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

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

[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. This paper presents an efficient approach for 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 all the 48 classes into which the general affine group $AGL(2,5)$ partitions the cosets of $RM(1,5)$. Second, we describe how to find the affine equivalence classes together with their sizes of Boolean functions in 6 variables. We perform the same classification for these classes. Moreover, we also determine the classification of $RM(3,7)/RM(1,7)$. We also study the algebraic immunity of the corresponding affine equivalence classes. Moreover, several relations are derived between the algebraic immunity and other cryptographic properties. Finally, we introduce two new indicators which can be used to distinguish affine inequivalent Boolean functions when the known criteria are not sufficient. From these indicators a method can be derived for finding the affine relation between two functions (if such exists). The efficiency of the method depends on the structure of the Walsh or autocorrelation spectrum.

1 Introduction

Many constructions of Boolean functions with properties relevant to cryptography are recursive [30, 24, 20, 28, 32]. 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 [24, 23]. 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 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 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 [24, 25, 4, 28]. In this paper, we go 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 $RM(3,6)$. We also describe the classification of $RM(3,7)/RM(1,7)$.

Since the introduction of algebraic attacks [8], we also need to take into account the property of algebraic immunity [22] in order to construct cryptographic "strong" functions. We derive relations

between the algebraic immunity and the properties weight, nonlinearity, linear structures, and normality. Moreover, we also compute the algebraic immunity of the affine equivalence classes of the cosets of $RM(1,5)$ and $RM(3,6)/RM(1,6)$.
Furthermore we introduce two new indicators for distinguishing affine inequivalent functions: we show that the number of bases in the set of vectors with the same absolute value in the Walsh spectrum and in the autocorrelation spectrum is an affine invariant. As already mentioned by Millan and Fuller [12], the frequency distribution of the absolute values in the Walsh and autocorrelation spectra does not suffice to distinguish all affine equivalence classes starting from dimension 6. For instance, there are 31 000 different Walsh and autocorrelation frequency distributions compared to the 150 357 affine equivalence classes. Using these new criteria we can distinguish affine inequivalent functions with the same Walsh spectrum and autocorrelation spectrum. This also leads to an efficient algorithm for finding the affine relations between two affine equivalent Boolean functions.
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 equivalence classes together with the orders of their sizes of Boolean functions in 6 variables. Using this information we classify the classes of $RM(3,6)/RM(1,6)$ according to the most important cryptographic properties. Finally in that section we describe our approach to classify $RM(3,7)/RM(1,7)$. Sect. 6 deals with the algebraic immunity of a function. In Sect. 7, we describe two new affine invariant properties and show how they can be used to find affine relations between two affine equivalent functions. Numerical results are presented in the Appendices.

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 number of variables in the longest 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 than 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 $\overline{x}\cdot\overline{\omega} = \overline{x}\overline{\omega}^t = x_1\omega_1 \oplus x_2\omega_2 \oplus \cdots \oplus x_n\omega_n$ 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 [26]:

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

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

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 [13].

Definition 1. *[13] A function $f(\overline{x})$ is $CI(t)$ if and only if its Walsh transform W_f satisfies $W_f(\overline{\omega}) = 0$, for $1 \le wt(\overline{\omega}) \le t$. 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 $1 \le wt(\overline{\omega}) \le p$. 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. *[25] A function $f(\overline{x})$ is $PC(p)$ if and only if its autocorrelation transform r_f satisfies $r_f(\overline{\omega}) = 0$, for $1 \le wt(\overline{\omega}) \le p$. If also $W_{f(\overline{x})\oplus f(\overline{x}\oplus\overline{w})}(\overline{a}) = 0$ for all $\overline{a}$ with $0 \le wt(\overline{a}) \le t$, 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 [10].
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 [29]) If a function f on $\mathbb{F}_2^n$ is $CI(t)$, then $\deg(f) \le n-t$. If f is t-resilient and $t \le n-2$, then $\deg(f) \le n-t-1$.*

Theorem 2. *[25] If a a function f on $\mathbb{F}_2^n$ satisfies $PC(p)$ of order t with $0 \le t < n-2$, then $\deg(f) \le n-t-1$ for all p. If $t = n-2$ then the degree of f is equal to 2.*

Theorem 3. *[34] If a function f on $\mathbb{F}_2^n$ is t-resilient and satisfies $PC(p)$, then $p+t \le n-1$. 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 [6].

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*

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

From this Theorem together with Dickson's theorem on the canonical represenations of quadratic Boolean functions [19], 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 $\sum_{i=0}^{h} x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2h-1}x_{2h} \oplus \varepsilon$ 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) function 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 to (depending on the parameter h) [19]:

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 [31].

3 General Outline of Our Method

In this section we shall give a description of 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*. We call any set of n linearly independent vectors in $\mathbb{F}_2^n$ a basis. The method employs the idea behind the "change of basis" construction as previously used by Maitra and Pasalic [21], and Clark et al. [7].

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 $f \in T$. We shall 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) which we shall also call a *zero-set* of f.

From equations (4) and (5) and the definition of the corresponding C-property, it follows that for any function with this property which is 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 affine transformation to f (derived by the basis and the constant) such that its image $\widetilde{f}$ possesses the C-property. Therefore the number N_f of functions that are affine equivalent to f and satisfy 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 a one-to-one correspondence between the sets of their proper bases in the zero-sets. However, in this way we count each function with a C-property $|S(f)| = S_f$ times, where $S(f)$ is the stabilizer subgroup of function f in $AGL(2,n)$. Therefore the number N_T of functions affine equivalent to the functions from T satisfying the C-property is equal to

$$N_T = N_f = \frac{2^n n! B_f}{S_f}\,, \tag{7}$$

where B_f is the number of proper bases in ZC_f. The factor $n!$ appears because any arrangement of a given basis represents different function.
Let $\nu_{\mathcal{O}}$ is the number of cosets in the orbit $\mathcal{O}$. Then substituting $S_f = \frac{|AGL(2,n)|}{\nu_{\mathcal{O}}|T|}$ in (7) we get

$$N_T = \frac{2^n n! \nu_{\mathcal{O}} B_f |T|}{|AGL(2,n)|} = K_{\mathcal{O}} B_f |T|\,, \tag{8}$$

where $K_{\mathcal{O}} = \frac{n!\nu_{\mathcal{O}}}{|GL(2,n)|}$ 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:

$$\sum_{T\in\mathcal{T}} N_T = K_{\mathcal{O}} \sum_{T\in\mathcal{T}} B_f|T| = K_{\mathcal{O}} \sum_{f\in\mathcal{R}} B_f\,. \tag{9}$$

In order to avoid difficulties when determining affine equivalent functions in $\mathcal{R}$ we will use the last expression of (9). Thus, to compute the number $\mathcal{N}_C$ of functions with C-property in the orbit $\mathcal{O}$ we shall apply the following formula

$$\mathcal{N}_C = K_{\mathcal{O}} \sum_{f\in\mathcal{R}} B_f. \tag{10}$$

4 Boolean Functions of 5 Variables

For the study of functions in n variables with $n \le 4$, we refer to [4] and [25]. In [4, Section 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 [25, Table 1], the number of quadratic functions that satisfy $PC(l)$ of order k with $k + l \le n$ are determined for $n \le 7$. Consequently, taking into account the trade-offs mentioned in Section 2, to cover all classes only the class with representative $x_1x_2x_3 \oplus x_1x_4$ in $n = 4$ 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 2816 $PC(1)$ 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 Section 3.

4.1 Correlation-Immune Functions

When we take into account Siegenthaler's inequality, we expect to find for functions of 5 variables $CI(1)$ functions of degree 4, $CI(1)$ and $CI(2)$ functions of degree 3, $CI(1)$, $CI(2)$ and $CI(3)$ functions of degree 2. Notice that only the linear functions $x_1\oplus x_2\oplus x_3\oplus x_4\oplus x_5\oplus c$ with $c \in \{0,1\}$ satisfy $CI(4)$.
We counted the number of correlation-immune functions in each class, according to the classification of Berlekamp and Welch, adapting the method described in the previous section for $n = 5$.
In this case we consider the sets ZW_f of vectors with zeroes in the Walsh spectrum $\mathrm{ZW}_f = \{\overline{w}|W_f(\overline{w}) = 0\}$, where f runs through the representative coset. A function that satisfies $CI(1)$ can be constructed from a basis of ZW_f by using the affine transformation $(\overline{x} \oplus \overline{a})(A^{-1})^t$ of the

input vector $\overline{x}$, where A is the matrix with rows containing the vectors of the basis in ZW_f and $\overline{a}$ is an arbitrary constant in $\mathbb{F}_2^n$. This property follows easily from relation (4). For functions that satisfy a higher order $t > 1$ of correlation-immunity, a proper basis should have the additional property that any sum of at least t basis vectors also belongs to ZW_f. It is easy to see that a $CI(t)$ function exists if and only if a basis that satisfies this property exists.
By applying (10) we compute the number of CI functions of orders 1, 2 and 3. The values of $\mathcal{N}$ for CI functions of 5 variables are given in Appendix B.1 and B.2.
Note that there are two cosets for which the set of balanced functions is divided into at least two subsets containing affine inequivalent functions. Namely these are the cosets with representatives $x_1x_2x_3 \oplus x_1x_4$ and $x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3$. These subsets contain functions with the same weight – 16, the same Walsh and autocorrelation spectrum but the number of bases B_f is different (see Table 1).

Table 1. Number of Bases in Coset

coset representative	B_f
x_1x_2	39552
$x_1x_2x_3$	16128
$x_1x_2x_3 \oplus x_1x_4$	$\begin{cases} 10240 \\ 9456 \end{cases}$
$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5$	1248
$x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3$	$\begin{cases} 4464 \\ 4232 \end{cases}$
$x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_5$	1512

4.2 Resilient Functions

The number of balanced (0-resilient) Boolean function of 5 variables is equal to $\binom{32}{16} = 601\,080\,390$. This number can also be obtained by computing the sum of the numbers of balanced functions in each even coset multiplied by the number of cosets in its orbit. (see Table 2 in [1]).
For 1-resilient functions, only the classes of Boolean functions with degree less or equal than 3 need to be considered. Equation (6) excludes three more cases, namely the orbits with representatives $x_1x_2x_3 \oplus x_4x_5$, $x_1x_2x_3 \oplus x_1x_4x_5$, $x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4$. To adapt our method for this case it makes sense to consider the zero-sets in Walsh spectrum only of balanced functions.
Because of Siegenthaler's inequality, 2-resilient functions of 5 variables have degree smaller or equal than 2. Then (6) implies that the weights are divisible by 8, which is not satisfied by the coset with representative $x_1x_2 \oplus x_3x_4$. The only class that can contain 2-resilient functions is those with representative x_1x_2. Their number turns out to be 520 as previously obtained in [4].
The number of resilient functions in each class is presented in Appendix B.1.

4.3 Propagation Characteristics

The frequency distribution of the autocorrelation values is an affine invariant property. In Appendix A, the autocorrelation spectra are computed for the representative cosets.
We can again apply the method from Sect. 3, using the zero-sets in the autocorrelation spectra [7]. This time, we apply the transformation $A^t\overline{x}^t$ on the input variables, with A a 5×5-matrix with rows the vectors of a basis for which the autocorrelation is zero. Similarly as for the case of

correlation-immune functions, there is a one-to-one correspondence between PC functions and such bases.

Remark 2. Note that for CI and resilient functions an arbitrary constant $\overline{a} \in \mathbb{F}_2^n$ was involved also in the transformation. This follows for PC functions from the fact that all functions $f(\overline{x}) \oplus \overline{x} \cdot \overline{a}$, $\forall \overline{a} \in \mathbb{F}_2^n$ have the same autocorrelation spectrum and thus the same level of PC.

As all functions belonging to a given coset have equal autocorrelation spectrum (in absolute value), we only need to count for the number of bases for one function in a coset. Consequently, this simplifies formula (10).

Note that functions which satisfy $PC(3)$ should have at least 25 zeroes in their autocorrelation spectra. This is satisfied only by the functions of the classes with representatives $x_1x_2 \oplus x_3x_4$ and $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5$. As proven for general dimension n in [5], functions that satisfy $PC(n-2)$ are of the form

$$g(x_1 \oplus x_n, \ldots, x_{i-1} \oplus x_n, x_i, x_{i+1} \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n)\,,$$
$$g(x_1 \oplus x_{n-1}, \ldots, x_{n-2} \oplus x_{n-1}, x_n) \oplus h(x_1, \ldots, x_n)\,,$$

where g is a bent function of dimension n and h is any affine function on $\mathbb{F}_2^n$. Moreover, functions satisfying $PC(n-1)$ are functions of the form $g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n)$, where g and h are defined above. As a consequence, only the class of $x_1x_2 \oplus x_3x_4$ contains $PC(3)$ and even $PC(4)$ functions, for which the number after computation turns out to be equal to 10 752 and 1792. The number 1792 for quadratic $PC(4)$ functions coincides with the result of [25]. We also get the same number as obtained by [25] for the number of quadratic functions satisfying PC of order p with $p \leq 4$. Moreover, we could conclude that there is only one class of degree 4 that contains $PC(2)$ functions. The numbers can be found in Appendix B.4 and B.5.

Note that in the set of orbits wich have as representatives odd cosets, there are no Boolean functions that satisfy a certain order of PC. This follows from the fact that if the autocorrelation has zeroes, the degree of the function should be less or equal than $n-1$, as proven in [25].

4.4 Propagation Characteristics and Correlation-Immunity

In order to compute the number of functions that satisfy both PC and CI (resp. resiliency), we determine first all PC functions and search in this set for functions that satisfy CI (resp. resiliency), where we take into account the divisibility theorem and the trade-off between the order of resiliency and the degree of PC into account. The balanced $PC(1)$ function with nonlinearity 12 and sum of the squared autocorrelation values equal to 1664, used in [28] can be found in the class of $x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_2x_4 \oplus x_3x_5$. In the Appendices B.1, B.2 and B.4, the numbers corresponding to the different classes are presented.

4.5 Propagation Characteristics of order t

Taking into account the tradeoff between the degree and the order of PC, we can now also search in the set of $PC(p)$ functions for functions that satisfy $PC(p)$ of order t. The results can be found in the Appendix B.3. Note that the numbers for all functions of degree 2 coincide with the results of [25].

5 Boolean Functions of 6 and 7 Variables

5.1 Equivalence Classes

The 150 357 equivalence classes (also called orbits) of the cosets of $RM(1,6)$ were firstly classified by Maiorana [11] in 1991. The truth tables of the representatives of Boolean functions with 6 input variables together with the degree, nonlinearity, maximum value in autocorrelation spectrum can also be found on the webpage maintained by Fuller: `http://www.isrc.qut.edu.au/people/fuller/`. But for our approach, we also need to know the sizes of the orbits. Therefore, we present a new method to derive the equivalence classes of Boolean functions in 6 variables.
The central task is to derive the equivalence classes of $RM(3,6)/RM(1,6)$. These classes can be obtained from the 6 representatives $f_i \oplus RM(2,6)$ for $1 \leq i \leq 6$ of $RM(3,6)/RM(2,6)$ as given in [17]. For each representative, we run through all functions which are sum of the representative with functions consisting only of quadratic terms and distinguish the affine inequivalent cosets of $RM(1,6)$ by using as invariants the frequency distribution of absolute values of the Walsh and autocorrelation spectra. These indicators suffice to distinguish all 34 affine equivalence classes.
In order to determine the equivalence classes of $RM(4,6)/RM(1,6)$, we start from the classes of $RM(4,6)/RM(2,6)$. These classes are immediately derived by dualizing the equivalence classes of $RM(3,6)/RM(1,6)$. Then, for each representative of $RM(4,6)/RM(2,6)$, we run through all functions consisting only of quadratic terms and distinguish the affine inequivalent cosets of $RM(1,6)$. Here, the invariants of frequency distribution of absolute values of the Walsh and autocorrelation spectra are not sufficient for finding all 2499 different classes. In combination with the invariant of the restrictions with respect to a hyperplane, the problem is solved. Here, for each representative the set of restrictions with respect to all 126 hyperplanes $c_1x_1 \oplus \cdots \oplus c_6x_6 \oplus c_7$ where $(c_1, \ldots, c_6) \in \mathbb{F}_2^6 \setminus \overline{0}$ and check to which of the 29 affine equivalence classes of $RM(4,5)/RM(1,5)$ it belongs. Therefore, it suffices to use the invariants of Walsh and autocorrelation spectrum. The classes of $RM(5,6)/RM(1,6)$ and $RM(6,6)/RM(1,6)$ are found in a similar way (with the same invariants but now the restrictions belong to one of the 48 equivalence classes of $RM(5,5)/RM(1,5)$). We start again from the classes of $RM(5,6)/RM(2,6)$ and $RM(6,6)/RM(2,6)$. In order to obtain the classes of $RM(5,6)/RM(2,6)$ and $RM(6,6)/RM(2,6)$, we need to dualize the equivalence classes of $RM(3,6)/RM(0,6)$ and $RM(3,6)/RM(-1,6)$. The equivalence classes of $RM(3,6)/RM(0,6)$ are found by running through all linear functions. The 120 different classes could then be distinguished by using as invariants the size of the annihilator set together with the number of flats on which a Boolean function is constant. Once the 120 equivalence classes of $RM(3,6)/RM(0,6)$ are obtained, the weight of the function determines if the respresentative of $RM(3,6)/RM(0,6)$ leads to one or two classes in $RM(3,6)/RM(-1,6)$.

5.2 Sizes of the Orbits

In order to employ the approach described in Sect. 3 we also need to know the sizes of these orbits. Let us first describe how to find the sizes of the representatives of $RM(3,6)/RM(1,6)$. The sizes were computed during the classification phase multiplying the final results by the sizes of the corresponding orbits in $RM(3,6)/RM(2,6)$ given in [17]. 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 [[19] Theorem 1 and Theorem 2, p.436]. The results obtained in these two ways coincide.
Also the sizes of $RM(3,6)/RM(0,6)$ and $RM(3,6)/RM(-1,6)$ were obtained during the classification phase, where we only need to run through all linear functions and constant functions respectively.

Since dual classes have the same sizes, the sizes of $RM(4,6)/RM(2,6)$, $RM(5,6)/RM(2,6)$, and $RM(6,6)/RM(2,6)$ are also known. Finally the sizes of $RM(4,6)/RM(1,6)$, $RM(5,6)/RM(1,6)$, and $RM(6,6)/RM(1,6)$ are again obtained in the classification phase by running through all functions consisting only of quadratic terms.

As an example, the representatives of the 34 equivalence classes of $RM(3,6)/RM(1,6)$, together with the number of cosets in each class, the Walsh spectrum and the autocorrelation spectrum are given in Appendix C. Then we count in each class the number of resilient and PC functions.

5.3 Cryptographic Properties

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 Appendix C.1, we present the classes together with the numbers of functions in these classes that satisfy resiliency and propagation characteristics.

5.4 Cubic Boolean Functions of 7 Variables

We start from the 12 equivalence classes of $RM(3,7)/RM(2,7)$ as given in [17] and run through all functions which are sum of representative with functions containing only quadratic terms. The fastest known invariant which leads to the complete classification is the invariant of the restrictions with respect to a hyperplane. For every explored function f, we compute all its restrictions with respect to the hyperplanes and determine corresponding affine equivalence classes of $RM(3,6)/RM(1,6)$ to which they belong. In order to do this, we first find out the class of a given restriction f_h in $RM(3,6)/RM(2,6)$ by the invariant $\delta(f_h) = (\delta_0(f_h), \delta_1(f_h), \delta_2(f_h), \delta_3(f_h))$, where $\delta_i(f_h) = |\{\overline{a} \in \mathbb{F}_2^6 : D_{\overline{a}}(f_h)$ is a plateaued function with an amplitude $2^{6-i}\}|$ for $0 \leq i \leq 3$, and then use the invariants of Walsh and autocorrelation spectrum to further distinguish its class in $RM(3,6)/RM(1,6)$.

The sizes of the orbits are computed during the classification phase (as in the case of 6 variables) and finally we multiply them by the sizes of the corresponding orbits of $RM(3,7)/RM(2,7)$, which can be found for example in [2]. We refer to Appendix D for a list of the 179 representatives of $RM(3,7)/RM(1,7)$ together with the sizes of the orbits.

The classification of $RM(3,7)/RM(1,7)$ has been recently and independently done by M. Qing-Shu et.al. in [27].

6 Algebraic Immunity

6.1 Invariance

The property of algebraic immunity is invariant under affine transformation, i.e. $f(\overline{x})$ and $f(\overline{x}A \oplus \overline{b})$, where A is an $n \times n$ matrix and $\overline{b} \in \mathbb{F}_2^n$ will have the same algebraic immunity. It is clear that if g is annihilator of f, then $g(\overline{x}A \oplus \overline{b})$ is annihilator of $f(\overline{x}A \oplus \overline{b})$.

However, the algebraic immunity of two functions $f(\overline{x})$ and $f(\overline{x}) \oplus \overline{c} \cdot \overline{x}$ with $\overline{c} \in \mathbb{F}_2^n$ can differ at most with 1. This can be easily seen as follows. Let g be annihilator of f such that $f(\overline{x}) \cdot g(\overline{x}) = 0$, then $g(\overline{x})(\overline{c} \cdot \overline{x} \oplus 1)$ is annihilator of $(f(\overline{x}) \oplus \overline{c} \cdot \overline{x})$ because $(f(\overline{x}) \oplus \overline{c} \cdot \overline{x})g(\overline{x})(\overline{c} \cdot \overline{x} \oplus 1) = f(\overline{x})g(\overline{x})(\overline{c} \cdot \overline{x} \oplus 1) \oplus (\overline{c} \cdot \overline{x})g(\overline{x})(\overline{c} \cdot \overline{x} \oplus 1) = 0$. The last equality follows from the fact that $\overline{c} \cdot \overline{x} \oplus 1$ is annihilator of $\overline{c} \cdot \overline{x}$. Finally note that the degree of $g(\overline{x})(\overline{c} \cdot \overline{x} \oplus 1)$ is upperbounded by $\deg(g) + 1$.

6.2 Relation with weight of the function

Theorem 5. *If $wt(f) < \sum_{i=0}^{d} \binom{n}{i}$ or $2^n - wt(f) < \sum_{i=0}^{d} \binom{n}{i}$, then there exists annihilator of f of degree at most d.*

Proof. In order to find function g for which $g \cdot f = 0$, we need to solve a system of $wt(f)$ linear equations, where the unknowns are the ANF coefficients of g (see [22, Section 5]). Since the system is homogeneous and the rank of the system is less than the number of unknowns, i.e. $wt(f) < \sum_{i=0}^{d} \binom{n}{i}$, it has non trivial solution. $\square$

As a consequence, we can conclude that the weight of the function or the order of balancedness is an important factor related to the algebraic immunity. Theorem 5 also shows that the AI is less or equal than $\lceil \frac{n}{2} \rceil$ as already proven in [8]. Moreover, Theorem 5 also implies that it does not exist a non-balanced function of n variables with n odd achieving the maximum AI $\lceil \frac{n}{2} \rceil$.

6.3 Relation with Walsh coefficients

Theorem 6. *If $\max_{v \in \mathbb{F}_2^n} |W_f(v)| > 2^n - 2\sum_{i=0}^{d-1} \binom{n}{i}$ then $AI(f) \leq d$.*

Proof. As already explained in Section 6.1, the AI of $f(\overline{x})$ and $f_{\overline{c}}(\overline{x}) = f(\overline{x}) \oplus \overline{c} \cdot \overline{x}$ can differ at most with 1. Since the Walsh coefficients of the two functions are related by $W_{f_{\overline{c}}}(\overline{v}) = W_f(\overline{v} \oplus \overline{c})$ for all $\overline{v} \in \mathbb{F}_2^n$, both functions have the same Walsh spectrum. Therefore, the condition on the weight of the function from Theorem 5 can be transformed into a condition on the Walsh coefficients of the function using Equation (2) but now with respect to annihilator of degree $d-1$. $\square$

The above theorem can be slightly improved.

Theorem 7. *If $\max_{\overline{v} \in \mathbb{F}_2^n} |W_f(\overline{v})| > 2^n - 2\left(\sum_{i=0}^{d-1} \binom{n}{i} + \binom{n-1}{d-1}\right) + 1$ then $AI(f) \leq d$.*

Proof. We will prove the following equivalent statement: if $wt(f) < \sum_{i=0}^{d-1} \binom{n}{i} + \binom{n-1}{d-1}$, then all functions in the coset of $RM(1,n)$ with representative f will have AI less or equal to d.
If $wt(f)$ satisfies this condition, there might not exist annihilator of f of degree $d-1$ but there are at least $\binom{n}{d} - \binom{n-1}{d-1} + 1 = \binom{n-1}{d} + 1$ degrees of freedom to choose annihilator of degree d. Let us fix a function $f_{\overline{c}}(\overline{x}) = f(\overline{x}) \oplus \overline{c} \cdot \overline{x}$ from the coset. Since $g(\overline{x})(\overline{c} \cdot \overline{x} \oplus 1)$ is annihilator of $f_{\overline{c}}(\overline{x})$, where $g(\overline{x})$ is an arbitrary function from the annihilator set of f, it can be easily seen that an annihilator of $f_{\overline{c}}(\overline{x})$ of this type with degree equal to d, will satisfy in addition at most $\binom{n-1}{d}$ linear constraints. Therefore we can construct a nontrivial such annihilator of $f_{\overline{c}}(\overline{x})$ of degree at most d. $\square$

Theorem 7 shows the relation between the nonlinearity of the function and its AI. Functions with bad nonlinearity have also low AI.

6.4 Relation with Linear Structures

It is well-known (see for instance [10],[18]) that any function with linear space of dimension k can be transformed by an affine transformation in the sum of two functions f_1 and f_2 where f_1 is a nonlinear function that depends on $n-k$ variables and f_2 a linear function. Since the AI of f_1 is less or equal than $\lceil \frac{n-k}{2} \rceil$, the AI of f will be less or equal than $\lceil \frac{n-k}{2} \rceil + 1$. Consequently, functions with linear space of dimension greater or equal than 4 for n even and 3 for n odd cannot have the maximal AI of $\lceil \frac{n}{2} \rceil$.

6.5 Relation with Normality and ANF

A function f on $\mathbb{F}_2^n$ is called k-(weakly) normal if there exists a flat V of dimension k such that f is (affine) constant when restricted to V. By definition, weakly normality is a property which is invariant under addition of a linear function. The next theorem, which represents a trade-off between AI and normality of a function, can be derived from [22, Section 4.1].

Theorem 8. *A function which is k-normal (k-weakly normal) has an annihilator of degree $n-k$ $(n-k+1)$.*

6.6 Functions of 5 and 6 variables w.r.t. AI

Dimension 5 A study on the 48 affine equivalence classes of the cosets of $RM(1,5)$ with respect to the algebraic immunity shows that Theorem 7 is rather strong. It allows to exclude 38 classes when considering functions with maximum possible AI (i.e. 3). From the 10 remaining classes, it turns out that there are 5 classes of degree 4 and 1 class of degree 3 that contain functions with algebraic immunity 3. Two classes of degree 4 can be distinguished in which not all balanced functions have $AI = 3$.
Note that all 2 304 balanced $PC(2)$ functions in the class of $x_2x_3x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_3x_5 \oplus x_2x_4$ have $AI = 3$, since all its balanced functions have this immunity. Consequently there does not seem to exist a trade-off between the properties PC and AI. Moreover, also a high maximum value in the autocorrelation spectrum (related to the absolute indicator $D_\infty f$ of the global avalanche characteristics [33]) does not seem to be related to the algebraic immunity since there are two functions with AI equal to 3 and with $D_\infty f = 24$. However this parameter can be related in some sense to the considered property because it determines the algebraic immunity of the first order derivatives of f.
It turns out that in the class of $x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_5$ there are 96 960 1-resilient functions which all have AI equal to 3. As a consequence, also between AI and resiliency there does not seem to exist a trade-off. See Appendix B.1 where we computed the number of cosets, denoted by $\mathcal{N}_{cos,AI=3}$, of the different classes which have $AI = 3$.

Dimension 6 and degree 3 Classes where all cosets contain only functions with AI less than 3 are very rare. Here Theorem 8 is efficient in order to distinguish these classes. The following representatives which have cosets with $AI \leq 2$ were found: $x_1x_2x_3$, $x_1x_2x_3 \oplus x_1x_4$, $x_1x_2x_3 \oplus x_1x_6 \oplus x_2x_5 \oplus x_3x_4$, $x_1x_2x_3 \oplus x_2x_4x_5$, $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_6$, $x_1x_2x_3 \oplus x_4x_5x_6$.
It is interesting to note also that all bent functions in the coset of $f = x_1x_2x_3 \oplus x_1x_6 \oplus x_2x_5 \oplus x_3x_4$ have AI equal to 2, from which we conclude that only high nonlinearity is not sufficient in order to have maximum possible algebraic immunity.

7 Affine Invariant Properties

The interest in studying linear and affine equivalence classes of Boolean functions for design of switching circuits dates already from the 1960s [14]. The problem of counting equivalence classes was solved for $n \leq 6$ in 1964 by Harrison [15] using Polya theory [9], by computing the cycle index polynomial of the linear and affine classes. Recently, Fuller and Millan posed the question whether affine equivalent Boolean functions introduce weaknesses in a cryptographic cipher [12]. They designed an algorithm for determining when two Boolean functions are affine equivalent by exploiting a new affine invariant property based on the local connection structure of the affine

equivalence classes. We now present two new affine invariant properties and show how they can be used in order to find the affine relation between two affine equivalent functions.
From the classification of correlation-immune and resilient functions, we could derive the following property.

Proposition 2. *The number of bases into the set of vectors with the same absolute value in the Walsh spectrum is an affine invariant property.*

The proof of this proposition follows from the fact that between the sets of bases there exists a bijective correspondence as expressed in (4). This new indicator for affine equivalence enables us in some cases to determine if two functions with the same frequency distribution of the Walsh spectrum are affine inequivalent. For instance, the functions $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5$, $x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_5$, $x_1x_2 \oplus x_3x_4$ have the same weight distribution of the corresponding cosets (see Appendix A), but by computing the number of bases in the zero-sets of their Walsh spectra we obtain 5 118 976, 5 099 264 and 5 203 968 bases respectively.
The classification of PC functions gives a similar property concerning the autocorrelation spectrum.

Proposition 3. *The number of bases into the set of vectors with the same absolute value in the autocorrelation spectrum is an affine invariant property.*

This time the equation (5) can be used to explain the bijective relation between the bases of the involved functions. We now explain how these indicators can be used in order to find affine relations between two affine equivalent functions. We first investigate the frequency distribution of the Walsh and autocorrelation values of the two functions f_1 and f_2. We then check if both have the same number of bases in all relatively small sets of vectors which have the same absolute value in the autocorrelation of Walsh spectrum. If the functions pass these tests, there is a high probability that they are affine equivalent. In order to find the affine relations, we proceed as follows. If there exists an absolute value in the Walsh spectrum with low frequency and for which there exists a basis in the set of vectors yielding that value in the spectrum, we need to consider a fixed basis (corresponding to the matrix B_1 which rows consist of the function values) and to check for all other bases (corresponding to matrix B_2) and vectors $\overline{b}$ if $f_1(\overline{x}B_2^t(B_1^{-1})^t \oplus \overline{b}) \oplus c$ matches with f_2 where $c \in \{0,1\}$. Similarly, for the autocorrelation, we need to check equivalence between $f_1(\overline{x}B_2^{-1}(B_1) \oplus \overline{b}\overline{x}^t \oplus c$ and f_2, with $c \in \{0,1\}$. These relations follow immediately from the equations (4) and (5).
The efficiency of the algorithm mainly depends on the structure of the Walsh or autocorrelation spectrum and is difficult to compare with the algorithm of Fuller and Millan [12]. For instance, for determining the affine relations between the output functions of the S-box in Rijndael as explained in [12], our algorithm turns out to be very efficient since we can find 13 vectors that yield 32 (in absolute value) in the autocorrelation spectrum and which form only 473 different (ordered) bases. Also in the Walsh spectrum 16 vectors are transformed to the (absolute) value 28 and form 4600 (ordered) bases.

8 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 determined 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. We derive interesting relations between algebraic immunity and cryptographic properties. Unfortunately, the conditions on certain cryptographic properties are necessary but not sufficient. It is still an open problem if such sufficient conditions exist. We also describe two new indicators for distinguishing affine inequivalent functions. The efficiency of these indicators depends on the structure of the Walsh and autocorrelation spectrum. It can be used for finding the affine relations between two affine equivalent functions.

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. Y. Borissov, N. Manev, On Minimal Codewords in the 3rd Order Binary Reed-Muller Codes, *Serdica*, 2004, Vol. 30, number 2-3, pp. 303–324.
3. 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.
4. P. Camion, C. Carlet, P. Charpin, N. Sendrier, On Correlation-Immune Functions, *Crypto 1991*, LNCS 576, Springer-Verlag, pp. 86-100, 1992.
5. C. Carlet, On the Propagation Criterion of Degree l and Order k, *Information and Computation*, Vol. 151 (1-2), pp. 32-56, 1999.
6. 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.
7. 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.
8. N. Courtois, W. Meier, Algebraic Attacks on Stream Ciphers with Linear Feedback, *Eurocrypt 2003*, LNCS 2656, Springer-Verlag, pp. 346-359, 2003.
9. N. G. de Bruijn, Polya's Theory of Counting, Applied Combinatorial Mathematics, Wiley, pp. 144-184, 1964.
10. J. H. Evertse, Linear Structures in Block Ciphers, *Eurocrypt 87*, LNCS 304, Springer-Verlag, pp. 249266.
11. 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.
12. J. Fuller, W. Millan, Linear Redundancy in S-Boxes. *FSW 2003*, LNCS 2887, Springer-Verlag, pp. 74-86, 2003.
13. 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.
14. M. A. Harrison, The Number of Transitivity Sets of Boolean Functions, *Journal of the Society for industrial and applied mathematics*, Vol. 11, pp. 806-828, 1963.
15. M. A. Harrison, On the Classification of Boolean Functions by the General Linear and Affine Group, *Journal of the Society for industrial and applied mathematics*, Vol. 12, pp. 284-299, 1964.
16. X. -D. Hou, $AGL(m, 2)$ Acting on $RM(r, m)/RM(s, m)$, *Journal of Algebra*, Vol. 171, pp. 921-938, 1995.
17. X. -D. Hou, $GL(m, 2)$ Acting on $R(r, m)/R(r-1, m)$, *Discrete Mathematics*, Vol. 149, pp. 99-122, 1996.
18. X. Lai, Additive and Linear Structures of Cryptographic Functions, *FSE 1994*, LNCS 1008, Springer-Verlag, pp. 75–85, 1994.
19. F. J. MacWilliams, N. J. A. Sloane, The Theory of Error- Correcting Codes, North-Holland Publishing Company, 1977.
20. S. Maitra, P. Sarkar, Construction of Nonlinear Boolean Functions with Important Cryptographic Properties, *Eurocrypt 2000*, LNCS 1807, Springer-Verlag, pp. 485-506, 2000.
21. 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.
22. W. Meier, E. Pasalic, C. Carlet, Algebraic Attacks and Decomposition of Boolean Functions, *Eurocrypt 2004*, LNCS 3027, Springer-Verlag, pp. 474-491, 2004.
23. W. Millan, A. Clark, E. Dawson, Heuristic Design of Cryptographically Strong Balanced Boolean Functions, *Eurocrypt 98*, LNCS 1403, Springer-Verlag, pp. 489-499, 1998.
24. 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.
25. 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.
26. B. Preneel, Analysis and design of cryptographic hash functions, PhD. Thesis, Katholieke Universiteit Leuven, 1993.
27. M. Qing-shu, Y. Min, Z. Huan-Quo, L. Yu-Zhen, Analysis of Affinely Equivalent Boolean Functions, *Cryptology ePrint Archive, Report 2005/025*

28. P. Stanica, S.H. Sung, Boolean Functions with Five Controllable Cryptogrpahic Properties, *Designs, Codes and Cryptography*, Vol. 31, pp. 147-157, 2004.
29. T. Siegenthaler, Correlation-Immunity of Non-linear Combining Functions for Cryptographic Applications, *IEEE Transactions on Information Theory*, Vol. 30 (5), pp. 776-780, 1984.
30. Y.V. Taranikov, On Resilient Functions with Maximum Possible Nonlinearity, *Indocrypt 2000*, LNCS 1977, Springer-Verlag, pp. 19-30, 2000.
31. Y. Tarannikov, P. Korolev, A. Botev, Autocorrelation Coefficients and Correlation Immunity of Boolean Functions, *Asiacrypt 2001*, LNCS 2248, Springer-Verlag, pp. 460-479, 2001.
32. Y. Zheng, X. M. Zhang, Cryptographically Resilient Functions, *IEEE Transactions on Information Theory*, Vol. 43 (5), pp. 1740-1747, 1997.
33. 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.
34. Y. Zheng, X. M. Zhang, On Relationship Among Avalanche, Nonlinearity, and Propagation Criteria, *Asiacrypt 2000*, LNCS 1976, Springer-Verlag, pp. 470-483, 2000.

A Classification of Cosets of $RM(1,5)$

The following two tables (Table 2, Table 3) present the 48 affine equivalence classes of the cosets of $RM(1,5)$. For each equivalence class, the number of such cosets, the weight distribution (from which the Walsh spectrum can be derived using Equation (2)) and the autocorrelation spectrum is given. The first table is also called the table of the even cosets, the second table is called the table of the odd cosets, since the weights of all functions in the coset are even, respectively odd.
The functions are represented in abbreviated notation (only the digits of the variables) and the sum should be considered modulo 2. In the second table all representatives have the extra term $x_1x_2x_3x_4x_5$. The frequency distribution of the autocorrelation function is given by a set of tuples, the first element represents the absolute value in the autocorrelation and the second value represents the number of times this value appears.

Table 2. Even cosets of $RM(1,5)$

Representative	# of such cosets	0	2	4	6	8	10	12	14	16	Autocorrelation Spectrum
		32	30	28	26	24	22	20	18	16	
2345	496	0	1	0	0	0	0	0	15	16	(32,2),(24,30)
2345+12	496 × 120	0	0	0	0	2	2	0	14	14	(32,1),(24,7),(8,7),(0,17)
2345+23	496 × 35	0	0	0	1	0	3	0	12	16	(32,2),(24,6),(8,24)
2345+23+45	496 × 28	0	0	0	0	0	6	0	10	16	(32,2),(8,30)
2345+12+34	496 × 840	0	0	0	0	0	2	8	14	8	(32,1),(24,1),(8,13),(0,17)
2345+123	17 360 × 2	0	0	1	0	0	0	3	16	12	(32,1),(24,6),(16,25)
2345+123+12	17 360 × 24	0	0	0	1	0	1	4	14	12	(32,1),(24,3),(16,9),(8,19)
2345+123+24	17 360 × 18	0	0	0	0	2	0	4	16	10	(32,1),(24,2),(16,9),(8,4),(0,16)
2345+123+14	17 360 × 192	0	0	0	0	1	2	4	14	11	(32,1),(24,1),(16,6),(8,13),(0,11)
2345+123+45	17 360 × 32	0	0	0	0	0	4	4	12	12	(32,1),(16,7),(8,6),(0,18)
2345+123+12+34	17 360 × 72	0	0	0	0	0	4	4	12	12	(32,1),(24,1),(16,1),(8,21),(0,8)
2345+123+14+35	17 360 × 576	0	0	0	0	0	2	8	14	8	(32,1),(16,2),(8,14),(0,15)
2345+123+12+45	17 360 × 96	0	0	0	0	1	0	8	16	7	(32,1),(16,3),(8,22),(0,6)
2345+123+24+35	17 360 × 12	0	0	0	0	0	0	12	16	4	(32,1),(16,1),(8,6),(0,24)
2345+123+145	13 888 × 320	0	0	0	0	1	1	6	15	9	(32,1),(16,6),(8,16),(0,9)
2345+123+145+45	13 888 × 32	0	0	0	1	0	0	6	15	10	(32,1),(16,15),(8,16)
2345+123+145+24+45	13 888 × 480	0	0	0	0	0	3	6	13	10	(32,1),(16,3),(8,16),(0,12)
2345+123+145+35+24	13 888 × 192	0	0	0	0	0	1	10	15	6	(32,1),(8,16),(0,15)
123	155 × 8	0	0	1	0	0	0	7	0	24	(32,4),(16,28)
123+45	155 × 512	0	0	0	0	0	4	0	28	0	(32,1),(16,7),(0,24)
123+14	155 × 168	0	0	0	0	2	0	8	0	22	(32,2),(16,12),(0,18)
123+14+25	155 × 336	0	0	0	0	0	0	16	0	16	(32,1),(16,4),(0,27)
123+145	868 × 32	0	0	0	1	0	1	0	30	0	(32,1),(8,16),(16,15)
123+145+23	868 × 320	0	0	0	0	1	0	12	0	19	(32,1),(16,6),(8,16),(0,9)
123+145+24	868 × 480	0	0	0	0	0	4	0	28	0	(32,1),(16,3),(8,16),(0,12)
123+145+23+24+35	686 × 192	0	0	0	0	0	0	16	0	16	(32,1),(8,16),(0,15)
12	155	0	0	0	0	4	0	0	0	28	(32,6),(0,24)
12+34	868	0	0	0	0	0	0	16	0	16	(32,2),(0,30)
-	1	1	0	0	0	0	0	0	0	31	(32,32)

Table 3. Odd cosets of $RM(1,5)$

Representative	# of such cosets	1	3	5	7	9	11	13	15	Autocorrelation Spectrum
		31	29	27	25	23	21	19	17	
12	32×155	0	0	0	1	3	0	0	28	(32,1),(28,7),(4,24)
12+34	32×868	0	0	0	0	0	6	10	16	(32,1),(28,1),(4,30)
123	4 960	0	1	0	0	0	0	7	24	(31,1),(28,3),(20,28)
123+12	$4\,960 \times 7$	0	0	1	0	0	3	4	24	(32,1),(28,3),(20,4),(12,24)
123+14	$4\,960 \times 84$	0	0	0	1	1	2	6	22	(32,1),(28,1),(20,6),(12,6),(4,18)
123+45	$4\,960 \times 64$	0	0	0	0	3	1	7	21	(32,1),(20,7),(4,24)
123+14+25	$4\,960 \times 336$	0	0	0	0	0	6	10	16	(32,1),(20,1),(12,3),(4,27)
123+12+45	$4\,960 \times 448$	0	0	0	0	1	3	13	15	(32,1),(20,1),(12,6),(4,24)
123+12+34	$4\,960 \times 84$	0	0	0	0	2	4	4	22	(32,1),(28,1),(12,12),(4,18)
123+145	$27\,776 \times 10$	0	0	0	1	1	0	12	18	(32,1),(4,16),(12,9),(20,6)
123+145+12	$27\,776 \times 6$	0	0	1	0	0	1	10	20	(32,1),(20,10),(12,21)
123+145+23	$27\,776 \times 80$	0	0	0	1	0	3	9	19	(32,1),(20,3),(12,15),(4,13)
123+145+45+23	$27\,776 \times 16$	0	0	0	1	0	1	15	15	(32,1),(12,21),(4,10)
123+145+24	$27\,776 \times 180$	0	0	0	0	2	2	10	18	(32,1),(20,3),(12,15),(4,13)
123+145+24+23	$27\,776 \times 240$	0	0	0	0	1	5	7	19	(32,1),(20,1),(12,9),(4,21)
123+145+35+24	$27\,776 \times 240$	0	0	0	0	1	3	13	15	(32,1),(12,9),(4,22)
123+145+35+24+23	$27\,776 \times 192$	0	0	0	0	0	6	10	16	(32,1),(12,6),(4,25)
123+145+45+35+24+23	$27\,776 \times 60$	0	0	0	0	0	4	16	12	(32,1),(12,3),(4,28)

B Cryptographic Properties of Cosets of $RM(1,5)$

In this section, we show which classes of the even cosets of $RM(1,5)$ contain functions with certain cryptographic properties and how often they occur in the class.

B.1 The Number of 1-CI, 1-Resilient, 1-PC Functions, 1-PC Functions with Resiliency and cosets with $AI = 3$

Table 4. The Number of functions satisfying 1-CI, 1-Resilient, 1-PC, 1-PC with resiliency properties, and cosets with $AI = 3$.

Representative	$\mathcal{N}_{CI(1)}$	$\mathcal{N}_{R(1)}$	$\mathcal{N}_{PC(1)}$	$\mathcal{N}_{PC(1)\cap Bal}$	$\mathcal{N}_{PC(1)\cap CI(1)}$	$\mathcal{N}_{PC(1)\cap R(1)}$	$\mathcal{N}_{cos,AI=3}$
2345	512	0	0	0	0	0	0
2345+12	28 160	0	163 840	71 680	0	0	0
2345+23	1 790	0	0	0	0	0	0
2345+23+45	14 336	0	0	0	0	0	32
2345+12+34	1 146 880	0	0	0	0	0	16
2345+123	6 400	0	0	0	0	0	0
2345+123+12	76 800	0	0	0	0	0	0
2345+123+24	17 280	0	645 120	201 600	0	0	0
2345+123+14	385 400	0	737 280	253 440	640	0	0
2345+123+45	102 400	0	1 904 640	714 240	0	0	0
2345+123+12+34	230 400	0	0	0	0	0	16
2345+123+14+35	122 880	0	11 550 720	2 887 680	0	0	8
2345+123+12+45	7 680	0	0	0	0	0	0
2345+123+24+35	0	0	3 440 640	430 080	0	0	0
2345+123+145	138 240	0	276 480	77 760	0	0	0
2345+123+145+45	27 648	0	0	0	0	0	0
2345+123+145+24+45	414 720	0	1 966 080	614 400	4 160	0	0
2345+123+145+35+24	6 144	0	2 654 208	497 664	384	0	12
123	16 640	11 520	0	0	0	0	0
123+45	0	0	1 310 720	0	0	0	0
123+14	216 000	133 984	94 720	65 120	10 560	5 280	0
123+14+25	69 120	24 960	1 582 080	791 040	19 200	0	0
123+145	0	0	0	0	0	0	0
123+145+23	1 029 120	537 600	0	0	0	0	0
123+145+24	0	0	0	0	0	0	0
123+145+23+24+35	233 472	96 960	0	0	0	0	32
12	4 840	4 120	2 560	2 240	1 120	840	0
12+34	896	0	46 592	23 296	896	0	0

B.2 The Number of 2-Correlation-Immune Functions

Table 5. 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

B.3 The Number of $PC(1)$ of order 1 and 2 Functions

Table 6. 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

B.4 The Number of $PC(2)$ Functions

Table 7. 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

B.5 The Number of $PC(3)$ and $PC(4)$ Functions

Table 8. The Number of functions satisfying $PC(3)$ and $PC(4)$.

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

C Classification of $RM(3,6)/RM(1,6)$ under the action of $AGL(2,6)$

The six representatives of $RM(3,6)/RM(2,6)$ as distinguished by Hou [17] can be represented by

$$\begin{aligned} f_1 &= 0 \\ f_2 &= 123 \\ f_3 &= 123 + 245 \\ f_4 &= 123 + 456 \\ f_5 &= 123 + 245 + 346 \\ f_6 &= 123 + 145 + 246 + 356 + 456 \end{aligned}$$

The number of cosets, the Walsh spectrum and autocorrelation spectrum of the 34 affine equivalence classes of $RM(3,6)/RM(1,6)$ can be found in Table 9. The numbers of 1-and 2-resilient functions are presented in Table 10.

Table 9. The number of cosets, weight distribution and autocorrelation spectra of affine equivalent classes of $RM(3,6)/RM(1,6)$.

	Representative	Number of Cosets	Walsh transform	Autocorrelation Transform
f_1	0	1	(0,63),(64,1)	(0,63),(64,1)
	12	651	(0,60),(32,4)	(0,48),(64,16)
	14+23	18 228	(0,48),(16,16)	(0,60),(64,16)
	16+25+34	13 888	(8,64)	(0,63),(64,1)
f_2	0	$1\,395 \times 8$	(0,56),(16,7),(48,1)	(32,56),(64,8)
	14	$1\,395 \times 392$	(0,54),(16,8),(32,2)	(0,36),(32,24),(64,4)
	24+15	$1\,395 \times 2\,352$	(0,48),(16,16)	(0,54),(32,8),(64,2)
	16+25+34	$1\,395 \times 1\,344$	(64,8)	(0,63),(64,1)
	45	$1\,395 \times 3\,584$	(0,32),(8,28),(24,2)	(0,48),(32,14),(64,2)
	16+45	$1\,395 \times 25\,088$	(0,24),(8,32),(16,8)	(0,57),(32,6),(64,1)
f_3	0	$54\,684 \times 32$	(0,32),(8,30),(24,1),(40,1)	(16,32),(32,30),(64,2)
	13	$54\,684 \times 320$	(0,51),(16,12),(32,1)	(0,18),(16,32),(32,12),(64,2)
	14	$54\,684 \times 480$	(0,32),(8,28),(24,4)	(0,24),(16,32),(32,6),(64,2)
	16	$54\,684 \times 7\,680$	(0,28),(8,30),(16,4),(24,2)	(0,39),(16,16),(32,8),(64,1)
	26	$54\,684 \times 32$	(0,30),(8,32),(32,2)	(0,32),(32,30),(64,2)
	26+13	$54\,684 \times 320$	(0,48),(16,16)	(0,51),(32,12),(64,1)
	26+14	$54\,684 \times 480$	(0,24),(8,32),(16,8)	(0,57),(32,6),(64,1)
	13+15+26+34	$54\,684 \times 192$	(8,64)	(0,63),(64,1)
	34+13+15	$54\,684 \times 23\,040$	(0,48),(16,16)	(0,30),(16,32),(64,2)
	34+16	$54\,684 \times 192$	(0,24),(8,32),(16,8)	(0,45),(16,16),(64,1)
f_4	0	$357\,120 \times 64$	(4,49),(12,14),(36,1)	(16,49),(32,14),(64,1)
	14	$357\,120 \times 3\,136$	(4,49),(12,12),(28,1),(20,2)	(0,24),(16,33),(32,6),(64,1)
	15+24	$357\,120 \times 64$	(4,46),(20,3),(12,15)	(0,36),(16,25),(32,2),(64,1)
	34+25+16	$357\,120 \times 64$	(4,42),(12,21),(20,1)	(0,42),(16,21),(64,1)
f_5	0	$468\,720 \times 448$	(0,27),(8,32),(16,4),(32,1)	(0,9),(16,48),(32,6),(64,1)
	12+13	$468\,720 \times 18$	(0,28),(8,30),(16,4),(24,2)	(0,27),(16,32),(32,4),(64,1)
	15	$468\,720 \times 14\,336$	(0,26),(8,31),(24,1),(16,6)	(0,30),(16,32),(32,1),(64,1)
	12+13+25	$468\,720 \times 2\,222$	(0,48),(16,16)	(0,27),(16,32),(32,4),(64,1)
	14+25	$468\,720 \times 1\,344$	(0,24),(8,32),(16,8)	(0,45),(16,16),(64,1)
	35+26+25+12	$468\,720 \times 14\,336$	(8,64)	(0,63),(64,1)
	25+15+16	$468\,720 \times 64$	(0,24),(8,32),(16,8)	(0,39),(16,24),(64,1)
f_6	0	$166\,656 \times 3\,584$	(4,45),(12,18),(28,1)	(0,18),(16,45),(64,1)
	12+13	$166\,656 \times 21\,504$	(4,46),(12,15),(20,3)	(0,30),(16,33),(64,1)
	23+15+14	$166\,656 \times 7\,680$	(4,42),(12,21),(20,1)	(0,42),(16,21),(64,1)

C.1 Number of Resilient and PC functions in affine equivalent classes of $RM(3,6)/RM(1,6)$

Table 10. The number of resilient and PC functions in the classes of $RM(3,6)/RM(1,6)$.

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

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.
3-Resilient functions can only belong to the class with representative x_1x_2 and there are in total 1120 3-resilient functions of dimension 6 (see also [4]).

D Classification of $RM(3,7)/RM(1,7)$ under the action of $AGL(2,7)$

Denote $\nu(r,n,f)$ as the number of cosets in the orbit containing $f \oplus RM(r-1,n)$. The values of $\nu(3,7,f_i)$ for the twelve representatives $f_i, 1 \le i \le 12$ of $RM(3,7)/RM(2,7)$ are represented in Table 11:
The orders of the sizes, the Walsh spectrum and autocorrelation spectrum of the 179 affine equivalence classes of $RM(3,7)/RM(1,7)$ can be found in the next table.

Table 11. Representatives of $RM(3,7)/RM(2,7)$ together lenths of orbits

Class	Representative	$\nu(3,7,f)$
f_1	0	1
f_2	123	11 811
f_3	123+245	2 314 956
f_4	123+456	45 354 240
f_5	123+245+346	59 527 440
f_6	123+145+246+356+456	21 165 440
f_7	127+347+567	1 763 776
f_8	123+456+147	2 222 357 760
f_9	123+245+346+147	238 109 760
f_{10}	123+456+147+257	17 778 862 080
f_{11}	123+145+246+356+456+167	444 471 552
f_{12}	123+145+246+356+456+167+247	13 545 799 680

	Coset of $RM(3,7)$	Number of Cosets ($\times\nu(7,3,f)$)	Walsh transform	Autocorrelation Transform
f_1	0	1	(0,127),(128,1)	(128,128)
	12	2 667	(0,124),(64,4)	(0,96),(128,32)
	14+23	330 708	(0,112),(32,16)	(0,120),(128,32)
	16+25+34	1 763 776	(0,64),(16,64)	(0,126),(128,2)
f_2	0	8	(0,120),(32,7),(96,1)	(64,112),(128,16)
	14	840	(0,118),(32,8),(64,2)	(0,72),(64,48),(128,8)
	24+15	11760	(0,112),(32,16)	(0,108),(64,16),(128,4)
	16+24+34	20 160	(0,64),(16,64)	(0,126),(128,2)
	45	17920	(0,96),(16,28),(48,2)	(0,96),(64,28),(128,4)
	16+45	3766320	(0,88),(16,32),(32,8)	(0,114),(64,12),(128,2)
	45+17+26	752 640	(0,64),(16,64)	(0,123),(64,4),(128,1)
	47+56	917 504	(8,112),(24,16)	(0,120),(64,7),(128,1)
f_3	0	32	(0,96),(16,30),(48,1),(80,1)	(32,64),(64,60),(128,4)
	13	320	(0,115),(32,12),(64,1)	(0,36),(32,64),(64,24),(128,4)
	14	480	(0,92),(16,28),(48,4)	(0,48),(32,64),(64,12),(128,4)
	16	23040	(0,92),(16,30),(32,4),(48,2)	(0,78),(32,32),(64,16),(128,2)
	26	96	(0,94),(16,32),(64,2)	(0,66),(64,60),(128,4)
	26+13	960	(0,112),(32,16)	(0,102),(64,24),(128,2)
	26+14	1440	(0,88),(16,32),(32,8)	(0,114),(64,12),(128,2)
	26+17	23 040	(0,88),(16,32),(32,8)	(0,60),(32,64),(128,1)
	34+13+15	192	(0,112),(32,16)	(0,60),(32,64),(128,4)
	34+16	69120	(0,88),(16,32),(32,8)	(0,90),(32,32),(128,2)
	13+15+26+34	576	(0,64),(16,64)	(0,126),(128,2)
	34+26+17	69 120	(0,64),(16,64)	(0,123),(64,4),(128,1)
	36+17	983 040	(8,112),(24,16)	(0,108),(32,16),(64,3),(128,1)
	46+17	491 520	(0,76),(16,48),(32,4)	(0,105),(32,16),(64,6),(128,1)
	46+35+17	184 320	(0,64),(16,64)	(0,111),(32,16),(128,1)
	67	184 320	(8,120),(24,4),(40,4)	(0,96),(32,16),(64,15),(128,1)
	67+13	327 680	(0,64),(16,64)	(0,111),(32,16),(128,1)
	67+14	491 520	(0,76),(16,48),(32,4)	(0,105),(32,16),(64,6),(128,1)
	6+34+14+137	196 608	(8,120),(24,4),(40,4)	(0,96),(32,16),(64,15),(128,1)
f_4	0	64	(0,64),(8,49),(24,14),(72,1)	(32,98),(64,28),(128,2)
	14	3, 136	(0,64),(8,49),(24,12),(40,2),(56,1)	(0,48),(32,66),(64,12),(128,2)
	17	7 168	(0,48),(8,56),(16,14),(24,8),(48,2)	(0,72),(32,42),(64,13),(128,1)
	15+24	18816	(0,64),(8,46),(24,15),(40,3)	(0,72),(32,50),(64,4),(128,2)
	24+17	150 528	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,96),(32,26),(64,5),(128,1)
	34+25+16	10752	(0,64),(8,42),(24,21),(40,1)	(0,84),(32,42),(128,2)
	34+25+17	301 056	(0,32),(8,56),(16,32),(24,8)	(0,108),(32,18),(64,1),(128,1)
	47+17	100 352	(0,38),(8,60),(16,24),(24,2),(32,2),(40,2)	(0,87),(32,34),(64,6),(128,1)
	47+25+17	131 360	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,99),(32,26),(64,2),(128,1)
	47+35+26+16	602 112	(0,32),(8,56),(16,32),(24,8)	(0,105),(32,22),(128,1)

f_5	0	448	(0,91),(16,32),(32,4),(64,1)	(0,18),(32,96),(64,12),(128,2)
	12+13	1792	(0,92),(16,30),(32,4),(48,2)	(0,54),(32,64),(64,8),(128,2)
	15	14336	(0,90),(16,31),(32,6),(48,1)	(0,60),(32,64),(64,2),(128,2)
	17	114 688	(8,116),(24,10),(40,2)	(0,84),(32,40),(64,3),(128,1)
	12+13+25	448	(0,112),(32,16)	(0,54),(32,64),(64,8),(128,2)
	14+25	1344	(0,88),(16,32),(32,8)	(0,90),(32,32),(64,4),(128,2)
	25+15+16	14336	(0,88),(16,32),(32,8)	(0,78),(32,48),(128,2)
	25+17	344 064	(0,76),(16,48),(32,4)	(0,93),(32,32),(64,2),(128,1)
	26+17	344 064	(8,112),(24,16)	(0,102),(32,24),(64,1),(128,1)
	27	3 584	(0,80),(16,46),(48,2)	(0,69),(32,48),(64,10),(128,1)
	27+13	10 752	(0,88),(16,32),(32,8)	(0,87),(32,32),(64,8),(128,1)
	27+14	10 752	(0,76),(16,48),(32,4)	(0,105),(32,16),(64,6),(128,1)
	27+15	114 688	(8,112),(24,16)	(0,102),(32,24),(64,1),(128,1)
	27+16	43 008	(0,76),(16,48),(32,4)	(0,93),(32,32),(64,2),(128,1)
	35+26+25+12+13+14	64	(0,64),(16,64)	(0,126),(128,2)
	35+26+25+17	114 688	(0,64),(16,64)	(0,111),(32,16),(128,1)
	35+27+13+14	3 584	(0,64),(16,64)	(0,123),(64,4),(128,1)
	35+27+16	43 008	(0,64),(16,64)	(0,111),(32,16),(128,1)
	56+17	458 752	(8,112),(24,16)	(0,99),(32,28),(128,1)
	56+25+17	458 752	(0,70),(16,56),(32,2)	(0,99),(32,28),(128,1)
f_6	0	3584	(0,64),(8,45),(24,18),(56,1)	(0,36),(32,90),(128,2)
	12+13	21504	(0,64),(8,46),(24,15),(40,3)	(0,60),(32,66),(128,2)
	17	129 024	(0,32),(8,60),(16,32),(24,2),(40,2)	(0,81),(32,46),(128,1)
	23+15+14	7680	(0,64),(8,42),(24,21),(40,1)	(0,84),(32,42),(128,2)
	23+16	1 290 240	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,93),(32,34),(128,1)
	25+17	645 120	(0,32),(8,56),(16,32),(24,8)	(0,105),(32,22),(128,1)
f_7	0	128	(8,126), (56,1), (72,1)	(16,64), (64,63), (128,1)
	12	43 008	(0,90), (16,31), (32,6), (48,1)	(0,45), (16,64), (64,18), (128,1)
	13	40 320	(8,120), (24,4), (40,4)	(0,48), (16,64), (64,15), (128,1)
	23+14	645 120	(0,76),(16,48), (32,4)	(0,57), (16,64), (64,6), (128,1)
	23+14+12	516 096	(8,112), (24,16)	(0,60), (16,64), (64,3), (128,1)
	23+15	483 840	(8,112), (24,16)	(0,60), (16,64), (64,3), (128,1)
	34+25+23+16+14	368 640	(0,64), (16,64)	(0,63), (16,64), (128,1)
f_8	0	128	(0,37),(8,64),(16,24),(32,2),(64,1)	(16,32),(32,82),(64,13),(128,1)
	15	768	(0,38),(8,64),(16,22),(32,2),(48,2)	(0,36),(16,32),(32,50),(64,9),(128,1)
	17	1 024	(0,48),(8,55),(16,16),(24,7),(40,1),(56,1)	(0,27),(16,32),(32,58),(64,10),(128,1)
	15+23	3 072	(0,48),(8,52),(16,16),(24,10),(40,2)	(0,63),(16,32),(32,26),(64,6),(128,1)
	23+17	2 048	(0,60),(8,50),(24,13),(32,4),(40,1)	(0,54),(16,32),(32,34),(64,7),(128,1)
	15+24	1 152	(0,34),(8,64),(16,24),(32,6)	(0,72),(16,32),(32,18),(64,5),(128,1)
	25	4608	(0,36),(8,64),(16,23),(32,4),(48,1)	(0,48),(16,32),(32,42),(64,5),(128,1)
	25+16	9 216	(0,34),(8,64),(16,24),(32,6)	(0,66),(16,32),(32,26),(64,3),(128,1)
	25+17	18 432	(0,48),(8,52),(16,16),(24,10),(40,2)	(0,57),(16,32),(32,34),(64,4),(128,1)
	25+23+16	18 432	(0,48),(8,48),(16,16),(24,16)	(0,75),(16,32),(32,18),(64,2),(128,1)
	25+23+17	18 423	(0,48),(8,50),(16,16),(24,13),(40,1)	(0,66),(16,32),(32,26),(64,3),(128,1)
	27	24 576	(0,38),(8,60),(16,24),(24,2),(32,2),(40,2)	(0,57),(16,32),(32,34),(64,4),(128,1)
	27+15	73 728	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,75),(16,32),(32,18),(64,2),(128,1)
	27+23	12 288	(0,46),(8,56),(16,15),(24,8),(32,2),(48,1)	(0,48),(16,32),(32,42),(64,5),(128,1)
	27+15+23	36 684	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,66),(16,32),(32,26),(64,3),(128,1)
	34+25+16	4608	(0,22),(8,64),(16,40),(32,2)	(0,84),(16,32),(32,10),(64,1),(128,1)
	34+27+23	12 288	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,66),(16,32),(32,26),(64,3),(128,1)
	34+27+23+15	36 864	(0,32),(8,56),(16,32),(24,8)	(0,84),(16,32),(32,10),(64,1),(128,1)
	35+26	12 288	(0,48),(8,48),(16,16),(24,16)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+26+17	36 864	(0,28),(8,64),(16,32),(32,4)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+26+23+17	12 288	(0,28),(8,64),(16,32),(32,4)	(0,72),(16,32),(32,22),(64,1),(128,1)

	27+35	147 456	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+27+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,81),(16,32),(32,14),(128,1)
	35+27+34	147 456	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,72),(16,32),(32,22),(64,1),(128,1)
	35+27+23+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,81),(16,32),(32,14),(128,1)
	57+27	147 456	(0,38),(8,58),(16,24),(24,5),(32,2),(40,1)	(0,63),(16,32),(32,30),(64,2),(128,1)
	57+27+16	294 912	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,72),(16,32),(32,22),(64,1),(128,1)
	57+34+27+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,81),(16,32),(32,14),(128,1)
	57+36+27	589 824	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,75),(16,32),(32,20),(128,1)
f_9	0	1 024	(8,119),(24,7),(40,1),(56,1)	(16,64),(32,56),(64,7),(128,1)
	15	21 504	(8,116),(24,10),(40,2)	(0,36),(16,64),(32,24),(64,3),(128,1)
	17	14 336	(0,78),(16,47),(32,2),(48,1)	(0,27),(16,64),(32,32),(64,4),(128,1)
	23+17	14 336	(0,88),(16,32),(32,8)	(0,27),(16,64),(32,32),(64,4),(128,1)
	25+16	86 016	(0,76),(16,48),(32,4)	(0,45),(16,64),(32,16),(64,2),(128,1)
	26+15	43 008	(8,112),(24,16)	(0,54),(16,64),(32,8),(64,1),(128,1)
	27+17+15	57 344	(8,112),(24,16)	(0,54),(16,64),(32,8),(64,1),(128,1)
	35+27+16+15	24 576	(0,64),(16,64)	(0,63),(16,64),(128,1)
	56	229 376	(0,76),(16,48),(32,4)	(0,42),(16,64),(32,20),(64,1),(128,1)
	56+17	229 376	(8,114),(24,13),(40,1)	(0,42),(16,64),(32,20),(64,1),(128,1)
	56+16+15	688 128	(0,76),(16,48),(32,4)	(0,42),(16,64),(32,20),(64,1),(128,1)
	56+27+15	688 128	(8,112),(24,16)	(0,51),(16,64),(32,12),(128,1)
f_{10}	0	768	(0,40),(8,57),(16,24),(24,6),(56,1)	(0,12),(16,48),(32,64),(64,3),(128,1)
	13	9216	(0,38),(8,60),(16,23),(24,4),(32,2),(48,1)	(0,33),(16,48),(32,44),(64,2),(128,1)
	15	1 536	(0,40),(8,58),(16,24),(24,3),(40,3)	(0,36),(16,48),(32,40),(64,3),(128,1)
	16	9 216	(0,40),(8,56),(16,24),(24,6),(40,2)	(0,42),(16,48),(32,36),(64,1),(128,1)
	23+14	18 432	(0,46),(8,54),(16,16),(24,9),(32,2),(40,1)	(0,45),(16,48),(32,32),(64,2),(128,1)
	15+23	9 216	(0,36),(8,60),(16,24),(24,4),(32,4)	(0,57),(16,48),(32,20),(64,2),(128,1)
	23+16	36 864	(0,36),(8,60),(16,24),(24,4),(32,4)	(0,54),(16,48),(32,24),(64,1),(128,1)
	23+16+13	18 432	(0,46),(8,52),(16,16),(24,12),(32,2)	(0,54),(16,48),(32,24),(64,1),(128,1)
	24+15	768	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,60),(16,48),(32,16),(64,3),(128,1)
	24+16	9 216	(0,40),(8,52),(16,24),(24,12)	(0,66),(16,48),(32,12),(64,1),(128,1)
	26+16	9 216	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,54),(16,48),(32,24),(64,1),(128,1)
	27+17+16	18 432	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,54),(16,48),(32,24),(64,1),(128,1)
	27+23+17+13	512	(0,48),(8,52),(16,15),(24,12),(48,1)	(0,36),(16,48),(32,40),(64,3),(128,1)
	27+23+17+13	512	(0,58),(8,52),(24,12),(32,6)	(0,36),(16,48),(32,40),(64,3),(128,1)
	27+23+17+16+13	9 216	(0,46),(8,52),(16,16),(24,12),(32,2)	(0,54),(16,48),(32,24),(64,1),(128,1)
	34+16	6 144	(0,30),(8,60),(16,32),(24,4),(32,2)	(0,63),(16,48),(32,16),(128,1)
	34+16+13	36 864	(0,40),(8,52),(16,24),(24,12)	(0,63),(16,48),(32,16),(128,1)
	34+17+16+13	18 432	(0,30),(8,60),(16,32),(24,4),(32,2)	(0,63),(16,48),(32,16),(128,1)
	34+23+17+16+13	36 864	(0,30),(8,60),(16,32),(24,4),(32,2)	(0,63),(16,48),(32,16),(128,1)
	34+26+23	3 072	(0,36),(8,60),(16,24),(24,4),(32,4)	(0,51),(16,48),(32,28),(128,1)
	34+26+23+14	3 072	(0,24),(8,60),(16,40),(24,4)	(0,75),(16,48),(32,4),(128,1)
	34+26+23+17+13	6 144	(0,40),(8,52),(16,24),(24,12)	(0,63),(16,48),(32,16),(128,1)
	36	98 304	(0,33),(8,60),(16,28),(24,4),(32,3)	(0,57),(16,48),(32,22),(128,1)
	36+13	32 768	(0,40),(8,54),(16,24),(24,9),(40,1)	(0,51),(16,48),(32,28),(128,1)
	36+15+13	98 304	(0,40),(8,52),(16,24),(24,12)	(0,63),(16,48),(32,16),(128,1)
	36+24+15	32 768	(0,27),(8,60),(16,36),(24,4),(32,1)	(0,69),(16,48),(32,10),(128,1)
	37	73 728	(0,38),(8,58),(16,24),(24,5),(32,2),(40,1)	(0,48),(16,48),(32,30),(64,1),(128,1)
	37+14	73 728	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,60),(16,48),(32,18),(64,1),(128,1)
	37+16	294 912	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,63),(16,48),(32,16),(128,1)
	37+25+13	6 144	(0,40),(8,56),(16,23),(24,8),(48,1)	(0,36),(16,48),(32,42),(64,1),(128,1)
	37+25+13+14	18 432	(0,44),(8,56),(16,16),(24,8),(32,4)	(0,48),(16,48),(32,30),(64,1),(128,1)
	37+23+15+13	18 432	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,60),(16,48),(32,18),(64,1),(128,1)
	37+23+16	147 456	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,57),(16,48),(32,22),(128,1)
	37+25+24+15+14+13	6 144	(0,32),(8,56),(16,32),(24,8)	(0,72),(16,48),(32,6),(64,1),(128,1)
	37+24+23+16	147 456	(0,32),(8,56),(16,32),(24,8)	(0,69),(16,48),(32,10),(128,1)
	37+36	98304	(0,35),(8,58),(16,28),(24,5),(32,1),(40,1)	(0,51),(16,48),(32,28),(128,1)
	37+36+13	294 912	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,57),(16,48),(32,22),(128,1)
	37+36+15	294 912	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,63),(16,48),(32,16),(128,1)
	37+36+24+15+13	98 304	(0,32),(8,56),(16,32),(24,8)	(0,69),(16,48),(32,10),(128,1)

f_{11}	0	6 144	(0,30),(8,64),(16,31),(32,2),(48,1)	(16,96),(32,30),(64,1),(128,1)
	23	5 120	(0,24),(8,64),(16,39),(48,1)	(0,12),(16,96),(32,18),(64,1),(128,1)
	23+12	15 360	(0,34),(8,64),(16,24),(32,6)	(0,12),(16,96),(32,18),(64,1),(128,1)
	23+17	61 440	(0,48),(8,50),(16,16),(24,13),(40,1)	(0,12),(16,96),(32,18),(64,1),(128,1)
	25	30 720	(0,28),(8,64),(16,32),(32,4)	(0,24),(16,96),(32,6),(64,1),(128,1)
	27	737 280	(0,38),(8,56),(16,24),(24,8),(32,2)	(0,21),(16,96),(32,10),(128,1)
	27+14	245 760	(0,32),(8,58),(16,32),(24,5),(40,1)	(0,21),(16,96),(32,10),(128,1)
	34+25+17+16+14	10 240	(0,48),(8,48),(16,16),(24,16)	(0,24),(16,96),(32,6),(64,1),(128,1)
	27+34	983 040	(0,35),(8,56),(16,28),(24,8),(32,1)	(0,27),(16,96),(32,4),(128,1)
	27+23+24	2 048	(0,60),(8,48),(24,16),(32,4)	(16,96),(32,30),(64,1),(128,1)
f_{12}	0	129 024	(0,39),(8,56),(16,24),(24,7),(32,1),(40,1)	(0,36),(16,64),(32,27),(128,1)
	12	16 128	(0,36),(8,58),(16,27),(24,6),(48,1)	(0,24),(16,64),(32,39),(128,1)
	16+15+13	32 256	(0,34),(8,60),(16,28),(24,3),(32,2),(40,1)	(0,36),(16,64),(32,27),(128,1)
	17+15+13+12	128	(0,28),(8,63),(16,36),(56,1)	(16,64),(32,63),(128,1)
	23	110 592	(0,36),(8,56),(16,28),(24,7),(40,1)	(0,42),(16,64),(32,21),(128,1)
	23+12	258 048	(0,37),(8,58),(16,24),(24,6),(32,3)	(0,42),(16,64),(32,21),(128,1)
	23+12+13	129 024	(0,39),(8,54),(16,24),(24,10),(32,1)	(0,48),(16,64),(32,15),(128,1)
	23+15	387 072	(0,34),(8,58),(16,28),(24,6),(32,2)	(0,48),(16,64),(32,15),(128,1)
	23+15+13	387 072	(0,39),(8,54),(16,24),(24,10),(32,1)	(0,48),(16,64),(32,15),(128,1)
	23+15+13+12	43 008	(0,45),(8,54),(16,16),(24,10),(32,3)	(0,36),(16,64),(32,27),(128,1)
	25+16+13	48 384	(0,34),(8,58),(16,28),(24,6),(32,2)	(0,48),(16,64),(32,15),(128,1)
	25+17+15+12+13	8 064	(0,28),(8,60),(16,36),(24,3),(40,1)	(0,48),(16,64),(32,15),(128,1)
	34+25+12	258 048	(0,36),(8,54),(16,28),(24,10)	(0,54),(16,64),(32,9),(128,1)
	34+25+16+12	258 048	(0,31),(8,58),(16,32),(24,6),(32,1)	(0,54),(16,64),(32,9),(128,1)
	34+26+17+15+14+13+12	32 256	(0,28),(8,58),(16,36),(24,6)	(0,60),(16,64),(32,3),(128,1)