# New covering radius of Reed-Muller codes for $t$-resilient functions *

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

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

**Abstract**

From a view point of cryptography, we define a new covering radius of Reed-Muller codes as the maximum distance between *$t$-resilient* functions and the $r$-th order Reed-Muller code $RM(r, n)$. We next derive its lower and upper bounds. We also present a table of numerical data of our bounds.

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

## 1 Introduction

Let $X = (x_1, \ldots, x_n)$, where each $x_i$ is a binary variable. Then any Boolean function $g(X)$ is uniquely written as the algebraic normal form such that

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

*A preliminary version of this paper was presented at SAC '2001 and appeared in *Lecture Notes in Computer Science* **2259** (2001), 75–86.

The degree of $g(X)$, denoted by $\deg(g)$, is defined as the degree of the highest degree term in the algebraic normal form.

Now let $g(X)$ be a Boolean function such that $\deg(g) \le r$. Let $f(X)$ be a noisy version of $g(X)$ in some sense. Then in coding theory,

- $g(X)$ is a codeword of the $r$th order Reed-Muller code $RM(r,n)$,
- $f(X)$ is a received word when $g(X)$ is sent
- and the noise should be small.

The covering radius of $RM(r,n)$ is defined as

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

where the maximum is taken over *any* $f(X)$.

In cryptography, on the other hand,

- $f(X)$ is used as a main component of stream ciphers. In nonlinear combination generators, it must be $t$-resilient [2, 1] to resist the fast correlation attack [9].
- $g(X)$ is an approximation of $f(X)$ which attackers make use of
- and the noise should be large to resist attacks.

In this paper, we introduce a new covering radius of $RM(r,n)$ from a view point of cryptography. It is defined as the maximum distance between *t-resilient* functions and the $r$-th order Reed-Muller code $RM(r,n)$. That is,

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

where the maximum is taken over *t-resilient* functions $f(X)$. It is clear that

$$0 \le \hat{\rho}(t,r,n) \le \rho(r,n).$$

We next derive some lower bounds and upper bounds on $\hat{\rho}(t,r,n)$. We finally present a table of numerical data of our bounds. One of our upper bounds is a generalization of the result of Sarkar and Maitra for $r = 1$ [12].

## 2 Preliminaries

For two Boolean functions $f(X)$ and $g(X)$, let

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

For a set of Boolean functions $\Delta$, define

$$d(f,\Delta) = \min_{g(X)\in\Delta} d(f,g).$$

### 2.1 Stream Cipher [10]

In a stream cipher, a ciphertext sequence $\{c_i\}$ is computed as

$$c_i = m_i + s_i \bmod 2,$$

where $\{m_i\}$ is a plaintext sequence and $\{s_i\}$ is a keystream. If some part of $\{m_i\}$ is known to an attacker, then the corresponding part of $s_i$ is obtained as

$$s_i = m_i + c_i \bmod 2.$$

The attacker's goal is to find a key $K$ which generates the whole (or almost all of) $\{s_i\}$ from a short segment of $\{s_i\}$.

An LFSR (linear feedback shift register) is a basic component of keystream generators. It generates a sequence $\{s_i\}$ recursively in such a way that

$$s_i = c_1 s_{i-1} + \cdots + c_L s_{i-L} \bmod 2.$$

The smallest $L$ which can generate $\{s_i\}$ by the above equation is called the linear complexity of $\{s_i\}$. An LFSR is not used as a keystream generator because Berlekamp-Massey algorithm [10, pp.200-201] can find the initial value $(s_{-1},\ldots,s_{-L})$ from only $2L$ consecutive bits of $\{s_i\}$.

Hence keystream generators usually combine several LFSRs nonlinearly. A nonlinear combination generator is one of the most common keystream generatros such that

$$s_i = f(x_1(i),\ldots,x_n(i)),$$

where $f(X)$ is a nonlinear Boolean function and $x_j(i)$ is the output of the $j$th LFSR at time $i$, where $1 \leq j \leq n$.

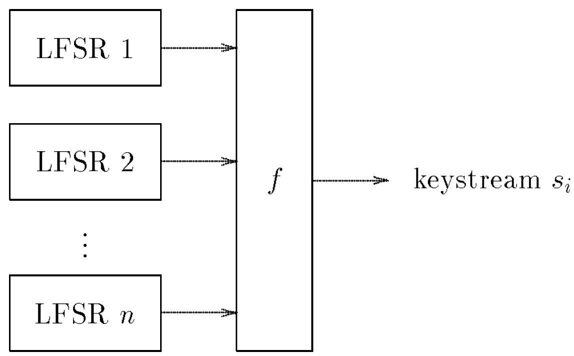


Figure 1: Nonlinear combination generator

### 2.2 Nonlinearity

In a nonlinear combination generator of Fig.1, let $L_j > 2$ denote the linear complexity of the $j$th LFSR for $1 \leq j \leq n$. Then the linear complexity of $\{s_i\}$ generated by the nonlinear combination generator is given by the following proposition under some condition [10, page 205].

**Proposition 2.1** *Suppose that each LFSR has maximum length and $L_1, \ldots, L_n$ are pairwise distinct. Then the linear complexity of $\{s_i\}$ is $f(L_1, \ldots, L_n)$, where $f(L_1, \ldots, L_n)$ is evaluated over integers.*

We assume that the condition of Proposition 2.1 is satisfied in the rest of this paper.

For example, if $f(X)$ is an affine function, i.e.,

$$f(X) = a_0 + a_1 x_1 + \cdots + a_n x_n \bmod 2,$$

then the linear complexity of $\{s_i\}$ is given by

$$L_0 = a_0 + a_1 L_1 + \cdots + a_n L_n.$$

The above $L_0$ is not large enough to resist the Berlekamp-Massey attack. Therefore, it must be that $\deg(f) \geq 2$.

Interestingly even if $f(X)$ is approximated by an affine function, Ding et al. showed that a linear attack can break the nonlinear combinaiton generator [9]. (In [9], the authors called the linear attack the BAA attack, where BAA stands for best affine approximation.) Hence $f(X)$ of Fig.1 must have a large distance from the set of affine functions.

Hence the nonlinearity of $f(X)$, denoted by $nl(f)$, is defined as a distance between $f(X)$ and the set of affine functions $\Delta_{affine}$. That is,

$$nl(f) \stackrel{\text{def}}{=} d(f, \Delta_{affine}).$$

### 2.3 Resiliency

We say that $f(X)$ is balanced if

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

Equivalently

$$\Pr(f(X) = 0) = \Pr(f(X) = 1) = 1/2.$$

$f(X)$ used in nonlinear combination generators must be balanced because the keystream $\{s_i\}$ must be random.

Further, the output

$$z = f(x_1, \ldots, x_n)$$

should not be correlated with any small subset of $\{x_1, \ldots, x_n\}$. Otherwise, the fast correlation attack succeeds [9]. For example, if $z$ is correlated with some $x_j$, then the initial value of the $j$th LFSR can be found by the fast correlation attack [9].

We have the following definitions.

**Definition 2.1** *[14] We say that $f(X)$ is correlation immune of order $t$ if $f(X)$ is not correlated with any $t$-subset of $\{x_1, \ldots, x_n\}$. That is, $f(X)$ is correlation immune of order $t$ if*

$$\Pr(f(X) = 0 \mid x_{i_1} = b_{i_1}, \ldots, x_{i_t} = b_{i_t}) = \Pr(f(X) = 0)$$

*for any $t$ positions $i_1, \ldots, i_t$ and any $t$ bits $b_{i_1}, \ldots, b_{i_t}$.*

**Definition 2.2** *[2, 1] We say that $f(X)$ is $t$-resilient if $f(X)$ is balanced and $f(X)$ is correlation immune of order $t$. That is, $f(X)$ is $t$-resilient if*

$$\Pr(f(X) = 0 \mid x_{i_1} = b_{i_1}, \ldots, x_{i_t} = b_{i_t}) = 1/2$$

*for any $t$ positions $i_1, \ldots, i_t$ and any $t$ bits $b_{i_1}, \ldots, b_{i_t}$.*

Consequently, $f(X)$ must be $t$-resilient for large $t$.

### 2.4 Previous Work

From the above discussion, we see that $f(X)$ must be $t$-resilient for large $t$ and $nl(f)$ should be as large as possible in nonlinear combination generators. Sarkar and Maitra derived an upper bound on $nl(f)$ of $t$-resilient functions as follows.

**Proposition 2.2** *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 2.3** *Suppose that $f(X)$ is a $t$-resilient function.*

1. *If $n$ is even and $t+1 > \frac{n}{2} - 1$, then*
$$nl(f) \leq 2^{n-1} - 2^{t+1}.$$
2. *If $n$ is even and $t+1 \leq \frac{n}{2} - 1$, then*
$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{t+1}.$$
3. *If $n$ is odd and $2^{t+1} > 2^{n-1} - nlmax(n)$, then*
$$nl(f) \leq 2^{n-1} - 2^{t+1}.$$
4. *If $n$ is odd and $2^{t+1} \leq 2^{n-1} - nlmax(n)$, then $nl(f)$ is the highest multiple of $2^{t+1}$ which is less than or equal to $2^{n-1} - nlmax(n)$,*

*where $nlmax(n)$ is the maximum possible nonlinearity of an $n$-variable function.*

## 3 Low Degree Approximation Attack

In this section, we generalize the linear attack of [3] to a low degree approximation attack. It is shown that nonlinear combination generators are broken by this attack if $f(X)$ of Fig.1 is approximated by a low degree Boolean function.

In general, suppose that $\{s_i\}$ is approximated by $\{\hat{s}_i\}$. That is,

$$\Pr(\hat{s}_i = s_i) \approx 1.$$

Roughly speaking, if the linear complexity of $\{\hat{s}_i\}$ is not large enough, then the fast correlation attack [9] can find the initial value of $\{\hat{s}_i\}$ from a short segment of $\{s_i\}$.

### 3.1 Linear attack

In Fig.1, suppose that $f(X)$ is approximated by an affine function

$$g(X) = a_0 + a_1 x_1 + \cdots + a_n x_n \bmod 2.$$

That is, $d(f, g)$ is small. Let $\{s_i\}$ the output sequence of the nonlinear combnation generator and let $\{\hat{s}_i\}$ be the sequence obtained by replacing $f(X)$ with $g(X)$. Then

1. $\{\hat{s}_i\}$ is an approximation of $\{s_i\}$.

2. From Proposition 2.1, there exists an LFSR which generates $\{\hat{s}_i\}$ such that the size of the LFSR is

$$L_0 = a_0 + a_1 L_1 + \cdots + a_n L_n.$$

The linear attack [3] is to find the initial value $\hat{K}$ of $\{\hat{s}_i\}$ from a short segment of $\{s_i\}$ by the fast correlation attack. It succeeds because $L_0$ is not large enough. If $\hat{K}$ is found, then we can obtain the whole sequence of $\{\hat{s}_i\}$. This implies that a large part of $\{s_i\}$ is leaked since $\{\hat{s}_i\}$ is an approximation of $\{s_i\}$. Therefore, a large part of the plaintext sequence is leaked.

(Remark) In [3], the authors cited the method of Zeng [15] instead of the fast correlation attack [9].

### 3.2 Low degree approximation attack

The linear attack is generalized as follows. In Fig.1, suppose that $f(X)$ is approximated by a low degree Boolean function $g(X)$. In this case, the keystream $\{s_i\}$ is approximated by the output sequence $\{\hat{s}_i\}$ of an LFSR whose linear complexity is $L_0 = g(L_1, \ldots, L_n)$. Then the initial value $\hat{K}$ of $\{\hat{s}_i\}$ is obtaind from a short segment of $\{s_i\}$ by the fast correlation attack [9] as far as $L_0$ is not large enough. If $\hat{K}$ is found, then we can obtain $\{\hat{s}_i\}$. This implies that a large part of the keystream $\{s_i\}$ is leaked since $\{\hat{s}_i\}$ is a noisy version of $\{s_i\}$ and the noise is small.

## 4 New Covering Radius for $t$-Resilient Functions

### 4.1 Covering Radius of RM-Code

The $r$th order Reed-Muller code $RM(r, n)$ is identical to the set of Boolean functions $g(X)$ such that $\deg(g) \leq r$. The covering radius of $RM(r, n)$ is defined as the maximum distance between $f(X)$ and $RM(r,n)$. That is,

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

where the maximum is taken over $f(X)$.

Some numerical bounds on $\rho(r,n)$ are illustrated in the following table [11, page 802]. The entry $\alpha$-$\beta$ means that $\alpha \le \rho(r,n) \le \beta$.

Table 1. Numerical bounds on $\rho(r,n)$.

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $r=1$ | 0 | 1 | 2 | 6 | 12 | 28 | 56 |
| $r=2$ | | 0 | 1 | 2 | 6 | 18 | 40-44 |
| $r=3$ | | | 0 | 1 | 2 | 8 | 20-23 |
| $r=4$ | | | | 0 | 1 | 2 | 8 |
| $r=5$ | | | | | 0 | 1 | 2 |
| $r=6$ | | | | | | 0 | 1 |
| $r=7$ | | | | | | | 0 |

## 4.2 New Covering Radius for $t$-Resilient Functions

$f(X)$ of Fig.1 should not be approximated even by low degree Boolean functions to resist the low degree approxamation attack shown in Sec. 3. Further, $f(X)$ should be $t$-resilient to be secure against the fast correlation attacks.

From this point of view, we define a new covering radius of $RM(r,n)$ as the maximum distance between a $t$-resilient function $f(X)$ and $RM(r,n)$. That is,

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

where the maximum is taken over *$t$-resilient functions* $f(X)$.

It is clear that

$$0 \le \hat{\rho}(t,r,n) \le \rho(r,n).$$

Further, Siegenthalar's inequality on resilient functions [14] immediately gives us the following proposition.

**Proposition 4.1** *If $n \le t+r+1$, then*

$$\hat{\rho}(t,r,n) = 0.$$

In what follows, we will derive lower bounds and upper bounds on $\hat{\rho}(t, r, n)$ for $n > t + r + 1$.

(Remark) Note that

$$nl(f) = d(f, RM(1, n)).$$

Sarkar et al. [12] derived an upper bound on $\hat{\rho}(t, 1, n)$ in our terminology.

# 5 Lower bounds on $\hat{\rho}(t, r, n)$

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

## 5.1 Lower bound for $t = 0$

**Theorem 5.1**

$$\hat{\rho}(0, r, n) \geq \hat{\rho}(0, r-1, n-1) \ .$$

*Proof*. Suppose that $\hat{\rho}(0, r-1, n-1)$ is achieved by $g(x_1, x_2, \ldots, x_{n-1})$. That is, $g$ is balanced and

$$d(g, RM(r-1, n-1)) = \hat{\rho}(0, r-1, n-1).$$

We first constrcut balanced $g'$ and $g''$ such that

$$g = g' \oplus g''$$

as follows. Since $g$ is balanced, there are $2^{n-2}$ zeros and $2^{n-2}$ ones in the truth table. Now choose $2^{n-3}$ out of $2^{n-2}$ zeros arbitrarily and change them to $2^{n-3}$ ones. Similarly, choose $2^{n-3}$ out of the original $2^{n-2}$ ones arbitrarily and change them to $2^{n-3}$ zeros. Let $g'$ be a Boolean function which have the resulting truth table. Let

$$g'' \stackrel{\text{def}}{=} g \oplus g'.$$

Then it is easy to see that $g'$ and $g''$ are balanced.

For example, consider $g$ with $n = 5$ such that its truth table is

$$(0110100110010110) \ .$$

Choose 4 zeros and 4 ones as follows.

$$(\check{0}1\check{1}\check{0}\check{1}0\check{0}1\check{1}00\check{1}\check{0}110) \ .$$

| $x_1,\ldots,x_{n-1}$ | $x_n$ | $f$ |
|---|---|---|
| $0\cdots\cdots0$ | 0 | |
| $\vdots$ | $\vdots$ | $g''$ |
| $1\cdots\cdots1$ | 0 | |
| $0\cdots\cdots0$ | 1 | |
| $\vdots$ | $\vdots$ | $g'$ |
| $1\cdots\cdots1$ | 1 | |

Figure 2: Truth table of $f$.

Then $g'$ has the following truth table.

$$(1101001100001110)\ .$$

$g''$ has the following truth table.

$$(1011101010011000)\ .$$

We can see that $g'$ and $g''$ are balanced.

Next define $f(x_1,\ldots,x_n)$ as

$$f \stackrel{\text{def}}{=} g'' \oplus x_n \cdot g.$$

If $x_n = 0$, then $f = g''$. If $x_n = 1$, then $f = g'' \oplus g = g'$. Therefore $f$ is balanced because $g'$ and $g''$ are balanced. (See Fig.2 for the truth table of $f$. )

Finally let

$$u(x_1,x_2,\ldots,x_n) = u_1(x_1,x_2,\ldots,x_{n-1}) \oplus x_n u_2(x_1,x_2,\ldots,x_{n-1})\ .$$

be a Boolean function such that

$$d(f,u) = d(f, RM(r,n)),$$

where $u(x_1,x_2,\ldots,x_n) \in RM(r,n)$. Then we have

$$\begin{aligned} d(f,u) &= d((u_1, u_1 \oplus u_2), (g'', g')) \\ &= w(u_1 \oplus g'') + w(u_1 \oplus u_2 \oplus g') \end{aligned}$$

$$
\begin{aligned}
&= w(u_1 \oplus g'') + w(u_1 \oplus g'' \oplus u_2 \oplus g' \oplus g'') \\
&\geq w(u_1 \oplus g'') + w(u_2 \oplus g' \oplus g'') - w(u_1 \oplus g'') \\
&= w(u_2 \oplus g'' \oplus g') \\
&= w(u_2 \oplus g) \\
&= d(g, u_2)
\end{aligned}
$$

where $w(\alpha)$ denotes the Hamming weight of $\alpha$.

Now since $u_2 \in RM(r-1, n-1)$, we have

$$d(f, u) \geq d(g, u_2) \geq d(g, RM(r-1, n-1)) = \hat{\rho}(0, r-1, n-1)$$

On the other hand, we have

$$d(f, u) = d(f, RM(r, n)) \leq \hat{\rho}(0, r, n) \ .$$

Therefore

$$\hat{\rho}(0, r, n) \geq \hat{\rho}(0, r-1, n-1) \ .$$

□

## 5.2 Lower bound for any $t$ (I)

**Theorem 5.2**

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

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

### 5.3 Lower bound for any $t$ (II)

**Theorem 5.3** *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

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

Now $g$ 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 we have

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

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

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

$\square$

**Corollary 5.2** $\hat{\rho}(0,3,7)\geq 18$.

*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 [13]

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

Let $r = 2$, $n = 6$, $m = 5$ and $l = 2$ in Theorem 5.3. Then we obtain this corollary. $\square$

**Corollary 5.3** *Suppose that $n = 4k + s$, where $0 \le s \le 3$ and $k \ge 1$. Let $t = 2k - 1$. Then*

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

*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 5.3, 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 $s \ge 0$.

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 $\deg(g) \le 1$,

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

Hence

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

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

Therefore, this corollary holds from Theorem 5.3. □

# 6 Upper bounds on $\hat{\rho}(t,r,n)$

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

## 6.1 Upper booound (I)

**Theorem 6.1** *For $t \ge 1$,*

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

*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

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

Choose $g_1$ such that $\deg(g_1) \le r$ 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,

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

□

### 6.2 Upper boound (II)

**Lemma 6.1** *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 $d(f,g) \equiv 0 \bmod 2$. □

**Theorem 6.2** *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 2.2.

**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

$$\begin{cases} d(f, g^*) = d_{0 \ldots 0} + \cdots + d_{1 \ldots 10} + d_{1 \ldots 1} = 2^{\lfloor \frac{t}{r_0+1} \rfloor + 1} k \\ d(f, g) = d_{0 \ldots 0} + \cdots + d_{1 \ldots 10} + 2^{n - (r_0 + 1)} - d_{1 \ldots 1} \end{cases}$$

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

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

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

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

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

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

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 6.1** *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 6.2 □

**Corollary 6.2** *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 6.1 and Theorem 6.2. □

**Theorem 6.3** *1. If $n$ is even and $\lfloor \frac{t}{r} \rfloor + 1 > \frac{n}{2} - 1$, then*

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

*2. If $n$ is even and $\lfloor \frac{t}{r} \rfloor + 1 \leq \frac{n}{2} - 1$, then*

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

*3. If $n$ is odd and $2^{\lfloor \frac{t}{r} \rfloor + 1} > 2^{n-1} - nlmax(n)$, then*

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

*4. If $n$ is odd and $2^{\lfloor \frac{t}{r} \rfloor + 1} \leq 2^{n-1} - nlmax(n)$, then $\hat{\rho}(t, r, n)$ is the highest multiple of $2^{\lfloor \frac{t}{r} \rfloor + 1}$ which is less than or equal to $2^{n-1} - nlmax(n)$.*

*Proof*. We prove only cases 1 and 2, the other cases being similar.

1. Using Theorem 6.2 for any $n$-variable, $t$-resilient function $f$ and $g \in RM(r, n)$, we have $d(f, g) \equiv 0 \bmod 2^{\lfloor \frac{t}{r} \rfloor + 1}$. Thus, $d(f, g) = 2^{n-1} \pm k 2^{\lfloor \frac{t}{r} \rfloor + 1}$ for some $k$. Cleary $k$ cannot be 0 for all $g$ and hence $d(f, RM(r, n))$ is at most $2^{n-1} - 2^{\lfloor \frac{t}{r} \rfloor + 1}$.
2. As in 1, we have $d(f, g) = 2^{n-1} \pm k 2^{\lfloor \frac{t}{r} \rfloor + 1}$ for some $k$. Let $2^{\frac{n}{2}-1} = p 2^{\lfloor \frac{t}{r} \rfloor + 1}$ (we can write in this way as $\lfloor \frac{t}{r} \rfloor + 1 \leq \frac{n}{2} - 1$). If for all $l$ we have $k \leq p$, then $f$ must necessarily be bent and hence cannot be resilient. Thus there must be some $l$ such that the corresponding $k > p$. This shows that $d(f, RM(r, n))$ is at most $2^{n-1} - 2^{\frac{n}{2}-1} - 2^{\lfloor \frac{t}{r} \rfloor + 1}$.

□

(Remark)

1. Proposition 2.2 is obtained as a special case of Theorem 6.2.
2. Proposition 2.3 is obtained as a special case of Theorem 6.3.

# 7 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 $\alpha$-$\beta$ means that $\alpha \le \hat{\rho}(t,r,n) \le \beta$.

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

1. $(a)$ is obtained from Theorem 5.2.
2. $(b)$ is obtained from Theorem 5.1.
3. $(c)$ is obtained from Theorem 5.3.
4. $(d)$ is obtained from Corollary 5.2.
5. $(e)$ is obtained from Corollary 6.1.
6. $(f)$ is obtained from Corollary 5.3.
7. $(g)$ is obtained from Proposition 2.2.
8. $(h)$ is obtained from Proposition 2.3.
9. $(i)$ is obtained from [12, Table 1].
10. Unmarked values are obtained from $\rho(r,n)$.

## References


[1] C.H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing* **17** (1988), 210–229.

[2] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S Rudich and R. Smolensky. The bit extraction problem or $t$-resilient functions. *26th IEEE symposium on Foundations of Computer Science*, pages 396–407, 1985.

[3] Ding, C., Xiao, G. and Shan, W.: "The stability theory of stream ciphers"; Lecture Notes in Computer Science 561, Springer-Verlag, 1991.

[4] X.D.Hou. Some results on the covering radii of Reed-Muller codes. *IEEE Transactions on Information Theory*, IT-39:366-378, 1993.

[5] X.D.Hou. Further results on the covering radii of the Reed-Muller codes. *Designs, Codes and Cryptography*, vol.3, pages 167–177, 1993.

[6] T.Johansson and F.Jonsson, "Fast Correlation Attacks through Reconstruction of Linear Polynomials", Advances in Cryptology, Crypto 2000, LNCS vol.1880, pp.300-315, Springer-Verlag, 2000.

[7] 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.

[8] 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 on Applied Mathematics*, vol. 37, no. 2, October 1979.

[9] W. Meier and O. Staffelbach, "Fast Correlation Attacks on Certain Stream Ciphers", Journal of Cryptology, pp.159-176, 1989.

[10] A.Menezes, P. van Oorschot and S.Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[11] V.S.Pless and W.C.Huffman, editors, "Handbook of Coding Theory", North Holland, 1998.

[12] P.Sarkar and S.Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. *Advances in Cryptology — CRYPTO 2000, LNCS 1880*, pages 515–532, 2000.

[13] 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.

[14] T.Siegentharler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776-780 September 1984.

[15] K.Zeng. The entropy leakage in cryptosystems. *The Graduate School of Science and Technology of China*, Beijing, PRC, 1987