

On the Covering Radius of Second Order Binary Reed-Muller Code in the Set of Resilient Boolean Functions

Yuri Borissov¹, An Braeken², Svetla Nikova², and Bart Preneel²

¹ Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
8 G.Bonchev, 1113 Sofia, Bulgaria
yborisov@moi.math.bas.bg

² Department Electrical Engineering - ESAT/SCD/COSIC,
Katholieke Universiteit Leuven, Kasteelpark Arenberg 10,
B-3001 Leuven, Belgium

an.braeken,svetla.nikova,bart.preneel@esat.kuleuven.ac.be

Abstract. Let $\mathcal{R}_{t,n}$ denote the set of t -resilient Boolean functions of n variables. First, we prove that the covering radius of the binary Reed-Muller code $RM(2,6)$ in the sets $\mathcal{R}_{t,6}$, $t = 0, 1, 2$ is **16**. Second, we show that the covering radius of the binary Reed-Muller code $RM(2,7)$ in the set $\mathcal{R}_{3,7}$ is **32**. We derive a new lower bound for the covering radius of the Reed-Muller code $RM(2,n)$ in the set $\mathcal{R}_{n-4,n}$. Finally, we present new lower bounds in the sets $\mathcal{R}_{t,7}$, $t = 0, 1, 2$.

1 Introduction

In the standard model of stream cipher the outputs of several independent Linear Feedback Shift Register (LFSR) sequences are combined using a nonlinear Boolean function to produce the keystream. Siegenthaler [14] was the first to point out that the combining function should possess certain properties in order to resist divide-and-conquer attacks. A Boolean function to be used in stream ciphers should satisfy several properties. *Balancedness* – the Boolean function has to output zeros and ones with equal probabilities. *High nonlinearity* - the Boolean function has to be at sufficiently high distance from any affine function. *Correlation-immunity* (of order t) - the output of the function should be statistically independent of the combination of any t of its inputs. A balanced correlation-immune function is called *resilient*. Other important factors are high algebraic degree and simple implementation in hardware. It is known that there are certain trade-offs involved among these parameters. In order to achieve the desired trade-offs designers typically fix one or two parameters and try to optimize the others.

Recently also algebraic attacks [3, 4] have been applied successfully to stream ciphers. The central idea in the algebraic attacks is to use a lower degree approximation of the combining Boolean function and then to solve an over-defined system of nonlinear multivariate equations of low degree by efficient methods such as XL or simple linearization [5]. In order to resist these attacks, the Boolean function should also have a high distance to lower order degree functions.

Kurosawa *et al.* [7] have introduced a new covering radius, which measures the maximum distance between t -resilient functions and r -th degree functions or the r -th order Reed-Muller code $RM(r, n)$. That is $\hat{\rho}(t, r, n) = \max d(f(\bar{x}), RM(r, n))$, where the maximum is taken over the set $\mathcal{R}_{t,n}$ of t -resilient Boolean functions of n variables. They also provide a table with certain lower and upper bounds for $\hat{\rho}(t, r, n)$.

In this paper we prove exact values of the covering radius $\hat{\rho}(t, 2, 6)$, for $t = 0, 1, 2$ and $\hat{\rho}(3, 2, 7)$. We also generalize our method and find a new lower bound for the covering radius of the Reed-Muller code $RM(2, n)$ in the set $\mathcal{R}_{n-4,n}$.

The rest of the paper is organized as follows. In Sect. 2 we give some definitions and known results that will be used later in our investigations. Our main results are described in Sect. 3 and 4. In Sect. 3 we prove that the covering radius of the binary Reed-Muller code $RM(2, 6)$ in the sets $\mathcal{R}_{t,6}$, $t = 0, 1, 2$ is **16** and in Sect. 4 we present a proof that the covering radius of the binary Reed-Muller code $RM(2, 7)$ in the set $\mathcal{R}_{3,7}$ is **32**. In this section we derive a new lower bound for the covering radius of the Reed-Muller code $RM(2, n)$ in the set $\mathcal{R}_{n-4,n}$. Finally, the lower bounds of [7] in the sets $\mathcal{R}_{t,7}$, $t = 0, 1, 2$ are improved.

2 Background and Related Work

Let $f(\bar{x})$ be a Boolean function on \mathbb{F}_2^n . Any Boolean function can be uniquely expressed in algebraic normal form (ANF):

$$f(\bar{x}) = \sum_{(a_1, \dots, a_n) \in \mathbb{F}_2^n} h(a_1, \dots, a_n) x_1^{a_1} \cdots x_n^{a_n},$$

h is a function on \mathbb{F}_2^n , defined by $h(\bar{a}) = \sum_{\bar{x} \leq \bar{a}} f(\bar{x})$ for any $\bar{a} \in \mathbb{F}_2^n$, where $\bar{x} \leq \bar{a}$ means that $x_i \leq a_i$ for all $i \in \{1, \dots, n\}$. The *algebraic degree* of f , denoted by $\deg(f)$, is defined as the number of variables in the highest term $x_1^{a_1} \cdots x_n^{a_n}$ in the ANF of f , for which $h(a_1, \dots, a_n) \neq 0$. If the highest term of f that contains x_i has degree at most one, x_i is called a linear variable. If $\deg(f) \leq 1$ then f is called an affine function.

The minimum distance between f and the set of all affine functions is called the *nonlinearity* of f and is denoted by N_f .

Let $\bar{x} = (x_1, x_2, \dots, x_n)$, $\bar{\omega} = (\omega_1, \omega_2, \dots, \omega_n)$ be vectors in $\mathbb{F}_2^n = GF(2)^n$, and $\bar{x} \cdot \bar{\omega} = x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n$ be their *dot product*. The Walsh transform of $f(\bar{x})$ is a real-valued function over \mathbb{F}_2^n that is defined as

$$W_f(\bar{\omega}) = \sum_{\bar{x} \in \mathbb{F}_2^n} (-1)^{f(\bar{x}) + \bar{x} \cdot \bar{\omega}}.$$

A very important equation related to the values in the Walsh spectrum of a Boolean function $f(\bar{x})$ is the *Parseval equation*:

$$\sum_{\bar{\omega} \in \mathbb{F}_2^n} W_f^2(\bar{\omega}) = 2^{2^n}.$$

Correlation-immune Boolean functions can be defined in various ways, but for our purposes it is convenient to use as a definition the following spectral characterization given by Xiao and Massey [16].

Definition 1. *A function $f(\bar{x})$ is t -th order correlation-immune if and only if its Walsh transform W_f satisfies $W_f(\bar{\omega}) = 0$, for $1 \leq wt(\bar{\omega}) \leq t$. Balanced t -th order correlation-immune functions are called t -resilient functions, i.e. $W_f(\bar{\omega}) = 0$, for $0 \leq wt(\bar{\omega}) \leq t$.*

Siegenthaler's Inequality [13] states that if the function f is a correlation-immune function of order t then $\deg(f) \leq n - t$. Moreover, if f is t -resilient then $\deg(f) \leq n - t - 1$, $t < n - 1$.

If a variable x_i is linear for a function f we can present f in the form

$$f(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) = g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) + x_i.$$

A Boolean function $f(\bar{x})$ on \mathbb{F}_2^n is said to be a *plateaud* function if its Walsh transform W_f only takes three values 0 and $\pm\lambda$, where λ is a positive integer, called amplitude of the plateaud function. Because of the Parseval's relation, λ cannot be zero and must be a power 2^r , where $\frac{n}{2} \leq r \leq n$.

Lemma 1. [15] *Let x_{n+1} be a linear variable, i.e., $f(x_1, \dots, x_n, x_{n+1}) = g(x_1, \dots, x_n) + cx_{n+1}$, where $c \in \{0, 1\}$ and $g(x_1, \dots, x_n)$ is t -resilient. Then $f(x_1, \dots, x_n, x_{n+1})$ is $t + 1$ -resilient and $N_f = 2N_g$.*

Recently Sarkar and Maitra [11], Tarannikov [15], Zhang and Zheng [18] have proved independently that when $t > \frac{n-1}{2}$, the nonlinearity N_f of a t -resilient function satisfies the condition $N_f \leq 2^{n-1} - 2^{t+1}$.

Let f be a Boolean function on \mathbb{F}_2^n and $\bar{\omega}$ be a vector in \mathbb{F}_2^n , such that $wt(\bar{\omega}) = r$. By $f_{\bar{\omega}}$ we denote the Boolean function on \mathbb{F}_2^{n-r} , defined as follows. Let i_1, \dots, i_r be such that $\omega_{i_1} = \dots = \omega_{i_r} = 1$ and $\omega_j = 0$ for $j \notin \{i_1, \dots, i_r\}$. Then $f_{\bar{\omega}}$ is formed from f by setting the variable x_j to 0 if and only if $j \in \{i_1, \dots, i_r\}$.

Theorem 1. [10] *Let $f(x_1, \dots, x_n)$ be a Boolean function and $\bar{\omega} \in \mathbb{F}_2^n$. Then*

$$\sum_{\bar{\theta} \leq \bar{\omega}} W_f(\bar{\theta}) = 2^n - 2^{wt(\bar{\omega})+1} wt(f_{\bar{\omega}}).$$

It is well known that the codewords of the r -th order Reed-Muller code of length 2^n (denoted by $RM(r, n)$) may be presented by the set of Boolean functions of degree $\leq r$ in n variables. The *covering radius* of $RM(r, n)$ is defined as

$$\rho(r, n) = \max d(f(\bar{x}), RM(r, n)),$$

where the maximum is taken over all Boolean functions $f(\bar{x})$.

A new covering radius of $RM(r, n)$ from a cryptographic point of view was introduced in [7]. It is defined as the maximum distance between t -resilient functions $\mathcal{R}_{t,n}$ and the r -th order Reed-Muller code $RM(r, n)$. That is,

$$\hat{\rho}(t, r, n) = \max_{f(\bar{x}) \in \mathcal{R}_{t,n}} d(f(\bar{x}), RM(r, n)).$$

It is clear that $0 \leq \hat{\rho}(t, r, n) \leq \rho(r, n)$. The Siegentaler's inequality gives that $\hat{\rho}(t, r, n) \neq 0$, when $n > t + r + 1$. Note that $nl(f(\bar{x})) = d(f, RM(1, n))$. In fact, in this terminology an upper bound on $\hat{\rho}(t, 1, n)$ has been derived in [11, 15, 18].

For the new covering radius $\hat{\rho}(t, r, n)$ the authors in [7] derived some lower and upper bounds which are presented in Table 1. The entry $a - b$ means that $a \leq \hat{\rho}(t, r, n) \leq b$

3 The Covering Radius of $RM(2, 6)$ in the Set $\mathcal{R}_{t,6}$ for $t = 0, 1, 2$

We begin with the following lemma.

Lemma 2. *If a Boolean function $f(\bar{x})$ on \mathbb{F}_2^6 is at distance 18 from $RM(2, 6)$, then its degree is 3.*

Table 1. Numerical data of the bounds on $\hat{\rho}(t, r, n)$

	n	1	2	3	4	5	6	7
$t = 0$	$r = 1$		0	2	4	12	26	56
	$r = 2$			0	2	6	12-18	36-44
	$r = 3$				0	2	6-8	18-22
	$r = 4$					0	2	6-8
	$r = 5$						0	2
	$r = 6$							0
	n	1	2	3	4	5	6	7
$t = 1$	$r = 1$			0	4	12	24	56
	$r = 2$				0	6	12-18	28-44
	$r = 3$					0	4-8	8-22
	$r = 4$						0	4-8
	$r = 5$							0
	n	1	2	3	4	5	6	7
$t = 2$	$r = 1$				0	8	24	48-56
	$r = 2$					0	12-16	24-44
	$r = 3$						0	8-22
	$r = 4$							0

Proof. Let $\bar{f} = (\bar{a}, \bar{b})$ be the truth table of $f(\bar{x})$, where \bar{a} and \bar{b} are two binary vectors of length 32. This means that we can represent $f(\bar{x})$ as follows:

$$f(\bar{x}) = a(\bar{x})(x_6 + 1) + b(\bar{x})x_6, \quad (1)$$

First we will prove that:

- (i) \bar{a} belongs to a coset of $RM(2, 5)$ of minimal weight 6.
- (ii) There exists $\bar{u} \in RM(2, 5)$, such that $\bar{b} + \bar{u}$ belongs to a coset of $RM(1, 5)$ of minimal weight 12.

Consider the coset $C_{\bar{a}}$ of $RM(2, 5)$, which contains the vector \bar{a} . Suppose that the minimal weight of $C_{\bar{a}}$ is less than 6 and let $\bar{u} \in RM(2, 5)$, such that $d(\bar{a}, \bar{u}) = \min_{w \in RM(2, 5)} d(\bar{a}, \bar{w}) < 6$, where $d(\cdot, \cdot)$ denotes Hamming distance between two vectors i.e. the number of position in which they differ. Let us also consider the coset $C_{\bar{b} + \bar{u}}$ of $RM(1, 5)$, which contains the vector $\bar{b} + \bar{u}$. Since the covering radius of $RM(1, 5)$ is 12 (see [1]), there exists a vector $\bar{v} \in RM(1, 5)$, such that $d(\bar{b} + \bar{u}, \bar{v}) \leq 12$. Since $d[(\bar{a}, \bar{b}), (\bar{u}, \bar{u} + \bar{v})] = d(\bar{a}, \bar{u}) + d(\bar{b} + \bar{u}, \bar{v})$, the vector $(\bar{u}, \bar{u} + \bar{v}) \in RM(2, 6)$ (see [9]) is at distance less than 18 from $\bar{f} = (\bar{a}, \bar{b})$.

But this contradicts our assumption that \bar{f} is at distance 18 from $RM(2, 6)$. Hence $C_{\bar{a}}$ is with maximal possible minimal weight 6 (see [1, 8]) i.e.

$\min_{w \in RM(2,5)} d(\bar{a}, \bar{w}) = d(\bar{a}, \bar{u}) = 6$. Similarly, we can prove that $C_{\bar{b}+\bar{u}}$ has minimal weight 12. Note that (ii) holds for \bar{a} as well, since (\bar{b}, \bar{a}) is at distance 18 from $RM(2, 6)$.

Table II from [1] shows that by an appropriate affine transformation of the variables, any Boolean function of 5 variables can be reduced to one of the functions with 8 possible parts consisting of terms of degree greater than 2. It is easy to see that only in the following two cases the minimal weight of the corresponding coset of $RM(2, 5)$ is 6:

1. $x_2x_3x_4x_5 + x_1x_2x_3 + x_1x_4x_5$;
2. $x_1x_2x_3 + x_1x_4x_5$.

Consulting Table I from [1] we can conclude that the first case is not possible for cosets of $RM(1, 5)$ with minimal weight 12. Therefore in the representation (1) of f both $a(\bar{x})$ and $b(\bar{x})$ have degree 3.

Similar representation (with subfunctions having degree 3) holds for any other variable x_j , $j = 1, \dots, 5$. Therefore all functions $f(\bar{x}|x_j = \text{const})$, $j = 1, \dots, 6$ are of degree 3 and hence f is of degree equal to 3. \square

Remark 1. J. Schatz proves in [12] that the covering radius of $RM(2, 6)$ is 18 by constructing a coset which has a minimal weight 18. This coset can be written as $\bar{f} + RM(2, 6)$, where $f(\bar{x}) = (x_1x_2x_3 + x_1x_4x_5 + x_2x_3 + x_2x_4 + x_3x_5)x_6 + (x_1x_2x_3 + x_1x_4x_5)(x_6 + 1)$.

Lemma 3. *The Boolean function $g_1(\bar{x}) = x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_2 + x_1x_3 + x_2x_5 + x_2 + x_3 + x_4 + x_5 + x_6$ is 2-resilient and it is at distance 16 from $RM(2, 6)$.*

Proof. By computing the Walsh transform and checking the spectrum, we see that $g_1(\bar{x})$ is 2-resilient. The cubic part of g_1 coincides with the Boolean function $f_5(\bar{x}) = x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6$ from [6], where Hou shows that the coset $\bar{f}_5 + RM(2, 6)$ has minimal weight 16. Therefore the function $g_1(\bar{x})$ is at distance 16 from $RM(2, 6)$. \square

From $g_1(\bar{x})$, by using the translation $\bar{x} \rightarrow \bar{x} + \bar{\alpha}$, $\bar{\alpha} \in \mathbb{F}_2^6$ and complementing the values, we can obtain 128 functions, which possess the same properties as $g_1(\bar{x})$.

The function $g_1(\bar{x})$ from Lemma 3 achieves maximal possible nonlinearity 24 among the 1-resilient functions of 6 variables, i.e. it is at distance 24 from $RM(1, 6)$. This holds since the Walsh spectrum of $g_1(\bar{x})$ is three valued, i.e. its Walsh transform values are 0, ± 16 only. In other words the

function $g_1(\bar{x})$ belongs to the class of so-called plateaued functions (see [17, 2]).

Theorem 2. *The covering radius of $RM(2, 6)$ in the sets $\mathcal{R}_{t,6}$, $t = 0, 1, 2$ is 16, i.e.,*

$$\hat{\rho}(t, 2, 6) = 16, \quad t = 0, 1, 2.$$

Proof. According to Lemma 2, any Boolean function at distance 18 from $RM(2, 6)$ has degree 3. By using the results in [6, p.113] we see that the unique orbit of the general linear group $GL(6, 2)$ in $RM(3, 6)/RM(2, 6)$, which has as a representative a coset of minimal weight 18, does not contain balanced functions. Therefore there exist no resilient functions at distance 18 from $RM(2, 6)$. On the other hand by Lemma 3 there exists a 2-resilient function at distance 16 from that code. To complete the proof we only need the obvious inclusion $\mathcal{R}_{t,n} \subset \mathcal{R}_{t-1,n}$. \square

4 The Covering Radius of $RM(2, 7)$ in the Set $\mathcal{R}_{t,7}$ for $t = 0, 1, 2, 3$

First, we shall prove that the covering radius of $RM(2, 7)$ in the set $\mathcal{R}_{3,7}$ is 32. Recall that due to the Siegenthaler's upper bound the degree of any 3-resilient function on \mathbb{F}_2^7 must be at most 3. From now on, when we say that a Boolean function f is linearly equivalent to \tilde{f} , we actually mean that f can be reduced by an invertible linear transformation of the variables to the Boolean function \tilde{f} .

The following lemma summarizes the results from Theorem 8.1 and Theorem 8.3 from [6].

Lemma 4. *Any Boolean function on \mathbb{F}_2^7 of degree 3 is linearly equivalent to a function with cubic part among:*

$$\begin{aligned}
f_2 &= x_1x_2x_3; \\
f_3 &= x_1x_2x_3 + x_2x_4x_5; \\
f_4 &= x_1x_2x_3 + x_4x_5x_6; \\
f_5 &= x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6; \\
f_6 &= x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6; \\
f_7 &= x_1x_2x_7 + x_3x_4x_7 + x_5x_6x_7; \\
f_8 &= x_1x_2x_3 + x_4x_5x_6 + x_1x_4x_7; \\
f_9 &= x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4x_7; \\
f_{10} &= x_1x_2x_3 + x_4x_5x_6 + x_1x_4x_7 + x_2x_5x_7; \\
f_{11} &= x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_6x_7; \\
f_{12} &= x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_6x_7 + x_2x_4x_7.
\end{aligned}$$

Let μ_j be the minimal weight of the coset $f_j + RM(2, 7)$, $2 \leq j \leq 12$. Then $\mu_2 = 16, \mu_3 = 24, \mu_4 = 28, \mu_5 = 32, \mu_6 = 36, \mu_7 = 28, \mu_8 = 32, \mu_9 = 36, \mu_{10} = 36, \mu_{11} = 40$ and $\mu_{12} = 36$.

Lemma 5. *Let f be a Boolean function on \mathbb{F}_2^7 of degree 3, linearly equivalent to a function with cubic part among $f_4, f_6, f_8, f_{10}, f_{11}$ or f_{12} . Then f cannot be 2-resilient.*

Proof. Suppose that f is 2-resilient and let \tilde{f} be the image of f under the linear transformation, such that the cubic part of $\tilde{f} \in \{f_4, f_6, f_8, f_{10}, f_{11}, f_{12}\}$. By [19, Lemma 2] and [11] the Walsh transform values of \tilde{f} are divisible by 16. Now applying Theorem 1 we get

$$W_{\tilde{f}}(0, 0, \dots, 1) + W_{\tilde{f}}(0, 0, \dots, 0) = 128 - 4 \cdot wt(\tilde{f}_{(0,0,\dots,1)}).$$

Thus, 4 is a divisor of $wt(\tilde{f}_{(0,0,\dots,1)})$. If $\tilde{f} \in \{f_4, f_8, f_{10}\}$ the function $\tilde{f}_{(0,0,\dots,1)}$ belongs to the coset $\tilde{f}_4 + RM(2, 6)$, if $\tilde{f} \in \{f_6, f_{11}, f_{12}\}$ then \tilde{f} belongs to the coset $\tilde{f}_6 + RM(2, 6)$ (recall that the subfunction $\tilde{f}_{(0,0,\dots,1)}$ is obtained by setting $x_7 = 0$). But from [6, p.113] we see that there is no weight divisible by 4 in these cosets, which leads to a contradiction. \square

Lemma 6. *Let f be a Boolean function on \mathbb{F}_2^7 of degree 3 linearly equivalent to a function with cubic part equal to $f_9 = x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4x_7$. Then f cannot be 3-resilient.*

Proof. We first proof by contradiction that a function \tilde{f} of the form $\tilde{f} = f_9 + g(\bar{x})$, where $g(\bar{x}) \in RM(2, 7)$, cannot be 3-resilient. Suppose the function f is 3-resilient. Notice that the weight of $\tilde{f}_{\bar{w}}$ is even, for each w with Hamming weight at most 3. By our assumption and Theorem 1, $W_{\tilde{f}}(\bar{w}) = 0$ for all \bar{w} with Hamming weight at most 3. Consider the following vectors $\bar{\omega}_i$, for $i = 1, \dots, 4$ with Hamming weight 4:

$$(0001111), (1010011), (1100101), (0110110).$$

These vectors are the only ones of Hamming weight 4 for which the corresponding function $\tilde{f}_{\bar{\omega}}$ from Theorem 1 has maximum degree and thus has odd Hamming weight. Applying Theorem 1 and Definition 1, those vectors have Walsh transform values which absolute value is equal to $32k$ with k an odd integer.

The vectors $\tilde{\omega}$ for which the set $\{\theta \mid \theta < \tilde{\omega}, wt(\tilde{\omega}) > 4 \text{ and } |W_{\tilde{f}}(\theta)| = 32k, \text{ with } k \text{ odd}\}$ has odd cardinality, will also have Walsh transform value with absolute value equal to $32k$ with k odd, based on the same arguments.

So, we also get the following vectors: 12 vectors of Hamming weight 5, formed by extending each of the previous vectors of Hamming weight 4:

$$\begin{aligned} &(0011111), (0101111), (1001111), \\ &(1110011), (1011011), (1010111), \\ &(1110101), (1101101), (1100111), \\ &(1110110), (0111110), (0110111) \end{aligned}$$

and four vectors of Hamming weight 6:

$$(1110111), (1111011), (1111101), (1111110).$$

In total we have 20 vectors which have nonzero Walsh transform values divisible by 32. The Parseval equation $\sum_{\omega} W_{\tilde{f}}^2(\omega) = 2^{14}$, leads to a contradiction.

However, because resiliency is not a linear invariant property, this proof does not imply that any other function which is linearly equivalent to a function of the class of f_9 , cannot be 3-resilient. If there exists a 3-resilient function which is linearly equivalent to a function of the class f_9 , it should be a plateaued function which has Walsh transform values equal to $\{-32, 0, 32\}$. This is explained by the fact that for a 3-resilient function the Walsh transform values should be divisible by 32 and the maximum Walsh value cannot be greater than 64 (otherwise the nonlinearity would

be less than 32, which contradicts the covering radius 36 of the class f_9). As the frequency distribution of the Walsh transform values is a linear invariant property, it suffices to show that there are no plateau functions with Walsh transform values equal to $\{-32, 0, 32\}$ in the set $\{f_9 + g(\bar{x}) \mid g(\bar{x}) \in RM(2, 7)\}$. By exhaustive search, we haven't found any function with Walsh spectrum $\{-32, 0, 32\}$. Also functions with 5-valued spectrum $\{-32, -16, 0, 16, 32\}$ do not belong to this set, which implies that there are no 2-resilient function which are linearly equivalent to a function of the class f_9 . \square

Lemma 7. *The Boolean function $g_2(\bar{x}) = x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_2 + x_1x_3 + x_2x_5 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7$ is 3-resilient and it is at distance 32 from $RM(2, 7)$.*

Proof. Since $g_2(x_1, \dots, x_7) = g_1(x_1, \dots, x_6) + x_7$ and g_1 achieves the covering radius if $RM(2, 6)$ in $\mathcal{R}_{2,6}$ then it is easy to see that $g_2(\bar{x})$ is 3-resilient and it is at distance 32 from $RM(2, 7)$. \square

The Walsh spectrum of $g_2(\bar{x})$ is three valued i.e. the Walsh transform values are 0, ± 32 only. Therefore the distance between g_2 and $RM(1, 7)$ is the maximal possible, namely 48.

Theorem 3. *The covering radius of $RM(2, 7)$ in the set $\mathcal{R}_{3,7}$ is 32.*

Proof. Lemma 5 and Lemma 6 imply that if a Boolean function is at distance greater than 32 from $RM(2, 7)$, it cannot be 3-resilient. On the other hand, by Lemma 7 there exists a 3-resilient function at distance 32 from $RM(2, 7)$, which completes the proof. \square

Theorem 4. *The covering radius of the Reed-Muller code $RM(2, n)$ in the set $\mathcal{R}_{n-4,n}$ is bounded from below by 2^{n-2} , when $n \geq 6$, i.e.*

$$2^{n-2} \leq \hat{\rho}(n-4, 2, n).$$

Proof. The proof is by induction on n . Lemma 3 is in fact the basis of the induction and then we proceed in a similar way as in Lemma 7.

In the following lemmas we improve the lower bounds for the covering radius in the sets $\mathcal{R}_{t,7}$ for $t = 0, 1$.

Proposition 1. *The Boolean function $g_3(\bar{x}) = x_1x_2x_3 + x_1x_4x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6 + x_1x_6x_7 + x_1 + x_2$ is 0-resilient (balanced) and it is at distance 40 from $RM(2, 7)$.*

Proposition 2. *The Boolean function $g_4(\bar{x}) = x_1x_2x_3 + x_1x_4x_7 + x_2x_4x_5 + x_3x_4x_6 + x_1x_7 + x_5 + x_6 + x_7$ is 1-resilient and it is at distance 36 from $RM(2, 7)$.*

In Table 2 below we present the numerical values of $\hat{\rho}(t, 2, n)$ that are obtained from Theorem 2, Theorem 3, Lemma 1 and Lemma 2.

Table 2. Numerical results for $\hat{\rho}(t, 2, n)$ from Theorem 2, Theorem 3, Lemma 1 and Lemma 2 (marked by (a), (b), (c) and (d) respectively). The entry $a - b$ means that $a \leq \hat{\rho}(t, r, n) \leq b$

	n	1	2	3	4	5	6	7
$t = 0$	$r = 2$			0	2	6	$16^{(a)}$	$40^{(c)}$ -44
$t = 1$	$r = 2$				0	6	$16^{(a)}$	$36^{(d)}$ -44
$t = 2$	$r = 2$					0	$16^{(a)}$	$32^{(b)}$ -44
$t = 3$	$r = 2$						0	$32^{(b)}$

5 Conclusions and Open Problems

In this paper we continued the study of the covering radius in the set of the resilient functions, started by [7]. This study is interesting because it enables us to investigate the trade-off among the resistance of different types of attacks.

Using some results of coding theory, we could find exact values in dimension 6 and improve the bounds in dimension 7 for the covering radius in the set of t -resilient functions with $t \leq n - 4$ of the second Reed-Muller code. We also generalized our methods to find a new lower bound for the covering radius in the set of the $n - 4$ resilient functions of the second Reed-Muller code.

The next step in our research is to improve the other lower bounds from Table 1 and to generalize our results for higher dimensions.

6 Acknowledgements

The joint work on the paper started during the visit of Yuri Borissov in K.U.Leuven. He would like to thank for the hospitality and the creative working environment at COSIC. Part of the work was done during the visit of Svetla Nikova visit in Ruhr University, Bochum. The authors were

partially supported by Concerted Research Action GOA-MEFISTO-666 of the Flemish Government.

References

1. E. Berlekamp, L. Welch, Weight Distribution of the Cosets of the (32,6) Reed-Muller Code, *IEEE IT*, vol. 18, January 1972, pp. 203-207.
2. C. Carlet, E. Prouff, On Plateaued Functions and their Constructions, *FSE'03*, Lund, Sweden, February 24-26, 2003, pp. 57-78.
3. N. Courtois, Higher Order Correlation Attacks, *XL Algorithm and Cryptanalysis of Toyocrypt*, ePrint Archive 2002/087, 2002.
4. N. Courtois, W. Meier, Algebraic Attacks on Stream Ciphers with Linear Feedback, *Eurocrypt'03*, LNCS 2656, Springer-Verlag 2003, pp. 345-359.
5. N. Courtois, A. Klimov, J. Patarin, A. Shamir, Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations, *Eurocrypt'00*, LNCS 1807, Springer-Verlag 2000, pp. 392-407.
6. X. D. Hou, $GL(m, 2)$ Acting on $R(r, m)/R(r-1, m)$, *Discrete Mathematics* vol. 149, 1996, pp. 99-122.
7. K. Kurosawa, T. Iwata, T. Yoshiwara, New Covering Radius of Reed-Muller Codes for t -Resilient Functions, *SAC'01*, LNCS 2259, Springer-Verlag 2001, pp. 75-86.
8. A. McLoughlin, The Covering Radius of the $(m-3)$ -rd Order Reed-Muller Codes and a Lower Bound on the $(m-4)$ -th Order Reed-Muller Codes, *SIAM J. Appl. Mathematics*, vol. 37, No. 2, October 1979, pp. 419-422.
9. F. J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
10. C. Carlet, P. Sarkar", Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions", *Finite Fields and Applications*, vol. 8, No. 1, January 2002, pp. 120-130.
11. P. Sarkar, S. Maitra, Nonlinearity Bounds and Constructions of Resilient Boolean Functions, *Crypto'00*, LNCS 1880, Springer-Verlag, 2000, pp. 515-532.
12. J. Schatz, The Second Order Reed-Muller Code of Length 64 has Covering Radius 18, *IEEE IT*, vol. 27, July 1981, pp. 529-530.
13. T. Siegenthaler, Correlation-Immunity of Non-linear Combining Functions for Cryptographic Applications, *IEEE Tran. on IT*, vol. 30, No. 5, 1984, pp. 776-780.
14. T. Siegenthaler, Decrypting a Class of Stream Ciphers Using Cyphertext Only, *IEEE Trans. Comp.* 34(1), 1985, pp. 81-85.
15. Y. Tarannikov, On Resilient Boolean Functions with Maximal Possible Nonlinearity, *Indocrypt'00*, LNCS 1977, Springer-Verlag 2000, pp. 19-30.
16. X. Guo-Zhen, J. Massey, A Spectral Characterization of Correlation-Immune Combining Functions, *IEEE IT*, vol. 34, No. 3, May 1988, pp. 569-571.
17. Y. Zheng, X. M. Zhang, Plateaued Functions, *ICICS'99*, LNCS 1726, Springer-Verlag 1999, pp. 284-300.
18. Y. Zheng, X. M. Zhang, Improved Upper Bound on the Nonlinearity of High Order Correlation Immune Functions, *SAC'00*, LNCS 2012, Springer-Verlag 2001, pp. 262-274.
19. Y. Zheng, X. M. Zhang, New Results on Correlation Immunity, *The 3rd International Conference on Information Security and Cryptography (ICISC'00)*, LNCS 2015, Springer-Verlag 2001, pp. 49-63.