Spectral Analysis of High Order Correlation Immune Functions

Yuriy Tarannikov
and Denis Kirienko

Mech. & Math. Department
Moscow State University
119899 Moscow, Russia
emails: yutaran@mech.math.msu.su, taran@vertex.inria.msu.ru, kirienko@mccme.ru

Abstract

We use the recent results on the spectral structure of correlation immune and resilient Boolean functions for the investigations of high order correlation immune functions. At first, we give simple proofs of some theorems where only long proofs were known. Next, we introduce the matrix of nonzero Walsh coefficients and establish important properties of this matrix. We use these properties to prove the nonexistence of some high order correlation immune functions. Finally, we establish the order of magnitude for the number of $(n-4)$th order correlation immune / resilient functions of n variables.

Keywords: *Boolean function, correlation immunity, resiliency, Walsh Transform.*

We consider F_2^n, the vector space of n-tuples of elements from F_2. An n-variable Boolean function is a map from F_2^n into F_2. The *weight* of a vector x is the number of ones in x and is denoted by $|x|$. The *weight* $wt(f)$ of a function f on F_2^n is the number of vectors x on F_2^n such that $f(x)=1$. A function f is said to be *balanced* if $wt(f)=wt(f\oplus 1)=2^{n-1}$. A *subfunction* of the Boolean function f is a function f' obtained by substituting some constants for some variables in f.

The following definitions and formulae are classical ones (see [5]). Let $x=(x_1,\ldots,x_n)$ and $u=(u_1,\ldots,u_n)$ be n-tuples over F_2. The *scalar product* of x and u is defined as

$$<x,u>=\sum_{i=1}^{n} x_i u_i.$$

The *Walsh Transform* of a Boolean function f is an integer-valued function over F_2^n that can be defined as

$$\widehat{\chi_f}(u)=\sum_{x\in F_2^n}(-1)^{f(x)+<u,x>}.$$

For every $u\in F_2^n$ the value $\widehat{\chi_f}(u)$ is called the *Walsh coefficient.* Frequently Walsh coefficients are called spectral coefficients.

Walsh coefficients satisfy the next formulae:

Inversion formula

$$(-1)^{f(x)}=2^{-n}\sum_{u\in F_2^n}\widehat{\chi_f}(u)(-1)^{<u,x>}.$$

Parseval's equation

$$\sum_{u\in F_2^n}\widehat{\chi_f}^2(u)=2^{2n}.$$

In [7] the next important theorem was proved. Note that in [7] the proof of this theorem takes up three pages. Here we give a simple proof of this theorem.

Theorem 1 (Sarkar, [7])
Let f be a Boolean function on F_2^n. Then for every $w \in F_2^n$

$$\sum_{\substack{u \in F_2^n \\ u \preceq w}} \widehat{\chi_f}(u) = 2^n - 2^{|w|+1} wt(f_w). \tag{1}$$

where f_w is the function obtained from f by substituting $0 \to x_i$ for all i such that $w_i = 1$.

Proof.

$$\begin{aligned}
\sum_{\substack{u \in F_2^n \\ u \preceq w}} \widehat{\chi_f}(u) &= \sum_{\substack{u \in F_2^n \\ u \preceq w}} \sum_{x \in F_2^n} (-1)^{f(x) + < x,u >} = \sum_{x \in F_2^n} (-1)^{f(x)} \sum_{\substack{u \in F_2^n \\ u \preceq w}} (-1)^{< x,u >} = \\
&\sum_{\substack{x \in F_2^n \\ < x,w > = 0}} (-1)^{f(x)} \sum_{\substack{u \in F_2^n \\ u \preceq w}} (-1)^{< x,u >} + \sum_{\substack{x \in F_2^n \\ < x,w > > 0}} (-1)^{f(x)} \sum_{\substack{u \in F_2^n \\ u \preceq w}} (-1)^{< x,u >} = \\
&2^{|w|} \sum_{\substack{x \in F_2^n \\ < x,w > = 0}} (-1)^{f(x)} + \sum_{\substack{x \in F_2^n \\ < x,w > > 0}} (-1)^{f(x)} \cdot 0 = \\
&2^{|w|} \widehat{\chi_{f_w}}(0) = 2^{|w|}(2^{n-|w|} - 2wt(f_w)) = 2^n - 2^{|w|+1} wt(f_w).
\end{aligned}$$

□

It is well known that a function f on F_2^n can be uniquely represented by a polynomial on F_2 whose degree in each variable is at most 1. Namely,

$$f(x_1, \ldots, x_n) = \bigoplus_{(a_1, \ldots, a_n) \in F_2^n} g(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n}$$

where g is also a function on F_2^n. This polynomial representation of f is called the *algebraic normal form* (briefly, ANF) of the function and each $x_1^{a_1} \ldots x_n^{a_n}$ is called a *term* in ANF of f. The *algebraic degree* of f, denoted by $\deg(f)$, is defined as the number of variables in the longest term of f. The *algebraic degree of variable* x_i in f, denoted by $\deg(f, x_i)$, is the number of variables in the longest term of f that contains x_i. If $\deg(f, x_i) = 1$, we say that f depends on x_i *linearly.* If $\deg(f, x_i) \neq 1$, we say that f depends on x_i *nonlinearly.* A term of length 1 is called a *linear* term. If $\deg(f) \leq 1$ then f is called an *affine* function. If f is an affine function and $f(0) = 0$ then f is called a *linear* function.

The *Hamming distance* $d(x_1, x_2)$ between two vectors x_1 and x_2 is the number of components where vectors x_1 and x_2 differ. For two Boolean functions f_1 and f_2 on F_2^n, we define the distance between f_1 and f_2 by $d(f_1, f_2) = \#\{x \in F_2^n | f_1(x) \neq f_2(x)\}$. It is easy to see that $d(f_1, f_2) = wt(f_1 \oplus f_2)$. The minimum distance between f and the set of all affine functions is called the *nonlinearity* of f and denoted by $nl(f)$.

It is easy to see that $\widehat{\chi_f}(0) = 0$ iff f is balanced.

A Boolean function f on F_2^n is said to be *correlation immune of order* m, with $1 \leq m \leq n$, if the output of f and any m input variables are statistically independent. This concept was introduced by Siegenthaler [8]. In equivalent non-probabilistic formulation the Boolean function f is called correlation immune of order m if $wt(f') = wt(f)/2^m$ for any its subfunction f' of $n - m$ variables. A balanced mth order correlation immune function is called an *m-resilient* function. In other words the Boolean function f is called m-resilient if $wt(f') = 2^{n-m-1}$ for any its subfunction f' of $n - m$ variables. In [4] a characterization of correlation immune functions by means of Walsh coefficients is given: A function f on F_2^n is an mth order correlation immune function iff $\widehat{\chi_f}(u) = 0$ for all $u \in F_2^n$ with $1 \leq |u| \leq m$. In [6] it is proved that

Theorem 2 [6] *If f is an mth order correlation immune function on F_2^n, $m \le n-1$, then* $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+1}}$. *Moreover, if f is m-resilient, $m \le n-2$, then* $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$.

Theorem 2 follows some upper bounds on the nonlinearity of correlation immune of order m Boolean functions on F_2^n. The similar upper bound were obtained independently in [12] and [13].

In the next lemma we give a spectral characterization of the linear dependence of the function f on the variable x_i.

Lemma 1 *The function f depends on the variable x_i linearly iff $\widehat{\chi_f}(u) = 0$ for all u such that $u_i = 0$.*

Proof. Suppose that the function f on F_2^n depends on the variable x_i linearly. Let u be a vector on F_2^n such that $u_i = 0$. Consider arbitrary two vectors x' and x'' such that $d(x', x'') = 1$, $x'_i \ne x''_i$. Then $f(x') \ne f(x'')$ and $(-1)^{f(x')+<u,x'>} + (-1)^{f(x'')+<u,x''>} = 0$. We can combine all vectors on F_2^n into pairs so that any pair (x', x'') contains vectors x' and x'' that differ in ith component and coincide in all other components. Therefore,

$$\widehat{\chi_f}(u) = \sum_{x \in F_2^n} (-1)^{f(x)+<u,x>} = 0.$$

On the other hand, suppose that $\widehat{\chi_f}(u) = 0$ for all u such that $u_i = 0$. Consider arbitrary two vectors x' and x'' such that $d(x', x'') = 1$, $x'_i \ne x''_i$. Then by inversion formula

$$(-1)^{f(x')} + (-1)^{f(x'')} = 2^{-n} \sum_{\substack{u \in F_2^n \\ u_i = 1}} \widehat{\chi_f}(u) \left((-1)^{<u,x'>} + (-1)^{<u,x''>} \right) = 0.$$

Therefore $f(x') \ne f(x'')$. It follows that f depends on x_i linearly. □

In [9] (the results of this work are given in [11]) it is proved that

Theorem 3 ([9, 11]) *For each positive integer k there exists a minimal nonnegative integer $p'(k)$ that any $(n-k)$th order correlation immune nonconstant function on F_2^n depends nonlinearly on at most $p'(k)$ variables.*

If the function f depends linearly on some variable then, obviously, f is balanced. Therefore Theorem 3 follows that

Theorem 4 ([9, 11]) *For each positive integer k there exists a minimal nonnegative integer $p(k)$ that any $(n-k)$-resilient function on F_2^n depends nonlinearly on at most $p(k)$ variables.*

Obviously, $p'(k) \ge p(k)$. Constructions in [9] and [12] shows that $p(k) \ge 3 \cdot 2^{k-2} - 2$ [11].

The proof of Theorem 3 in [9] is very long and does not give effective upper bounds on the values $p'(k)$ and $p(k)$. In the following theorem we give a simple proof of Theorem 3 and obtain an effective upper bound on $p(k)$.

Below we denote by $M = M(f)$ the $(0,1)$ matrix with n columns that obtained by writing in rows all vectors u such that $\widehat{\chi_f}(u) \ne 0$.

Theorem 5 $p(k) \le (k-1)4^{k-2}$ *for $k \ge 2$.*

Proof. Let f be $(m = n-k)$-resilient function on F_2^n. By Theorem 2 all Walsh coefficients of f are divisible by 2^{m+2}. By Parseval's equation we have that the number of nonzero Walsh coefficients is at most $2^{2n-2m-4} = 4^{k-2}$. For any vector u such that $\widehat{\chi_f}(u) \neq 0$ we have $|u| \geq m+1$, thus, u contains at most $k-1$ zero components. We form the $(0,1)$ matrix M with n columns writing in rows all vectors u such that $\widehat{\chi_f}(u) \neq 0$. The matrix M contains at most 4^{k-2} rows, any row of M contains at most $k-1$ zeroes, thus the matrix M has at most $(k-1)4^{k-2}$ columns with zeroes, all remained columns are all-ones. But if the ith column of M is all-ones then $\widehat{\chi_f}(u) = 0$ for all u such that $u_i = 0$. Therefore by Lemma 1 the function f depends on the variable x_i linearly. Thus, f depends nonlinearly on at most $(k-1)4^{k-2}$ variables and $p(k) \leq (k-1)4^{k-2}$. □

Concerning unbalanced nonconstant $(n-k)$th order correlation immune functions on F_2^n we can point out that by means of Bierbrauer–Friedman bound for orthogonal arrays [1, 3] in [9] it is proved that there do not exist such functions for $n \geq (k-1)2^{k-1} + k$. Therefore taking into account Theorem 5 we have that $p'(k) \leq (k-1)4^{k-2}$ for $k \geq 2$. But it is possible to apply spectral analysis for the study of unbalanced functions too.

Lemma 2 *Let f be a Boolean function on F_2^n. Let $M = M(f)$ be the matrix of nonzero Walsh coefficients of f introduced above. If M contains a column with exactly one symbol 0 then f has only one nonzero Walsh coefficient and f is an affine function.*

Proof. Suppose that the ith column of M contains exactly one symbol 0. Consider the vector w on F_2^n that contains zero in ith component and ones in all remained components. By construction $|w| = n-1$. By Theorem 1 the equation (1) holds. By hypothesis of lemma the left side of (1) has exactly one nonzero term. The right side of (1) is divisible by 2^n. Therefore there exists a nonzero Walsh coefficient that is divisible by 2^n. Then by Parseval's equation this coefficient is the only nonzero Walsh coefficient of f. It is clear that f is an affine function. □

The Lemma 2 allows to use for unbalanced $(n-k)$th order correlation immune functions on F_2^n the same technique as in the Theorem 5. Indeed, in this case the matrix M contains one all-zeroes row but each column of M must contain at least one symbol 0 more.

The next lemma is a sequence of results from [13].

Lemma 3 [13] *Let f be an mth order correlation immune function on F_2^n. If there exist $u \in F_2^n$ such that $\widehat{\chi_f}(u) \equiv 2^{m+1} \pmod{2^{m+2}}$ then $m < 0.6n - 0.4$.*

Corollary 1 *If for $n \geq 2.5k - 1$ there exists unbalanced nonconstant $(m = n-k)$th order correlation immune functions f on F_2^n then $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$ for each $u \in F_2^n$.*

Let f be an mth order correlation immune nonaffine function on F_2^n such that $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$ for each $u \in F_2^n$. The fact that f is nonaffine follows that $n - m \geq 2$. Decompose the matrix $M = M(f)$ into the matrices $M_1, M_2, \ldots$ where the matrix M_i contains all rows of M that correspond to vectors u such that $\widehat{\chi_f}(u) \equiv 2^{m+1+i} \pmod{2^{m+2+i}}$. Let r_i be the number of rows in M_i. Parseval's equation follows that $r_1 + 4r_2 + 16r_3 + \ldots \leq 4^{n-m-2}$.

Theorem 6 *In the matrix M_1 inside of any h columns, $h \leq n-m-2$, every possible h-tuple occurs in even number of rows.*

Proof. Take an arbitrary set S of h columns in the matrix M_1, $0 \leq h \leq n-m-2$. Let w be a vector on F_2^n such that $w_i = 0$ if ith column belongs to S and $w_i = 1$ in opposite case. It is clear that $|w| = n - h \geq m+2$. By Theorem 1 the equality (1) holds. The right side of (1) is divisible by 2^{m+3}. By assumption all terms in the left side of (1) are divisible by 2^{m+2}. Therefore the number of terms in the left side of (1) that equivalent to 2^{m+2} by modulo 2^{m+3} is even. Thus, in chosen h columns all-zeroes h-tuple occurs in even number of rows. Notice that the possibility $h = 0$ demonstrates that M_1 contains even number of rows. It follows easily that in M_1 inside of any h columns, $h \leq n - m - 2$, every h-tuple occurs in even number of rows. $\square$

The next theorem is a generalization of Theorem 6.

Theorem 7 *In the matrix M_i inside of any h columns, $0 < h \leq n - m - i - 1$, that are all-ones in the matrices $M_1, M_2, \ldots, M_{i-1}$, all-zeroes h-tuple occurs in even number of rows.*

Proof. The proof is analogous to the proof of Theorem 6. Take an arbitrary set S of h columns in the matrix M_i, $0 < h \leq n - m - i - 1$, such that each of these columns are all-ones in the matrices $M_1, M_2, \ldots, M_{i-1}$. Let w be a vector on F_2^n such that $w_i = 0$ if ith column belongs to S and $w_i = 1$ in opposite case. It is clear that $|w| = n - h \geq m + i + 1$. By Theorem 1 the equation (1) holds. The right side of (1) is divisible by 2^{m+i+2}. By assumption all terms in the left side of (1) are divisible by 2^{m+i+1}. Therefore the number of terms in the left side of (1) that equivalent to 2^{m+i+1} by modulo 2^{m+i+2} is even. Thus, in chosen h columns all-zeroes h-tuple occurs in even number of rows. $\square$

Theorem 8 *For $n \geq 7$ there does not exist unbalanced nonconstant $(n-3)$th order correlation immune function on F_2^n.*

Proof. Let f be an unbalanced nonconstant $(m = n-3)$th order correlation immune function on F_2^n. If $\widehat{\chi_f}(u) \equiv 2^{m+1} \pmod{2^{m+2}}$ for some $u \in F_2^n$ then by Corollary 1 we have $n \leq 6$. Suppose that $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$ for every $u \in F_2^n$. If $\widehat{\chi_f}(u) = \pm 2^n$ for some $u \in F_2^n$ then f is an affine function, so, it can not be unbalanced nonconstant. Thus, $\widehat{\chi_f}(u) = \pm 2^{n-1}$ for exactly four vectors $u \in F_2^n$ and $\widehat{\chi_f}(u) = 0$ for all remained vectors. In this case the matrix $M = M(f)$ is the matrix M_1. This matrix contains four rows. One of these rows is all-zeroes row, and each of another three rows contains at most two zeroes by spectral characterization [4]. By Lemma 2 each column of M must contain at least two zeroes. Therefore M contains at most 6 columns. $\square$

Note that there exist unbalanced nonconstant $(6-3)$th order correlation immune functions on F_2^6.

Lemma 4 *Let f be an $(m = n-4)$th order correlation immune function on F_2^n such that $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$ for all $u \in F_2^n$ and the matrix $M_1 = M_1(f)$ does not contain all-zeroes row. Then if some column of M_1 contains at least one symbol 0 then this column contains at least four zeroes.*

Proof. Suppose that f is an $(m = n-4)$th order correlation immune function on F_2^n such that $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$ and the matrix $M_1 = M_1(f)$ does not contain all-zeroes row. Consider an arbitrary (say, ith) column of M_1 that contains a zero. Then by Theorem 6 the ith column contains at least two zeroes. The matrix M_1 does not contain the same rows, therefore some row contains zeroes in ith and some other (say, jth) positions. Then by Theorem 6 there exist at least two rows in M_1 that contain zeroes in ith and jth components. The matrix M_1 does not contain the same rows, therefore the row l_1 contains zeroes in ith, jth and some other (say, kth) positions whereas the row l_2 contains zeroes in ith and jth positions and does not contain zero in kth position. But by Theorem 6 even number of rows contain zeroes in the ith and kth columns simultaneously. Therefore there exists the row l_3 in M_1 that contains zeroes in ith and kth columns. Thus, we have at least three rows that contain zero in the ith column. Then by Theorem 6 the ith column must contain at least four zeroes. $\square$

Theorem 9 *For $n \geq 10$ there does not exist unbalanced nonconstant $(n-4)$th order correlation immune function on F_2^n.*

Proof. Let f be an unbalanced nonconstant $(m = n-4)$th order correlation immune function on F_2^n. If $\widehat{\chi_f}(u) \equiv 2^{m+1} \pmod{2^{m+2}}$ for some $u \in F_2^n$ then by Corollary 1 we have $n < 9$. So, we can assume that $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$ for every $u \in F_2^n$. If $\widehat{\chi_f}(u) = \pm 2^n$ for some $u \in F_2^n$ then f is an affine function, so, it can not be unbalanced nonconstant. Thus, $\widehat{\chi_f}(u) \equiv 2^{n-2} \pmod{2^{n-1}}$ for r_1 vectors $u \in F_2^n$, $\widehat{\chi_f}(u) = \pm 2^{n-1}$ for r_2 vectors $u \in F_2^n$, and $\widehat{\chi_f}(u) = 0$ for all remained vectors. By Parseval's equation $r_1 + 4r_2 \leq 16$. We decompose the matrix $M = M(f)$ into the matrix M_1 with r_1 rows and the matrix M_2 with r_2 rows. One of two matrices M_1 and M_2 contains all-zeroes row. Suppose that M_1 contains all-zeroes row. Then by Theorem 6 any two columns in M_1 must have zeroes simultaneously in some other row. Each row in M_1 with ones contains at most three zeroes, therefore $r_1 - 1$ rows give at most $3(r_1 - 1)$ combinations of two zeroes in one row. It follows that $\frac{n(n-1)}{2} \leq 3(r_1 - 1) \leq 45$. Thus, $n \leq 10$. But if $n = 10$ then $r_1 - 1 = 15$ and 15 rows of M_1 give Steiner triple system. It is well-known that there does not exist Steiner triple system for even n. Therefore in this case $n \leq 9$. Now suppose that M_2 contains all-zeroes row. Then M_1 does not contain all-zeroes row. By Lemma 4 we have that each column with zeroes in M_1 contains at least 4 zeroes. It follows that the number of columns with zeroes in M_1 is at most $(3/4)r_1$. Note that $r_2 \geq 1$. By Lemma 2 the matrix M_2 contains at most $3(r_2 - 1)$ additional columns with zeroes. We have $n \leq (3/4)r_1 + 3(r_2 - 1) \leq (3/4)(16 - 4r_2) + 3(r_2 - 1) = 9$. Thus, in any case $n \leq 9$. □

Note that there exists unbalanced nonconstant $(9-4)$th order correlation immune function on F_2^9 (see [10]).

In [2] it is proved that $p(3) = 4$. In this work we establish the value $p(4)$.

Theorem 10 *For $n \geq 11$ there does not exist $(n-4)$-resilient function on F_2^n that depends nonlinearly on all its n variables.*

Proof. Let f be an $(m = n-4)$-resilient function on F_2^n that depends nonlinearly on all its n variables. It follows that the matrix $M = M(f)$ does not contain all-ones columns. By Theorem 2 we have that $\widehat{\chi_f}(u) \equiv 0 \pmod{2^{m+2}}$ for every $u \in F_2^n$. If $\widehat{\chi_f}(u) = \pm 2^n$ for some $u \in F_2^n$ then f is an affine function, so, it depends linearly on some variables. Thus, $\widehat{\chi_f}(u) \equiv 2^{n-2} \pmod{2^{n-1}}$ for r_1 vectors $u \in F_2^n$, $\widehat{\chi_f}(u) = \pm 2^{n-1}$ for r_2 vectors $u \in F_2^n$, and $\widehat{\chi_f}(u) = 0$ for all remained vectors. By Parseval's equation $r_1 + 4r_2 \leq 16$. We decompose the matrix $M = M(f)$ into the matrix M_1 with r_1 rows and the matrix M_2 with r_2 rows. By Lemma 4 we have that each column with zeroes in M_1 contains at least 4 zeroes. It follows that the number of columns with zeroes in M_1 is at most $(3/4)r_1$. If $r_2 = 1$ then the matrix M_1 contains at most 9 columns with zeroes, and by Lemma 2 the matrix M_2 does not contain additional columns with zeroes. If $r_2 = 2$ then the matrix M_1 contains at most 6 columns with zeroes, and by Lemma 2 the matrix M_2 contains at most 2 additional columns with zeroes. If $r_2 = 3$ then the matrix M_1 contains at most 3 columns with zeroes, and by Lemma 2 the matrix M_2 contains at most 4 additional columns with zeroes. If $r_2 = 4$ then the matrix M_1 is empty, and by Lemma 2 the matrix M_2 contains at most 6 additional columns with zeroes. Thus, if $r_2 \geq 1$ then $n \leq 9$. The only remained case is $r_2 = 0$. Therefore we can assume that the matrix M_2 is empty. If $|\widehat{\chi_f}(u)| = 3 \cdot 2^{n-2}$ for some $u \in F_2^n$ then M_1 contains at most 8 rows. It follows that $n \leq 6$. So, we assume that all nonzero Walsh coefficients are $\pm 2^{n-2}$ and M_1 contains exactly 16 rows. It follows that $n \leq 12$. For $n = 11, 12$ we have found by means of computer search all nonequivalent $(0,1)$ matrices of size $(16 \times n)$ without the same rows, all-ones columns and with at most three zeroes in each row that contain even number of appearances for every possible 2-tuple inside of any two columns. For each of such matrices we have checked all 2^{16} possible distributions of $\pm$ signs for nonzero Walsh coefficients and tried to calculate the values of Boolean function via inversion formula. But in all cases for some $x \in F_2^n$ the value $2^{-n} \sum\limits_{u \in F_2^n} \widehat{\chi_f}(u)(-1)^{<u,x>}$ was not equal to ± 1. Thus, we conclude that $n \leq 10$. □

Note that there exists $(10-4)$-resilient function on F_2^{10} that depends nonlinearly on all its 10 variables (see constructions in [10, 12]). Thus, Theorems 9 and 10 follow that

Theorem 11 *p'(4)=p(4)=10.*

Theorem 11 together with results of [9, 11] follows that

Theorem 12 *The number of $(n-4)$th order correlation immune functions as well as the number of $(n-4)$-resilient functions on F_2^n is $\Theta(n^{10})$.*

References

[1] J. Bierbrauer, Bounds on orthogonal arrays and resilient functions, Journal of Combinatorial Designs, V. 3, 1995, pp. 179–183.

[2] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science, V. 576, 1991, pp. 86–100.

[3] J. Friedman, On the bit extraction problem, Proc. 33rd IEEE Symposium on Foundations of Computer Science, 1992, pp. 314–319.

[4] Xiao Guo-Zhen, J. Massey, A spectral characterization of correlation-immune combining functions, IEEE Transactions on Information Theory, V. 34, No 3, May 1988, pp. 569–571.

[5] F. J. Mac Williams, N. J. A. Sloane, The theory of error correcting codes, North-Holland, Amsterdam, 1977.

[6] P. Sarkar, S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, In Advanced in Cryptology: Crypto 2000, Proceedings, Lecture Notes in Computer Science, V. 1880, 2000, pp. 515–532.

[7] P. Sarkar, Spectral domain analysis of correlation immune and resilient Boolean functions, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/049, September 2000, 10 pp.

[8] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Transactions on Information theory, V. IT-30, No 5, 1984, p. 776–780.

[9] Yu. Tarannikov. Ramsey-like theorems on the structure and numbers of higher order correlation-immune functions, Moscow State University, French-Russian Institute of Applied Mathematics and Informatics, Preprint No 5, Moscow, October 1999, 20 pp.

[10] Yu. Tarannikov. On a method for the constructing of cryptographically strong Boolean functions, Moscow State University, French-Russian Institute of Applied Mathematics and Informatics. Preprint No 6, Moscow, October 1999, 24 pp.

[11] Yu. Tarannikov, On the structure and numbers of higher order correlation-immune functions, Proceedings of 2000 IEEE International Symposium on Information Theory ISIT2000, Sorrento, Italy, June 25–30, 2000, p. 185.

[12] Yu. Tarannikov, On resilient Boolean functions with maximal possible nonlinearity, Cryptology ePrint archive (http://eprint.iacr.org/), Report 2000/005, March 2000, 18 pp., to appear in Proceedings of Indocrypt 2000, Lecture Notes in Computer Science.

[13] Y. Zheng, X.-M. Zhang, Improving upper bound on nonlinearity of high order correlation immune functions, to appear in SAC 2000, Lecture Notes in Computer Science, Springer Verlag, 2000.