Classification of Boolean Functions of 6 Variables or Less with Respect to Some Cryptographic Properties*

An Braeken[1], Yuri Borissov[2], Svetla Nikova[1], and Bart Preneel[1]

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

Abstract. This paper presents an efficient approach to the classification of the affine equivalence classes of cosets of the first order Reed-Muller code with respect to cryptographic properties such as correlation-immunity, resiliency and propagation characteristics. First, we apply the method to completely classify with this respect all the 48 classes into which the general affine group $AGL(2, 5)$ partitions the cosets of $RM(1, 5)$. Second, after distinguishing the 34 affine equivalence classes of cosets of $RM(1, 6)$ in $RM(3, 6)$ we perform the same classification for these classes.

1 Introduction

Many constructions of Boolean functions with properties relevant to cryptography are recursive. The efficiency of the constructions relies heavily on the use of appropriate functions of small dimensions. Another important method for construction is the random and heuristic search approach. As equivalence classes are used to provide restricted input of such optimization algorithms, it is very important to identify which equivalence classes obtain functions with desired properties.

In this paper, we present an efficient approach (based on some group-theoretical considerations) for the classification of affine equivalence classes of cosets of the first order Reed-Muller code with respect to cryptographic properties such as correlation-immunity, resiliency, propagation characteristics and

* The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT and by Concerted Research Action GOA Ambiorix 2005/11 of the Flemish Government. An Braeken is research assistent of the FWO.

L. Caires et al. (Eds.): ICALP 2005, LNCS 3580, pp. 324–334, 2005.

their combinations. We apply this method to perform a complete classification of all the 48 orbits of affine equivalent cosets of $RM(1,5)$ (classified by Berlekamp and Welch [1] according to weight distributions), with respect to the above mentioned cryptographic properties. Partial results for this case on the existence and their number have already been mentioned in [3, 13, 14, 16]. In this paper, we study this problem into more detail and show in which classes these functions appear and how to enumerate them. The method also allows us, if necessary, to generate all the Boolean functions of 5 variables that possess good cryptographic properties. Our approach can also be extended for Boolean functions of higher dimension. As an illustration we apply it to the cubic functions of 6 variables using a proper classification of the cosets of $RM(1,6)$ in $RM(3,6)$.

The paper is organized as follows. In Sect. 2, we present some general background on Boolean functions. In Sect. 3, we describe our approach which will be used in Sect. 4 for a complete classification of the affine equivalence classes of the Boolean functions of 5 variables. In Sect. 5, we first show how to derive the $RM(3,6)/RM(1,6)$ equivalence classes together with their sizes. Using this information we classify them according to the most important cryptographic properties.

2 Background on Boolean Functions

A Boolean function f is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. It can be represented by a *truth table*, which is a vector of length 2^n consisting of its function values $(f(\overline{0}),\ldots,f(\overline{1}))$. Another way of representing a Boolean function is by means of its *algebraic normal form* (ANF):

$$f(\overline{x}) = \bigoplus_{(a_1,\ldots,a_n)\in\mathbb{F}_2^n} h(a_1,\ldots,a_n)\, x_1^{a_1}\ldots x_n^{a_n}\,,$$

where f and h are functions on $\mathbb{F}_2^n$. The *algebraic degree* of f, denoted by $\deg(f)$, is defined as the highest number of variables in the term $x_1^{a_1}\ldots x_n^{a_n}$ in the ANF of f.

Two Boolean functions f_1 and f_2 on $\mathbb{F}_2^n$ are called *equivalent* if and only if

$$f_1(\overline{x}) = f_2(\overline{x}A \oplus \overline{a}) \oplus \overline{x}\overline{B}^t \oplus b,\;\; \forall x \in \mathbb{F}_2^n\,, \tag{1}$$

where A is a nonsingular binary $n\times n$-matrix, b is a binary constant, and $\overline{a},\overline{B}$ are n-dimensional binary vectors. If $\overline{B},b$ are zero, the functions f_1 and f_2 are said to be affine equivalent. A property is called affine invariant if it is invariant under affine equivalence.

The study of properties of Boolean functions is related to the study of *Reed-Muller codes.* The codewords of the r-th order Reed-Muller code of length 2^n, denoted by $RM(r,n)$, are the truth tables of Boolean functions with degree less or equal to r. The number of codewords is equal to $2^{\sum_{i=0}^{r}\binom{n}{i}}$ and the minimum number of positions in which any two codewords $\overline{u},\overline{v}$ differ (denoted by $d(\overline{u},\overline{v})$)

is 2^{n-r}. The *Hamming weight* of a vector $\overline{v}$ is denoted by $wt(\overline{v})$ and equals the number of non-zero positions, i.e. $wt(\overline{v}) = d(\overline{v}, \overline{0})$.

In 1972, Berlekamp and Welch classified all 2^{26} cosets of $RM(1,5)$ into 48 equivalence classes under the action of the general affine group $AGL(2,5)$ [1]. Moreover for each equivalence class the weight distribution and the number of cosets in that class has been determined.

Before describing the cryptographic properties that are investigated in this paper, we first mention two important tools in the study of Boolean functions f on $\mathbb{F}_2^n$. The *Walsh transform* of f is a real-valued function over $\mathbb{F}_2^n$ that can be defined as

$$W_f(\overline{\omega}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x}) \oplus \overline{x} \cdot \overline{\omega}} = 2^n - 2wt(f \oplus \overline{x} \cdot \overline{\omega}), \tag{2}$$

where $\overline{x} \cdot \overline{\omega} = \overline{x \omega}^t = x_1\omega_1 \oplus x_2\omega_2 \oplus \cdots \oplus x_n\omega_n$ is the *dot product* of $\overline{x}$ and $\overline{\omega}$. The *nonlinearity* N_f of the function f is defined as the minimum distance between f and any affine function which can be expressed as $N_f = 2^{n-1} - \frac{1}{2} \max_{\overline{\omega} \in \mathbb{F}_2^n} |W_f(\overline{\omega})|$.

The *autocorrelation function* of f is a real-valued function over $\mathbb{F}_2^n$ that can be defined as

$$r_f(\overline{\omega}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\omega})}. \tag{3}$$

For two equivalent functions f_1 and f_2 such that $f_1(\overline{x}) = f_2(\overline{x}A \oplus \overline{a}) \oplus \overline{x}\overline{B}^t \oplus b$, it holds that [15]:

$$W_{f_1}(\overline{w}) = (-1)^{\overline{a}A^{-1}\overline{w}^t + \overline{a}A^{-1}\overline{B}^t + b} W_{f_2}(((\overline{w} \oplus \overline{B})(A^{-1})^t) \tag{4}$$

$$r_{f_1}(\overline{w}) = (-1)^{\overline{w}\overline{B}^t} r_{f_2}(\overline{w}A). \tag{5}$$

A Boolean function is said to be *correlation-immune* of order t, denoted by $CI(t)$, if the output of the function is statistically independent of the combination of any t of its inputs. If the function is also *balanced* (equal number of zeros and ones in the truth table), then it is said to be *resilient* of order t, denoted by $R(t)$. These definitions of correlation-immunity and resiliency can be expressed by spectral characterization as given by Xiao and Massey [8].

Definition 1. *[8] A function $f(\overline{x})$ is $CI(t)$ if and only if its Walsh transform W_f satisfies $W_f(\overline{\omega}) = 0$, for $1 \leq wt(\overline{\omega}) \leq t$. If also $W_f(\overline{0}) = 0$, the function is called t-resilient.*

A Boolean function is said to satisfy the *propagation characteristics* of degree p, denoted by $PC(p)$ if the function $f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\omega})$ is balanced for $1 \leq wt(\overline{\omega}) \leq p$. If the function $f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\omega})$ is also t-resilient, the function f is called a $PC(p)$ function of order t. Or, by using the autocorrelation and Walsh spectrum, the definition can also be expressed as follows:

Definition 2. *[14] A function $f(\overline{x})$ is $PC(p)$ if and only if its autocorrelation transform r_f satisfies $r_f(\overline{\omega}) = 0$, for $1 \leq wt(\overline{\omega}) \leq p$. If also $W_{f(\overline{x}) \oplus f(\overline{x} \oplus \overline{w})}(\overline{a}) = 0$ for all $\overline{a}$ with $0 \leq wt(\overline{a}) \leq t$, the function f is said to satisfy $PC(p)$ of order t.*

If $r_f(\overline{\omega}) = \pm 2^n$, the vector $\overline{\omega}$ is called a *linear structure* of the function f. It is easy to prove that the set of linear structures forms a linear space [6].

We now present some known results which will be used in the rest of the paper. First of all, we start with mentioning several trade-offs between the above described properties of a Boolean function.

Theorem 1. *(Siegenthaler's Inequality [17]) If a function f on $\mathbb{F}_2^n$ is $CI(t)$, then $\deg(f) \leq n - t$. If f is t-resilient and $t \leq n - 2$, then $\deg(f) \leq n - t - 1$.*

Theorem 2. *[14] If a function f on $\mathbb{F}_2^n$ satisfies $PC(p)$ of order t with $0 \leq t < n - 2$, then $\deg(f) \leq n - t - 1$ for all p. If $t = n - 2$ then the degree of f is equal to 2.*

Theorem 3. *[20] If a function f on $\mathbb{F}_2^n$ is t-resilient and satisfies $PC(p)$, then $p + t \leq n - 1$. If $p + t = n - 1$, then $p = n - 1$, n is odd and $t = 0$.*

Another important result is the following divisibility theorem proven by Carlet and Sarkar [4].

Theorem 4. *If a coset of the $RM(1, n)$ with representative Boolean function f of degree d contains CI(t) (resp. t-resilient) functions, then the weights of the functions in $f + RM(1, n)$ are divisible by*

$$2^{t + \left\lfloor \frac{n-t-1}{d} \right\rfloor} \quad \textit{(resp. } 2^{t+1+\left\lfloor \frac{n-t-2}{d} \right\rfloor}\textit{)}. \tag{6}$$

From this Theorem together with Dickson's theorem on the canonical representations of quadratic Boolean functions [11], we derive a classification of correlation-immune (resp. resilient) quadratic functions in any dimension.

Proposition 1. *If the coset of $RM(1, n)$ with representative $x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2h-1}x_{2h} \oplus \varepsilon$ where ε is an affine function of x_{2h+1} through x_n and $h \leq \left\lfloor \frac{n}{2} \right\rfloor$ given by Dickson's theorem contains $CI(t)$ (resp. t-resilient) functions then*

$$h \leq n - t - \left\lfloor \frac{n-t-1}{2} \right\rfloor - 1 \ \textit{(resp. } h \leq n - t - \left\lfloor \tfrac{n-t-2}{2} \right\rfloor - 2\textit{)}.$$

Proof. The weight of the function equals (depending on the parameter h) [11]:

weight	$2^{n-1} - 2^{n-h-1}$	2^{n-1}	$2^{n-1} - 2^{n-h-1}$
number	2^{2h}	$2^{n+1} - 2^{2h+1}$	2^{2h}

The statement of the proposition follows from the divisibility theorem of Carlet and Sarkar applied on the weights. □

Remark 1. Using Proposition 1 together with the bound $h \leq \left\lfloor \frac{n}{2} \right\rfloor$, we obtain that the order of resiliency for quadratic functions is less or equal to $\left\lceil \frac{n}{2} \right\rceil - 1$, which was also stated in [18].

3 General Outline of Our Method

In this section we describe our main approach for the classification of equivalence classes (also called orbits) of cosets of the first order Reed-Muller code $RM(1,n)$ with respect to cryptographic properties such as correlation-immunity, resiliency, propagation characteristics and their combinations. For the sake of simplicity we shall refer to such a property as a *C-property.* For a given function f we denote by ZC_f the set of vectors which are mapped to zero by the transform corresponding to the considered C-property (e.g. Walsh transform for correlation-immunity and resiliency, autocorrelation for propagation characteristics) and call it a *zero-set* of f with respect to this C-property. We also refer to any set of n linearly independent vectors in $\mathbb{F}_2^n$ as a basis.

Our method employs the idea behind the "change of basis" construction as previously used by Maitra and Pasalic [12], and Clark et al. [5].

Let $\mathcal{R}$ be a representative coset of a given orbit $\mathcal{O}$ under the action of the general affine group $AGL(2,n)$. $\mathcal{R}$ is partitioned into subsets consisting of affine equivalent functions. Denote by $\mathcal{T}$ the family of these subsets. Let us fix one $T \in \mathcal{T}$ and a function $f \in T$.

From equations (4) and (5) and the definition of the corresponding C-property, it follows that for any function with this property, affine equivalent to f, a basis in ZC_f with certain properties exists. Conversely, for any proper basis in ZC_f and a constant from $\mathbb{F}_2^n$ we can apply an invertible affine transformation to f (derived by the basis and the constant) such that its image $\widetilde{f}$ possess the C-property. Therefore the number N_f of functions affine equivalent to f and satisfying a certain C-property can be determined by counting bases in ZC_f. Moreover it can be seen that this number does not depend on the specific choice of f from T, since for two different functions f_1 and f_2 from T there exists one-to-one correspondence between the sets of their proper bases in the zero-sets. It is important to note that in case of Walsh transform we use the fact that vector $\overline{B}$ defined in previous section is $\overline{0}$.

In the following theorem we prove the formula that gives the number $\mathcal{N}_C$ of functions with C-property in the orbit $\mathcal{O}$.

Theorem 5. *Let $\mathcal{R}$ be a representative coset of a given orbit $\mathcal{O}$ under the action of the general affine group $AGL(2,n)$. Then the number $\mathcal{N}_C$ of functions with C-property in this orbit can be computed by the formula:*

$$\mathcal{N}_C = K_{\mathcal{O}} \sum_{f \in \mathcal{R}} B_f, \tag{7}$$

where B_f is the number of proper bases in ZC_f and $K_{\mathcal{O}} = \frac{n!|\mathcal{O}|}{|GL(2,n)|}$.

Proof. We will find the number of functions with C-property in the orbit $\mathcal{O}$ by counting bases in zero-sets ZC_f. But this way we count each function $|S(f)| = S_f$ times, where $S(f)$ is the stabilizer subgroup of function f in $AGL(2,n)$. Therefore taking into account considerations preceding the theorem, the number

N_T of functions equivalent to the functions from T and satisfying the C-property is equal to

$$N_T = N_f = \frac{2^n n! B_f}{S_f}\,, \tag{8}$$

where B_f is the number of proper bases in ZC_f. The factor $n!$ appears since any arrangement of a given basis represents different function. Let $|\mathcal{O}|$ be the number of cosets in the orbit $\mathcal{O}$. Then substituting $S_f = \frac{|AGL(2,n)|}{|\mathcal{O}||T|}$ in (8) we get

$$N_T = \frac{2^n n! |\mathcal{O}| B_f |T|}{|AGL(2,n)|} = K_{\mathcal{O}} B_f |T|\,, \tag{9}$$

where $K_{\mathcal{O}} = \frac{n!|\mathcal{O}|}{|GL(2,n)|}$ and $GL(2,n)$ is the general linear group.

Therefore the number of all functions with C-property belonging to the orbit $\mathcal{O}$ is:

$$\sum_{T \in \mathcal{T}} N_T = K_{\mathcal{O}} \sum_{T \in \mathcal{T}} B_f |T| = K_{\mathcal{O}} \sum_{f \in \mathcal{R}} B_f\,. \tag{10}$$

□

In order to avoid difficulties when determining affine equivalent functions in $\mathcal{R}$ we prefer to use the last expression of (10). Thus, to compute the number $\mathcal{N}_C$ of functions with C-property in the orbit $\mathcal{O}$ we shall apply the following formula

$$\mathcal{N}_C = K_{\mathcal{O}} \sum_{f \in \mathcal{R}} B_f\,. \tag{11}$$

4 Boolean Functions of Less Than 5 Variables

For the study of functions in n variables with $n \leq 4$, we refer to [3] and [14]. In [3, Sect. 4.2], a formula is derived for the number of $(n-3)$-resilient functions and the number of balanced quadratic functions of n variables. In [14, Table 1], the number of quadratic functions that satisfy $PC(l)$ of order k with $k + l \leq n$ are determined for $n \leq 7$. Consequently, taking into account the trade-offs mentioned in Sect. 2, to cover all classes only the class with representative $x_1x_2x_3 \oplus x_1x_4$ with $n = 4$ should be considered in relation with its propagation characteristics. It can be easily computed by exhaustive search that its size is 26 880 and that it contains 2 816 $PC(1)$ functions.

We now count the number of functions satisfying correlation-immunity, resiliency, propagation characteristics and their combinations in each of the 48 affine equivalence classes of $RM(1,5)$ by using the method explained in Sect. 3. Note that only the cosets with even weight need to be considered. Numerical results can be found in tables 1 through 5. In the tables, the functions are represented by means of an abbreviated notation (only the digits of the variables) and the sum should be considered modulo 2. We refer to the extended version of the paper concerning details about the computation.

Table 1. The Number of functions satisfying 1-CI, 1-Resilient, 1-PC, 1-PC with resiliency properties

Representative	$\mathcal{N}_{CI(1)}$	$\mathcal{N}_{R(1)}$	$\mathcal{N}_{PC(1)}$	$\mathcal{N}_{PC(1)\cap Bal}$	$\mathcal{N}_{PC(1)\cap CI(1)}$	$\mathcal{N}_{PC(1)\cap R(1)}$
2345	512	0	0	0	0	0
2345+12	28 160	0	163 840	71 680	0	0
2345+23	1 790	0	0	0	0	0
2345+23+45	14 336	0	0	0	0	0
2345+12+34	1 146 880	0	0	0	0	0
2345+123	6 400	0	0	0	0	0
2345+123+12	76 800	0	0	0	0	0
2345+123+24	17 280	0	645 120	201 600	0	0
2345+123+14	385 400	0	737 280	253 440	640	0
2345+123+45	102 400	0	1 904 640	714 240	0	0
2345+123+12+34	230 400	0	0	0	0	0
2345+123+14+35	122 880	0	11 550 720	2 887 680	0	0
2345+123+12+45	7 680	0	0	0	0	0
2345+123+24+35	0	0	3 440 640	430 080	0	0
2345+123+145	138 240	0	276 480	77 760	0	0
2345+123+145+45	27 648	0	0	0	0	0
2345+123+145+24+45	414 720	0	1 966 080	614 400	4 160	0
2345+123+145+35+24	6 144	0	2 654 208	497 664	384	0
123	16 640	11 520	0		0	0
123+45	0	0	1 310 720	0	0	0
123+14	216 000	133 984	94 720	65 120	10 560	5 280
123+14+25	69 120	24 960	1 582 080	791 040	19 200	0
123+145	0	0	0	0	0	0
123+145+23	1 029 120	537 600	0	0	0	0
123+145+24	0	0	0	0	0	0
123+145+23+24+35	233 472	96 960	0	0	0	0
12	4 840	4 120	2 560	2 240	1 120	840
12+34	896	0	46 592	23 296	896	0

Table 2. The Number of 2-CI functions

Representative	$\mathcal{N}_{CI(2)}$	$\mathcal{N}_{CI(2)\cap PC(1)}$
123+145+23+24+35	384	0
12	640	120

Table 3. The Number of functions satisfying $PC(1)$ of order 1 and 2

Representative	$\mathcal{N}_{PC(1)\ of\ ord\ 1}$	$\mathcal{N}_{PC(1)\ of\ ord\ 2}$
123+45	5 120	0
123+14	30 720	0
12	2 240	960
12+34	13 952	704

Table 4. The Number of functions satisfying $PC(2)$

Representative	$\mathcal{N}_{PC(2)}$	$\mathcal{N}_{PC(2)\cap Bal}$	$\mathcal{N}_{PC(2)\cap CI(1)}$	$\mathcal{N}_{PC(2)\,of\,ord\,1}$	$\mathcal{N}_{PC(2)\,of\,ord\,2}$
2345+123+145+35+24	12 288	2 304	384	0	0
123+14+25	199 680	99 840	3 840	0	0
12+34	28 672	23 296	896	1 792	64

Table 5. The Number of functions satisfying $PC(3)$ and $PC(4)$

Representative	$\mathcal{N}_{PC(3)}$	$\mathcal{N}_{PC(4)}$	$\mathcal{N}_{PC(3)\cap Bal}$	$\mathcal{N}_{PC(4)\cap Bal}$	$\mathcal{N}_{PC(3)\,of\,ord\,1}$	$\mathcal{N}_{PC(4)\,of\,ord\,1}$
12+34	10 752	1 792	5 376	896	1 792	64

5 Boolean Functions of 6 Variables and Degree 3

In this section first we show how to find the 34 affine equivalence classes of $RM(3,6)/RM(1,6)$, together with the orders of their size. Then we count in each class the number of resilient and PC functions.

5.1 Classification of $RM(3,6)/RM(1,6)$

Table 1 in [9] presents the number of affine equivalence classes of $RM(s,6)$ in $RM(r,6)$ with $-1 \leq s < r \leq 6$. In $RM(3,6)/RM(1,6)$ there are 34 equivalence classes. In order to classify the affine equivalence classes in $RM(3,6)/RM(1,6)$, we use the 6 representatives $f_i \oplus RM(2,6)$ for $1 \leq i \leq 6$ of the equivalence classes of $RM(3,6)/RM(2,6)$ as given in [10]: $f_1 = 0, f_2 = 123, f_3 = 123 + 245, f_4 = 123 + 456, f_5 = 123 + 245 + 346, f_6 = 123 + 145 + 246 + 356 + 456$. For each representative, we run through all functions consisting only of quadratic terms and distinguish the affine inequivalent cosets of $RM(1,6)$ by using the frequency distribution of absolute values of the Walsh and autocorrelation distribution as affine invariants. These indicators suffice to distinguish all 34 affine equivalence classes.

In order to employ the approach described in Sect. 3 we also need to know the sizes of these orbits. They were computed during the classification phase by multiplying the final results by the sizes of the corresponding orbits in $RM(3,6)/RM(2,6)$ given in [10]. To check these results in the cases of f_2, f_4 and f_6 we obtained linear systems for unknown sizes by taking into account the weight distributions of the cosets of $RM(1,6)$ and the weight distribution of the corresponding representative of $RM(3,6)/RM(2,6)$ to which these cosets belong. Of course if $f_1 = 0$ one can use also [11, Theorem 1 and Theorem 2, p.436]. The results obtained in these two ways coincide. We refer to Table 6 for the sizes of the orbits.

Remark 2. The 150 357 affine equivalence classes were classified for the first time by Maiorana [7]. They also are mentioned on the webpage maintained by

Table 6. The number of resilient and PC functions in the classes of $RM(3,6)/RM(1,6)$

	Representative	$\mathcal{N}_{R(1)}$	$\mathcal{N}_{R(2)}$	$\mathcal{N}_{PC(1)}(\times 128)$	$\mathcal{N}_{PC(2)}(\times 128)$	Number of Cosets
f_1	12	51 800	14 840	121	0	651
	14+23	569 696	0	13 440	4 900	18 228
	16+25+34	0	0	13 888	13 888	13 888
f_2	0	532 480	44 800	0	0	$1\,395 \times 8$
	14	19 914 720	826 560	17 240	0	$1\,395 \times 392$
	24+15	49 257 600	268 800	1 249 440	52 080	$1\,395 \times 2\,352$
	16+25+34	0	0	1 874 880	1 874 880	$1\,395 \times 1\,344$
	45	0	0	929 280	0	$1\,395 \times 3\,584$
	123+16+45	0	0	18 744 320	1 881 600	$1\,395 \times 25\,088$
f_3	0	0	0	0	0	$54\,684 \times 32$
	13	416 604 160	5 174 400	0	0	$54\,684 \times 320$
	14	0	0	0	0	$54\,684 \times 480$
	16	0	0	21 396 480	0	$54\,684 \times 7\,680$
	26	0	0	33 152	0	$54\,684 \times 32$
	26+13	264 627 040	1 411 200	4 659 200	47 040	$54\,684 \times 320$
	26+14	0	0	14 058 240	1 411 200	$54\,684 \times 480$
	13+15+26+34	0	0	10 499 328	10 499 328	$54\,684 \times 192$
	34+16	0	0	0	0	$54\,684 \times 23\,040$
	34+13+15	$1\,89807 \cdot 10^{10}$	82 897 920	1 250 304	0	$54\,684 \times 192$
f_4	0	0	0	0	0	$357\,120 \times 64$
	14	0	0	2 486 400	0	$357\,120 \times 3\,136$
	15+24	0	0	$572\,315 \cdot 10^{10}$	0	$357\,120 \times 64$
	34+25+16	0	0	$505\,258 \cdot 10^{10}$	1 290 240	$357\,120 \times 64$
f_5	0	0	0	0	0	$468\,720 \times 448$
	12+13	0	0	3 609 586	0	$468\,720 \times 18$
	15	0	0	60 211 200	0	$468\,720 \times 14\,336$
	12+13+25	3 287 027 200	8 601 600	0	0	$468\,720 \times 2\,222$
	14+25	0	0	75 018 240	0	$468\,720 \times 1\,344$
	35+26+25+12	0	0	6 719 569 920	6 719 569 920	$468\,720 \times 14\,336$
	25+15+16	0	0	1 434 240	0	$468\,720 \times 64$
f_6	0	0	0	1 326 080	0	$166\,656 \times 3\,584$
	12+13	0	0	7 956 480	0	$166\,656 \times 21\,504$
	23+15+14	0	0	37 079 040	0	$166\,656 \times 7\,680$

Fuller: `http://www.isrc.qut.edu.au/people/fuller/` together with the degree, nonlinearity, maximum value in autocorrelation spectrum and truth tables of Boolean functions of dimension 6. Here we describe another approach for finding the 34 affine equivalence classes of functions of degree 3. One reason for this is that our method requires the sizes of the orbits, which are not given by Fuller.

5.2 Cryptographic Properties

In order to count the number of functions that satisfy certain cryptographic properties, the same approach as used for $n = 5$ is applied on these 34 classes of $RM(3,6)/RM(1,6)$. In Table 6, we present the classes together with the numbers of functions in these classes that satisfy t-resiliency with $t \leq 2$ and propagation characteristics of degree less or equal to 2. The last columns represents the sizes of the orbits.

By the Siegenthaler's inequality, 3-resilient functions should have degree less or equal to 2. Only the class with representative x_1x_2 contains 3-resilient functions and there are in total 1 120 3-resilient functions of dimension 6 (see also [3]).

For functions satisfying PC of higher degree, we have the following results. Besides the bent functions which are $PC(6)$, only the class with representative $x_1x_4 \oplus x_2x_3$ contains $PC(3)$ functions with a total of 128×420, as also computed in [14].

6 Conclusions

In this paper, we present a complete classification of the set of Boolean functions of 5 variables with respect to the most important cryptographic properties. Our method can also be applied to Boolean functions of dimension 6. As an example, we compute the 34 affine equivalence classes of $RM(3,6)/RM(1,6)$ and determine the number of resilient and PC functions belonging to each class. Moreover, we show a practical way to find the affine equivalence classes of Boolean functions. This method can be extended to dimension 7.

References

1. E. Berlekamp, L. Welch, Weight Distribution of the Cosets of the $(32,6)$ Reed-Muller Code, *IEEE Transactions on Information Theory*, Vol. 18, pp. 203-207, 1972.
2. E. Brier, P. Langevin, Classification of Boolean Cubic Forms of Nine Variables, *2003 IEEE Information Theory Workshop (ITW 2003)*, IEEE Press, pp. 179-182, 2003.
3. P. Camion, C. Carlet, P. Charpin, N. Sendrier, On Correlation-Immune Functions, *Crypto 1991*, LNCS 576, Springer-Verlag, pp. 86-100, 1992.
4. C. Carlet, P. Sarkar, Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions, *Finite Fields and Applications*, Vol. 8 (1), pp. 120-130, 2002.
5. J. Clark, J.L. Jacob, S. Stepney, S. Maitra, W. Millan, Evolving Boolean Functions Satisfying Multiple Criteria, *Indocrypt 2002*, LNCS 2551, Springer-Verlag, pp. 246-259, 2002.
6. J. H. Evertse, Linear Structures in Block Ciphers, *Eurocrypt 87*, LNCS 304, Springer-Verlag, pp. 249266.
7. J. Maiorana, A Classification of the Cosets of the Reed-Muller Code $R(1,6)$,*Mathematics of Computation*, vol. 57, No. 195, July 1991, pp. 403-414.
8. X. Guo-Zhen, J. Massey, A Spectral Characterization of Correlation-Immune Combining Functions, IEEE Transactions on Information Theory, Vol. 34 (3), pp. 569-571, 1988.
9. X. -D. Hou, $AGL(m,2)$ Acting on $RM(r,m)/RM(s,m)$, *Journal of Algebra*, Vol. 171, pp. 921-938, 1995.

10. X. -D. Hou, $GL(m,2)$ Acting on $R(r,m)/R(r-1,m)$, *Discrete Mathematics*, Vol. 149, pp. 99-122, 1996.
11. F. J. MacWilliams, N. J. A. Sloane, The Theory of Error- Correcting Codes, North-Holland Publishing Company, 1977.
12. S. Maitra, E. Pasalic, Further Constructions of Resilient Boolean Functions with Very High Nonlinearity, *IEEE Transactions on Information Theory*, Vol. 48 (7), pp. 1825-1834, 2002.
13. E. Pasalic, T. Johansson, S. Maitra, P. Sarkar, New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bounds on Nonlinearity, *Workshop on Coding and Cryptography 2001*, pp. 425-435, 2001.
14. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle, Propagation Characteristics of Boolean Functions, *Eurocrypt 1990*, LNCS 473, Springer-Verlag, pp. 161-173, 1990.
15. B. Preneel, Analysis and design of cryptographic hash functions, PhD. Thesis, Katholieke Universiteit Leuven, 1993.
16. P. Stanica, S.H. Sung, Boolean Functions with Five Controllable Cryptographic Properties, *Designs, Codes and Cryptography*, Vol. 31, pp. 147-157, 2004.
17. T. Siegenthaler, Correlation-Immunity of Non-linear Combining Functions for Cryptographic Applications, *IEEE Transactions on Information Theory*, Vol. 30 (5), pp. 776-780, 1984.
18. Y. Tarannikov, P. Korolev, A. Botev, Autocorrelation Coefficients and Correlation Immunity of Boolean Functions, *Asiacrypt 2001*, LNCS 2248, Springer-Verlag, pp. 460-479, 2001.
19. Y. Zheng, X. M. Zhang, GAC - the Criterion for Global Avalanche Characteristics of Cryptographic Functions, *Journal for Universal Computer Science*, Vol. 1 (5), pp. 316-333, 1995.
20. Y. Zheng, X. M. Zhang, On Relationship Among Avalanche, Nonlinearity, and Propagation Criteria, *Asiacrypt 2000*, LNCS 1976, Springer-Verlag, pp. 470-483, 2000.