1 \oplus h_2, g_2) - w(h_1 \oplus g_1) \\ &= d(h_1 \oplus h_2, g_2) \end{aligned}$$

Let $l(X) \stackrel{\text{def}}{=} x_1 \oplus \cdots \oplus x_{l-1} \oplus x_{m+1} \oplus \cdots \oplus x_n$. Then

$$\begin{aligned} d(h,g) &\geq d(h_1 \oplus h_2, g_2) \\ &= d(f_1 \oplus f_2 \oplus l, g_2) \\ &= d(f_1 \oplus f_2, g_2 \oplus l) \\ &\geq d(f, RM(r,n)) \end{aligned}$$

because $g_2 \in RM(r,n)$ and $g_2 \oplus l \in RM(r,n)$. Hence

$$\begin{aligned} d(h, RM(r+1, n+1)) &= d(h,g) \\ &\geq d(f, RM(r,n)) \\ &\geq k \end{aligned}$$

□

Corollary 4.2. $\hat{\rho}(0,3,7) \geq 18$.

Proof. Let

$$f(x_1, \ldots, x_6) = (x_1x_2x_3 \oplus x_1x_4x_5) \oplus (x_2x_3x_6 \oplus x_2x_4x_6 \oplus x_3x_5x_6) \ .$$

Then it is known that [6]

$$d(f, RM(2,6)) = 18 \ .$$

Let $r = 2$, $n = 6$, $m = 5$ and $l = 2$ in Theorem 4.2. Then we obtain this corollary. □

Corollary 4.3. *Suppose that $n = 4k + s$, where $0 \leq s \leq 3$ and $k \geq 1$. Let $t = 2k - 1$. Then*

$$\hat{\rho}(t, 2, n+1) \geq \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1} & \text{if } n = even \\ 2^{n-1} - 2^{\frac{n-1}{2}} & \text{if } n = odd \end{cases}$$

Proof. For $n = even$, let

$$f(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-1}x_n \ .$$

Then it is known that

$$d(f, RM(1,n)) = 2^{n-1} - 2^{\frac{n}{2}-1}$$

(f is a bent function). In Theorem 4.2, let

$$\begin{cases} f_1(x_1, \ldots, x_{2k}) = x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k}, \\ f_2(x_{2k+1}, \ldots, x_n) = x_{2k+1}x_{2k+2} \oplus \cdots \oplus x_{n-1}x_n \end{cases}$$

Then $m = 2k$ and $l = 2k + 1$. Hence

$$\begin{aligned} t &= \min(n - 2k - 1, 2k + 1 - 2) \\ &= \min(4k + s - 2k - 1, 2k - 1) \\ &= 2k - 1 \end{aligned}$$

because $s \geq 0$.

For $n = odd$, let

$$f(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-2}x_{n-1} \ .$$

Then for any $g(x_1, \ldots, x_n)$ such that $\deg(g) \leq 1$,

$$\begin{aligned} d(f, g) &= d(f, g)|_{x_n=0} + d(f, g)|_{x_n=1} \\ &\geq d(f, RM(1, n-1)) + d(f, RM(1, n-1)) \\ &= 2\left(2^{n-2} - 2^{\frac{n-1}{2}-1}\right) \\ &= 2^{n-1} - 2^{\frac{n-1}{2}} \end{aligned}$$

Hence

$$d(f, RM(1, n)) \geq 2^{n-1} - 2^{\frac{n-1}{2}} \ .$$

Finally similarly to $n = even$, we have $t = 2k - 1$.

Therefore, this corollary holds from Theorem 4.2. □

4.3 Upper Bounds on $\hat{\rho}(t, r, n)$

In this subsection, we derive upper bounds on $\hat{\rho}(t, r, n)$.

Theorem 4.3. *For $t \geq 1$,*

$$\hat{\rho}(t, r, n) \leq \hat{\rho}(t-1, r, n-1) + \rho(r-1, n-1) \ .$$

Proof. Any $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ are written as

$$\begin{cases} f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_{n-1}) \oplus x_n \cdot f_2(x_1, \ldots, x_{n-1}), \\ g(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_{n-1}) \oplus x_n \cdot g_2(x_1, \ldots, x_{n-1}). \end{cases}$$

Then

$$\begin{aligned} d(f, g) &= d(f, g)|_{x_n=0} + d(f, g)|_{x_n=1} \\ &= d(f_1, g_1) + d(f_1 \oplus f_2, g_1 \oplus g_2) \\ &= d(f_1, g_1) + d(f_1 \oplus f_2 \oplus g_1, g_2) \end{aligned}$$

Now let f be any t-resilient function such that

$$d(f, RM(r, n)) = \hat{\rho}(t, r, n) \ . \tag{1}$$

Choose g_1 such that $\deg(g_1) \leq r$ and

$$d(f_1, g_1) = d(f_1, RM(r, n-1))$$

arbitrarily. Choose g_2 such that $\deg(g_2) \leq r - 1$ and

$$d(f_1 \oplus f_2 \oplus g_1, g_2) = d(f_1 \oplus f_2 \oplus g_1, RM(r-1, n-1))$$

arbitrarily. Then

(1). $\deg(g) \leq r$. Therefore,

$$d(f,g) \geq d(f, RM(r,n)) = \hat{\rho}(t,r,n) \ .$$

(2). f_1 is $(t-1)$-resilient. Therefore,

$$d(f_1,g_1) = d(f_1, RM(r,n-1)) \leq \hat{\rho}(t-1,r,n-1) \ .$$

(3). It is easy to see

$$d(f_1 \oplus f_2 \oplus g_1, g_2) \leq \rho(r-1,n-1) \ .$$

Therefore,

$$\begin{aligned} \hat{\rho}(t,r,n) &\leq d(f,g) \\ &= d(f_1,g_1) + d(f_1 \oplus f_2 \oplus g_1, g_2) \\ &\leq \hat{\rho}(t-1,r,n-1) + \rho(r-1,n-1) \ . \end{aligned}$$

□

Lemma 4.1. *Suppose that $f(X)$ is balanced and $\deg(g(X)) \leq n-1$, where $X = (x_1, \ldots, x_n)$. Then*

$$d(f,g) \equiv 0 \bmod 2 \ .$$

Proof. Note that

$$d(f,g) = w(f) + w(g) - 2w(f \times g) \ .$$

Since $\deg(g) \leq n-1$, it holds that $w(g) \equiv 0 \bmod 2$. Therefore, it holds that $d(f,g) \equiv 0 \bmod 2$. □

We finally generalize Proposition 2.1 [5] and Proposition 2.2 [5].

Theorem 4.4. *Let $1 \leq r \leq n-2$ and $0 \leq t \leq n-r-2$. If $f(x_1, \ldots, x_n)$ is a t-resilient function, then*

$$d(f, RM(r,n)) \equiv 0 \bmod 2^{\lfloor \frac{t}{r} \rfloor + 1} \ .$$

Proof. We show that

$$d(f(X), g(X)) \equiv 0 \bmod 2^{\lfloor \frac{t}{r} \rfloor + 1} \tag{2}$$

for any $g(X)$ such that $\deg(g) \leq r$, where $X = (x_1, \ldots, x_n)$. Let $\alpha(g,r)$ be the number of degree r terms $x_{i_1} \cdots x_{i_r}$ involved in g.

Base step on r. If $r = 1$, then the theorem follows from Proposition 2.1.

Inductive step on r. Assume that (2) is true for $r = r_0$. We will show that it is true for $r = r_0 + 1$.

Base step on $\alpha(g, r_0+1)$. If $\alpha(g, r_0+1) = 0$, then $g(x_1, \ldots, x_n) \in RM(r_0, n)$. By an induction hypothesis on r, we have

$$\begin{aligned} d(f,g) &\equiv 0 \bmod 2^{\lfloor \frac{t}{r_0} \rfloor + 1} \\ &\equiv 0 \bmod 2^{\lfloor \frac{t}{r_0+1} \rfloor + 1} \ . \end{aligned}$$

Inductive step on $\alpha(g, r_0{+}1)$. Assume that (2) is true for $\alpha(g, r_0{+}1) \leq \alpha_0$. We show that (2) is true for $\alpha(g, r_0 + 1) = \alpha_0 + 1$. Without loss of generality, we assume that

$$g(x_1, \ldots, x_n) = x_1 \cdots x_{r_0+1} \oplus g^*(x_1, \ldots, x_n)$$

for some g^* such that $\alpha(g^*, r_0 + 1) = \alpha_0$.

Define

$$\begin{cases} f_{b_1 \ldots b_{r_0+1}} \stackrel{\text{def}}{=} f(b_1, \ldots, b_{r_0+1}, x_{r_0+2}, \ldots, x_n) \\ g^*_{b_1 \ldots b_{r_0+1}} \stackrel{\text{def}}{=} g^*(b_1, \ldots, b_{r_0+1}, x_{r_0+2}, \ldots, x_n) \\ d_{b_1 \ldots b_{r_0+1}} \stackrel{\text{def}}{=} d(f_{b_1 \ldots b_{r_0+1}}, g^*_{b_1 \ldots b_{r_0+1}}) \end{cases}$$

Then we have

$$\begin{cases} d(f, g^*) = d_{0\ldots0} + \cdots + d_{1\ldots10} + d_{1\ldots1} = 2^{\lfloor \frac{t}{r_0+1} \rfloor + 1} k \\ d(f, g) = d_{0\ldots0} + \cdots + d_{1\ldots10} + 2^{n-(r_0+1)} - d_{1\ldots1} \end{cases}$$

for some integer k by an induction hypothesis on $\alpha(g, r_0 + 1)$. Therefore we have

$$d(f, g) = 2^{\lfloor \frac{t}{r_0+1} \rfloor + 1} k + 2^{n-(r_0+1)} - 2d_{1\ldots1} \ .$$

From our condition on the parameters, it holds that

$$t \leq n - (r_0 + 1) - 2 \ .$$

Therefore, we have

$$n - (r_0 + 1) \geq t + 2 \geq \lfloor \frac{t}{r_0 + 1} \rfloor + 1$$

Hence

$$2^{n-(r_0+1)} \equiv 0 \bmod 2^{\lfloor \frac{t}{r_0+1} \rfloor + 1} \ .$$

Further, from the induction hypothesis on $\alpha(g, r_0 + 1)$, we have

$$\begin{aligned} d_{1\ldots1} &\equiv 0 \bmod 2^{\lfloor \frac{t-(r_0+1)}{r_0+1} \rfloor + 1} \\ &\equiv 0 \bmod 2^{\lfloor \frac{t}{r_0+1} \rfloor} \ . \end{aligned}$$

since $f_{1\ldots1}$ is a $(t-(r_0+1))$-resilient function and $\alpha(g^*_{1\ldots1}, r_0{+}1) \leq \alpha_0$. Therefore,

$$2d_{1\ldots1} \equiv 0 \bmod 2^{\lfloor \frac{t}{r_0+1} \rfloor + 1} \ .$$

Finally, putting all things together, we have

$$d(f, g) \equiv 0 \bmod 2^{\lfloor \frac{t}{r} \rfloor + 1}$$

for any g such that $\deg(g) \leq r$. Therefore, this Theorem holds. □

Corollary 4.4. *If $r \leq n-t-2$, then*

$$\hat{\rho}(t,r,n) \leq \rho(r,n) - \left(\rho(r,n) \bmod 2^{\lfloor \frac{t}{r} \rfloor + 1}\right) \ .$$

Proof. It is clear that $\hat{\rho}(t,r,n) \leq \rho(r,n)$. Then apply Theorem 4.4 □

Corollary 4.5. *Let $Y \stackrel{\text{def}}{=} \hat{\rho}(t-1,r,n-1) + \rho(r-1,n-1)$. Then*

$$\hat{\rho}(t,r,n) \leq Y - \left(Y \bmod 2^{\lfloor \frac{t}{r} \rfloor + 1}\right) \ .$$

Proof. From Theorem 4.3 and Theorem 4.4. □

5 Numerical Result

We present a table of numerical values of $\hat{\rho}(t,r,n)$ which are obtained from our bounds and the previous bounds. The entry α-β means that $\alpha \leq \hat{\rho}(t,r,n) \leq \beta$.

	n	1	2	3	4	5	6	7
	$r=1$		0	2^a	$4^{a,b}$	12^a	24^a-26^b	56^a
	$r=2$			0	2^a	6^c	12^a-18	36^a-44
$t=0$	$r=3$				0	2^a	4^a-8	18^d-22^e
	$r=4$					0	2^a	4^a-8
	$r=5$						0	2^a
	$r=6$							0
	n	1	2	3	4	5	6	7
	$r=1$			0	$4^{a,g}$	8^a-12	$24^{a,b}$	56^a
	$r=2$				0	6^f	12^a-18	28^f-44
$t=1$	$r=3$					0	4^a-8	8^a-22^e
	$r=4$						0	4^a-8
	$r=5$							0
	n	1	2	3	4	5	6	7
	$r=1$				0	$8^{a,g}$	16^a-24^g	48^a-56
$t=2$	$r=2$					0	12^a-16^e	24^a-44
	$r=3$						0	8^a-22^e
	$r=4$							0

(a) is obtained from Theorem 4.1, (b) is obtained from Proposition 2.2, (c) is obtained from Theorem 4.2, (d) is obtained from Corollary 4.2, (e) is obtained from Corollary 4.4, (f) is obtained from Corollary 4.3, and (g) is obtained from Proposition 2.1. Unmarked values are obtained from $\rho(r,n)$.

References

1. X.D.Hou. Some results on the covering radii of Reed-Muller codes. *IEEE Transactions on Information Theory*, IT-39:366-378, 1993.
2. X.D.Hou. Further results on the covering radii of the Reed-Muller codes. *Designs, Codes and Cryptography*, vol.3, pages 167–177, 1993.
3. 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.
4. A.M.MacLoughlin. The covering radius of the $(m-3)$-rd order Reed-Muller codes and lower bounds on the $(m-4)$-th order Reed-Muller codes. *SIAM Journal of Applied Mathematics*, vol. 37, no. 2, October 1979.
5. P.Sarkar and S.Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. *Advances in Cryptology — CRYPTO 2000, LNCS 1880*, pages 515–532, 2000.
6. J.R.Schatz. The second order Reed-Muller code of length 64 has covering radius 18. *IEEE Transactions on Information Theory*, IT-27(5):529-530 September 1981.
7. T.Siegentharler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776-780 September 1984.