On the Constructing of Highly Nonlinear Resilient Boolean Functions by Means of Special Matrices

Maria Fedorova * and Yuriy Tarannikov **

Mech. & Math. Department
Moscow State University
119899 Moscow, Russia

Abstract. In this paper we consider matrices of special form introduced in [11] and used for the constructing of resilient functions with cryptographically optimal parameters. For such matrices we establish lower bound $\frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$ for the important ratio $\frac{t}{t+k}$ of its parameters and point out that there exists a sequence of matrices for which the limit of ratio of these parameters is equal to lower bound. By means of these matrices we construct m-resilient n-variable functions with maximum possible nonlinearity $2^{n-1} - 2^{m+1}$ for $m = 0.5902\ldots n + O(\log_2 n)$. This result supersedes the previous record.

Keywords: *stream cipher, Boolean function, nonlinear combining function, correlation-immunity, resiliency, nonlinearity, special matrices.*

1 Introduction

Different types of ciphers use Boolean functions. So, LFSR based stream ciphers use Boolean functions as a nonlinear combiner or a nonlinear filter, block ciphers use Boolean functions in substitution boxes and so on. Boolean functions used in ciphers must satisfy some specific properties to resist different attacks. One of the most important desired properties of Boolean functions in LFSR based stream ciphers is *correlation immunity* introduced by Siegenthaler [9]. Another important properties are nonlinearity, algebraic degree and so on.

The most usual theoretic motivation for the investigation of highly nonlinear resilient Boolean functions is the using of such functions as nonlinear combiners in stream ciphers. But from the practical point of view the number of variables in such system can not be too big (in opposite case the key length will be too long). It is necessary to note that all important functions with small number of variables are found already by exhaustive search. At the same time another important practical type of stream ciphers uses Boolean functions as nonlinear filters. Here, in general, it is possible to use the functions with big number of

* e-mail: maria_fedorova@yahoo.com

** e-mails: yutaran@mech.math.msu.su, taran@vertex.inria.msu.ru

variables. But the main problems here is that effective (from implementation point of view) constructions of such functions can not be found by exhaustive search, and also it was pointed out [4] that stream cipher of such type can be transformed into an equivalent (in some sence) with worse resiliency but the same nonlinearity. It emphasizes the importance of direct effective constructions of Boolean functions with big number of variables and optimal combination of resiliency and nonlinearity.

Correlation immunity (or resiliency) is the property important in cryptography not only in stream ciphers. This is an important property if we want that the knowledge of some specified number of input bits does not give a (statistical) information about the output bit. In this respect such functions are considered in [3], [2] and other works.

It was proved independently in [8], [10] and [12] that the nonlinearity of n-variable m-resilient function does not exceed $2^{n-1} - 2^{m+1}$ for $m \leq n - 1$. It was proved that if this bound is achieved then $m > 0.5n - 2$. In [10] it was proved that if this bound is achieved then the algebraic degree of the function is maximum possible too (i. e. achieves *Siegenthaler's Inequality*) and equal to $n - m - 1$. In [10], [6] and [11] effective constructions of m-resilient n-variable functions with maximum possible nonlinearity $2^{n-1} - 2^{m+1}$ for $m \geq \frac{2n-7}{3}$, $m \geq \frac{2n-9}{3}$ and $m \geq 0.6n - 1$ correspondently were given. To obtain this result in [11] the concept of a *proper* (k_0, k, p, t)-matrix were introduced. In [11] it was pointed out that the mostly important to find a proper (k, k, p, t)-matrix where the ratio $\frac{t}{t+k}$ is as small as possible. In [11] it was given a proper $(4, 4, 6, 6)$-matrix for which this ratio is 0.6. At the same time the lowest possible value of the ratio $\frac{t}{t+k}$ for proper matrices was formulated in [11] as the open problem. In the present paper we investigate the problem of the lowest possible value of the ratio $\frac{t}{t+k}$ for proper matrices and establish that this ratio can not be less than $\frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$ At the same time we construct proper matrices that approach this lower bound with arbitrary precision. By means of these matrices we construct m-resilient n-variable functions with maximum possible nonlinearity $2^{n-1} - 2^{m+1}$ for $m = 0.5902\ldots n + O(\log_2 n)$. Note that our nonexistence results demonstrate that only proper matrices technique is not sufficient to construct m-resilient n-variable functions with maximum possible nonlinearity $2^{n-1} - 2^{m+1}$ for $m < 0.5902\ldots n + O(1)$. At the same time it is quite possible that such functions there exist for any m, n provide $0.5n - 2 < m \leq n - 2$. At least an opposite result have not proved. Thus, the constructing of such functions demands new methods and new techniques.

The rest of this paper is organized as follows. In Section 2 we give preliminary concepts and notions. In Section 3 we formulate necessary concepts and results from the previous work [11] on proper matrices. In Section 4 we give geometrical interpretation of proper matrices. In Section 5 we prove that there does not exist a proper (k_0, k, p, t)-matrix if $\frac{t}{k+t} < \frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$ In Section 6 we construct proper (k_0, k, p, t)-matrices with ratio $\frac{t}{k+t}$ close to $\frac{1}{\log_2(\sqrt{5}+1)}$ and $k > \alpha k_0$ where $\alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right) = 1.5523\ldots$. In Section 7 by means of proper matrices constructed in Section 6 we construct m-resilient n-variable functions with maximum possible nonlinearity $2^{n-1}-2^{m+1}$ for $m=\frac{1}{\log_2(\sqrt{5}+1)}n+O(\log_2 n)=0.5902\ldots n+O(\log_2 n)$. In Section 8 we discuss the method that probably gives the best possible in some sence concrete proper matrices.

2 Preliminary concepts and notions

We consider V^n, the vector space of n tuples of elements from $GF(2)$. A *Boolean function* is a function from V^n to $GF(2)$. The *weight* $wt(f)$ of a function f on V^n is the number of vectors x on V^n such that $f(x)=1$. A function f is said to be *balanced* if $wt(f)=wt(f\oplus 1)$. Obviously, if a function f on V^n is balanced then $wt(f)=2^{n-1}$. A *subfunction* of the Boolean function f is a function f' obtained by substitution some constants for some variables in f. If a variable x_i is not substituted by constant then x_i is called a *free* variable for f'.

The *Hamming distance* $d(x',x'')$ between two vectors x' and x'' is the number of components where vectors x' and x'' differ. For two Boolean functions f_1 and f_2 on V^n, we define the distance between f_1 and f_2 by $d(f_1,f_2)=\#\{x\in V^n|f_1(x)\neq f_2(x)\}$. The minimum distance between f and the set of all affine functions (i. e. functions of the form $f(x)=c_0\oplus\bigoplus\limits_{i=1}^{n}c_ix_i$) is called the *nonlinearity* of f and denoted by $nl(f)$.

A Boolean function f on V^n is said to be *correlation-immune of order* m, with $1\le m\le n$, if $wt(f')=wt(f)/2^m$ for any its subfunction f' of $n-m$ variables. This concept was introduced by Siegenthaler [9]. A balanced mth order correlation immune function is called an m*-resilient* function. From this point of view it is possible to consider formally any balanced Boolean function as 0-resilient (this convention is accepted in [1], [7], [5]) and an arbitrary Boolean function as (-1)-resilient (this convention is accepted in [10] and [11]). The concept of an m-resilient function was introduced in [3].

3 Results of previous work on proper matrices

In [11] for the constructing of new m-resilient n-variable Boolean functions with maximum possible nonlinearity $2^{n-1}-2^{m+1}$ the concept of a *proper matrix* was introduced.

Definition 1. [11] *Let $B=(b_{ij})$ be $(2^k\times p)$ matrix of 2^k rows and p columns with entries from the set $\{1,2,*\}$. Let k_0 and t be positive integers. We assume that*

(i) for every two rows i_1 and i_2 there exists a column j such that $b_{i_1j}=1$, $b_{i_2j}=2$ or $b_{i_1j}=2$, $b_{i_2j}=1$.

(ii) for every row i the inequality $\sum\limits_{j=1}^{p}b_{ij}\le t$ holds (a sign $*$ does not give an influence to these sums).

(iii) in every row the number of ones does not exceed k_0.

If the matrix B satisfies all properties (i), (ii), (iii) we say that B is a proper *(k_0, k, p, t)-matrix.*

The proper $(k_0,\ k,\ p,\ t)$-matrix is denoted in [11] by $B_{k_0,k,p,t}$. The next examples of proper matrices are given in [11].

$$B_{1,0,1,1} = (\,1\,)\,,\; B_{1,1,1,2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}\,,\; B_{3,2,3,3} = \begin{pmatrix} 2 & 1 & * \\ * & 2 & 1 \\ 1 & * & 2 \\ 1 & 1 & 1 \end{pmatrix}\,,$$

$$B_{3,3,4,5} = \begin{pmatrix} * & 1 & 2 & 2 \\ 2 & * & 1 & 2 \\ 2 & 2 & * & 1 \\ 1 & 2 & 2 & * \\ 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}, B_{4,4,6,6} = \begin{pmatrix} 2 & 2 & 2 & * & * & * \\ 1 & 2 & * & 1 & 2 & * \\ 1 & 2 & * & * & 1 & 2 \\ 1 & 2 & * & 2 & * & 1 \\ * & 1 & 2 & 1 & 2 & * \\ * & 1 & 2 & * & 1 & 2 \\ * & 1 & 2 & 2 & * & 1 \\ 2 & * & 1 & 1 & 2 & * \\ 2 & * & 1 & * & 1 & 2 \\ 2 & * & 1 & 2 & * & 1 \\ 2 & * & 1 & 1 & 1 & 1 \\ 1 & 2 & * & 1 & 1 & 1 \\ * & 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & * & 1 \\ 1 & 1 & 1 & 1 & 2 & * \\ 1 & 1 & 1 & * & 1 & 2 \end{pmatrix}.$$

The next definitions were given in [11].

Definition 2. *A Boolean function $f = f(x_1, \ldots, x_n)$ depends on a pair of its variables (x_i, x_j)* quasilinearly *if $f(x') \neq f(x'')$ for any two vectors x' and x'' of length n that differ only in ith and jth components. A pair (x_i, x_j) in this case is called a* pair of quasilinear variables *in f.*

Definition 3. *Let F be a set of Boolean functions such that for every s, $0 \leq s \leq k$, the set F contains an $(m+s)$-resilient function on V^{n+s} with nonlinearity at least $2^s(2^{n-1} - 2^{m+\lambda})$ (λ is not necessary integer). Moreover, we assume that each f_s contains s disjoint pairs of quasilinear variables. Then we say that F is a $S_{n,m,k,\lambda}$-*system *of Boolean functions.*

Remark. [11] To provide an existence of a $S_{n,m,k,\lambda}$-system of Boolean functions it is sufficient to have only one $(m+k)$-resilient function f on V^{n+k} with nonlinearity at least $2^k(2^{n-1} - 2^{m+\lambda})$ that contains k disjoint pairs of quasilinear variables. All other necessary functions of $S_{n,m,k,\lambda}$-system can be obtained from f by substitutions of constants for the variables from different disjoint pairs of quasilinear variables.

The next theorem was proved in [11].

Theorem 1. *[11] Suppose that there exists an $S_{n,m,k_0,\lambda}$-system of Boolean functions F and there exists a proper (k_0,k,p,t)-matrix B, $n \geq 2p-t$. Then there exists an $S_{n+k+t,m+t,k,\lambda}$-system of Boolean functions.*

An application of the construction given in Theorem 1 is denoted in [11] by

$$S_{n,m,k_0,\lambda}T_{k_0,k,p,t} = S_{n+k+t,m+t,k,\lambda}.$$

Lemma 1. *[11] There exists an $S_{2,-1,2,1}$-system of Boolean functions.*

Indeed, the functions $f_0' = x_1x_2$, $f_1' = (x_1 \oplus x_2)x_3 \oplus x_1$, $f_2' = (x_1 \oplus x_2)(x_3 \oplus x_4) \oplus x_1 \oplus x_3$ forms the $S_{2,-1,2,1}$-system of Boolean functions, i. e. for $i = 0, 1, 2$ the system contains $(2+i)$-variable $(-1+i)$-resilient Boolean function of nonlinearity $2^{1+i} - 2^i$.

The results of [11] demonstrate that if there exists a proper (k,k,p,t)-matrix then there exists a constant C' such that for any n and m provided $m \geq \frac{t}{k+t}n + C'$ there exists an m-resilient n-variable Boolean function with the nonlinearity $2^{n-1} - 2^{m+1}$. Thus, the important problem is to construct a proper (k,k,p,t)-matrix with ratio $\frac{t}{k+t}$ as small as possible. In [11] it was given an example of a proper $(4,4,6,6)$-matrix where the value $\frac{t}{k+t}$ is equal to 0.6.

In this work we study the problem of the existence of proper (k_0,k,p,t)-matrices.

4 Geometrical interpretation

In this paper we consider *a Boolean cube* B^p as the set of all vectors $(x_1,\dots,x_p)$ where $x_i \in \{1,2\}$. The *lth level* of the Boolean cube B^p is the set of all vectors of B^p with exactly l ones. The cardinality of lth level of B^p is $\binom{p}{l}$.

A proper (k_0,k,p,t)-matrix B can be interpreted [11] as a collection of 2^k disjoint subcubes in Boolean cube $\{1,2\}^p$. Indeed, a row of B can be interpreted as a subcube where the components with $*$ are free whereas the components with 1 or 2 are substituted by correspondent constants. The next illustration at the example of a proper $(3,3,4,5)$-matrix B is given in [11].

row of B	points of a subcube
$*122$	$\{(1,1,2,2),(2,1,2,2)\}$
$2*12$	$\{(2,1,1,2),(2,2,1,2)\}$
$22*1$	$\{(2,2,1,1),(2,2,2,1)\}$
$122*$	$\{(1,2,2,1),(1,2,2,2)\}$
2111	$\{(2,1,1,1)\}$
1211	$\{(1,2,1,1)\}$
1121	$\{(1,1,2,1)\}$
1112	$\{(1,1,1,2)\}$

The property (i) of a proper matrix provides that subcubes are disjoint. The properties (ii) and (iii) characterize the location of subcubes in a cube and the size of subcubes.

5 Lower bound for the value $\frac{t}{k+t}$

In this Section we prove that there does not exist a proper (k_0, k, p, t)-matrix if

$$\frac{t}{k+t} < \frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$$

Lemma 2. *If there exists a proper (k_0, k, p, t)-matrix B then for any $p' > p$ there exists a proper (k_0, k, p', t)-matrix.*

Proof. We obtain a proper (k_0, k, p', t)-matrix simply adding $p' - p$ new all-$*$ columns to B. □

The next lemma is obvious.

Lemma 3. *If there does not exist a proper (k_0, k, p, t)-matrix B then for any $k_0' < k_0$ there does not exist a proper (k_0', k, p, t)-matrix.*

Theorem 2. *There does not exist a proper (k_0, k, p, t)-matrix for*

$$\frac{t}{k+t} < \frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$$

Proof.

By Lemma 3 it is sufficient to prove this theorem for $k_0 = t$.

Let B be an arbitrary proper (t, k, p, t)-matrix. We can consider B as the set of disjoint subcubes of the Boolean cube B^p if we consider each row of B as a subcube. These subcubes are disjoint by item (i) in definition 1 of a proper matrix.

If t is even then we replace in rows with odd number of ones some asterisk by one (if there are not asterisks in a row then we add preliminary all-$*$ column to the matrix B, after this procedure the parameter p will increase but this is not important for us). If t is odd we do the same for all rows with even number of ones. Now for even t all rows contain even number of ones and for odd t all rows contain odd number of ones. If the matrix B contains rows where the sum of ones and twos is less than $t-1$ then we replace asterisks in these rows by twos (adding if necessary new all-$*$ columns to B) until the sum of ones and twos will become greater than $t-1$, i. e. t.

Thus, without loss of generality we can assume that the sum of ones and twos in any row of B is exactly t.

Consider a subcube defined by a row of B with exactly s twos and exactly r ones. Then lth level of Boolean cube B^p contains exactly $\binom{p-s-r}{l-r}$ vectors of this subcube if $l = r, \ldots, p-s$, and does not contain such vectors for another l.

Suppose that t is even (for odd t the reasoning is analogous). Then lth level of Boolean cube contains $\binom{p-t/2}{l}$ vectors from each subcube defined by the rows of B with exactly $t/2$ twos and exactly 0 ones, $\binom{p-t/2-1}{l-2}$ vectors from each subcube defined by the rows of B with exactly $t/2-1$ twos and exactly 2 ones and so on. Denote the number of rows of B with exactly i ones by c_i. Then for any $l = 0, 1, \dots, p$ the next inequality holds:

$$\sum_{i=0}^{t/2} c_{2i} \binom{p - t/2 - i}{l - 2i} \leq \binom{p}{l}.$$

It follows

$$\sum_{i=0}^{t/2} c_{2i} \frac{(p - t/2 - i)!}{(l-2i)!(p - t/2 - l + i)!} \leq \frac{p!}{l!(p-l)!}.$$

Put $l = \alpha \cdot p$. Then

$$\sum_{i=0}^{t/2} c_{2i} \frac{(p - t/2 - i)\dots(p - t/2 - t/2 + 1)}{(\alpha p - 2i)\dots(\alpha p - t + 1)(p(1-\alpha) - t/2 + 1)\dots(p(1-\alpha) - t/2 + i)} \leq$$
$$\frac{p(p-1)\dots(p - t/2 - t/2 + 1)}{\alpha p(\alpha p - 1)\dots(\alpha p - t + 1)(p(1-\alpha) - t/2 + 1)\dots(p(1-\alpha) - 1)(p(1-\alpha))}.$$

Note that adding new all-$*$ columns to B we can obtain a proper (t, k, p', t)-matrix for any $p' > p$. Thus, if there does not exist a proper (t, k, p', t)-matrix for any $p' > p$ then there does not exist a proper (t, k, p, t)-matrix B. Therefore below we can suppose p as large as necessary. Removing the parentheses we have

$$\sum_{i=0}^{t/2} c_{2i} \frac{p^{t/2-i} + a_i^1 p^{t/2-i-1} + \dots}{((\alpha p)^{t-2i} + a_i^2 (\alpha p)^{t-2i-1} + \dots)(((1-\alpha)p)^i + a_i^3((1-\alpha)p)^{i-1} + \dots)} \leq$$
$$\frac{p^t + b^1 p^{t-1} + \dots}{((\alpha p)^t + b^2(\alpha p)^{t-1} + \dots)((p(1-\alpha))^{t/2} + b^3(p(1-\alpha))^{t/2-1} + \dots)}$$

where $a_i^1, a_i^2, a_i^3, b^1, b^2, b^3$ — numbers that do not depend on p.

Next, we multiply both parts of this inequality by $p^{t/2}\alpha^t$ and transform the fractions. We have

$$\sum_{i=0}^{t/2} c_{2i} \left(\frac{\alpha^2}{1-\alpha}\right)^i (1 + a_i/p + O(1/p^2)) \leq$$
$$(1 + \max\{a_i\}/p + O(1/p^2)) \sum_{i=0}^{t/2} c_{2i} \left(\frac{\alpha^2}{1-\alpha}\right)^i \leq \frac{1}{(1-\alpha)^{t/2}}(1 + b/p + O(1/p^2))$$

where a_i, b do not depend on p. Next,

$$\sum_{i=0}^{t/2} c_{2i} \left(\frac{\alpha^2}{1-\alpha}\right)^i \leq \frac{1}{(1-\alpha)^{t/2}} \frac{(1 + b/p + O(1/p^2))}{(1 + \max\{a_i\}/p + O(1/p^2))} \leq$$
$$\frac{1}{(1-\alpha)^{t/2}}(1 + b'/p + O(1/p^2)).$$

Pointing in a view that we can take p as large as desired for fixed remained parameters, we have

$$\sum_{i=0}^{t/2} c_{2i}\left(\frac{\alpha^2}{1-\alpha}\right)^i \leq \frac{1}{(1-\alpha)^{t/2}}.$$

To find the sum of c_i we take $\alpha = \frac{\sqrt{5}-1}{2}$ (the root of the equation $\frac{\alpha^2}{1-\alpha} = 1$). This number is irrational but we can approach it by the sequence of rational numbers. As a result, we have:

$$\sum_{i=0}^{\lfloor t/2 \rfloor} c_{2i} \leq \left(\frac{\sqrt{5}+1}{2}\right)^t.$$

Therefore, $k \leq \log_2 \sum_{i=0}^{\lfloor t/2 \rfloor} c_{2i} \leq \log_2 \left(\frac{\sqrt{5}+1}{2}\right)^t$ and $\frac{t}{t+k} \geq \frac{1}{\log_2(\sqrt{5}+1)}$. □

6 The sequence of proper matrices with $\frac{t}{k+t} \to 0.5902\ldots$

In the previous Section we had demonstrated that for any proper (k_0, k, p, t)-matrix the inequality $\frac{t}{k+t} < \frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$ holds. Nevertheless, it appears that the ratio $\frac{t}{k+t}$ can approach the value $\frac{1}{\log_2(\sqrt{5}+1)} = 0.5902...$ with arbitrary precision. In this Section we construct proper (k_0, k, p, t)-matrices with ratio $\frac{t}{k+t}$ close to $\frac{1}{\log_2(\sqrt{5}+1)}$ and $k > \alpha k_0$ where $\alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right) = 1.5523\ldots$.

Lemma 4. *Suppose that* $\alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right)$. *Let*

$$k_0(t,\alpha) = \left\lfloor \frac{t}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2}\right) + \frac{1}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right) - 1 \right\rfloor.$$

Then

$$\binom{\left\lfloor \frac{t+k_0(t,\alpha)-1}{2} \right\rfloor}{k_0(t,\alpha)+1} \geq \binom{\left\lfloor \frac{t+k_0(t,\alpha)+1}{2} \right\rfloor}{k_0(t,\alpha)+3}(1+o(1))$$

and

$$\binom{\left\lfloor \frac{t+k_0(t,\alpha)}{2} \right\rfloor}{k_0(t,\alpha)+2} \geq \binom{\left\lfloor \frac{t+k_0(t,\alpha)+2}{2} \right\rfloor}{k_0(t,\alpha)+4}(1+o(1)).$$

Proof. We solve the inequality

$$\binom{\left\lfloor \frac{t+k_0(t,\alpha)-1}{2} \right\rfloor}{k_0(t,\alpha)+1} \geq \binom{\left\lfloor \frac{t+k_0(t,\alpha)+1}{2} \right\rfloor}{k_0(t,\alpha)+3} \tag{1}$$

(the inequality

$$\binom{\left\lfloor\frac{t+k_0(t,\alpha)}{2}\right\rfloor}{k_0+2} \geq \binom{\left\lfloor\frac{t+k_0(t,\alpha)+2}{2}\right\rfloor}{k_0+4}$$

gives the same asymptotics). Using the factorial representation for binomial coefficients we solve the quadratic inequality for $k_0(t,\alpha)$ considering t as some parameter. As a result we obtain that the inequality (1) holds if

$$k_0(t,\alpha) \geq \frac{1}{\sqrt{5}} t(1+o(1)). \tag{2}$$

But by the hypothesis of Lemma we have that $k_0(t,\alpha)$ is asymptotically $\frac{t}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2}\right)$ and $\alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right)$. It follows the same condition (2) on $k_0(t,\alpha)$ that completes the proof. □

Theorem 3. *For any α, $0 < \alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right) = 1.5523\ldots$, and any $\varepsilon > 0$ there exists a proper (k_0,k,p,t)-matrix such that $\frac{t}{t+k} < \frac{1}{\log_2(\sqrt{5}+1)} + \varepsilon$ and $k > \alpha k_0$.*

Proof. If this Theorem holds for some α, $0 < \alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right)$, then, obviously, this Theorem holds for any α', $0 < \alpha' < \alpha$. Therefore we can assume that $\alpha > \log_2\left(\frac{\sqrt{5}+1}{2}\right) = 0.6942\ldots$

At first, we construct recursively the sequence of matrices A_t, $t = 1, 2, \ldots$, that satisfy properties (i) and (ii) of proper matrices but the number of rows in these matrices is not necessary power of two. We denote by $s(t)$ the number of rows in the matrix A_t obtained after tth step.

At tth step we construct the matrix A_t such that the sum of ones and twos in any row of A_t does not exceed t and for any two different rows of A_t there exists a column such that one of these two rows has one in this column, and the second row has two in this column. We suppose that the matrices A_{t-1} and A_{t-2} were constructed at the previous steps. We suppose that the matrices A_{t-1} and A_{t-2} have the same number of columns (in opposite case we add to one of them the deficient number of all-$*$ columns). Next, we add to each of these matrices from the right side an additional column: the all-ones column to the matrix A_{t-1} and the all-twos column to the matrix A_{t-2}. Write the obtained matrices one over another. We say the resulting matrix is the matrix A_t, $A_t = \begin{pmatrix} A_{t-1} & \vec{\mathbf{1}}^T \\ A_{t-2} & \vec{\mathbf{2}}^T \end{pmatrix}$.

The matrix A_t is the matrix of desired form such that the sum of ones and twos in each row of A_t does not exceed t. The number of rows in A_t is equal to

$$s(t) = s(t-2) + s(t-1).$$

Thus, $s(t)$ forms the Fibonacci sequence and $s(t)$ is asymptotically $\frac{1}{\sqrt{5}} \cdot \left(\frac{\sqrt{5}+1}{2}\right) \cdot \left(\frac{\sqrt{5}+1}{2}\right)^t$ if we take the matrices $A_1 = (1)$ and $A_2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ as initial. In this construction the matrix A_t contains the rows with the number of ones greater than $k_0(t,\alpha) = \left\lfloor \frac{t}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2}\right) + \frac{1}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right) - 1\right\rfloor$. Calculate the ratio of the number of rows that contain more than k_0 ones to the number of all rows in A_t (i. e. $s(t)$). Denote by $l_j(t)$ the number of rows with exactly j ones in the matrix A_t. By construction $l_0(t) = l_0(t-2)$, $l_j(t) = l_j(t-2) + l_{j-1}(t-1)$ for $j \geq 1$. These recursive relations follow the next direct formula:

$$l_j(t) = \binom{\frac{t+j-2}{2}}{j} l_0(2) + \binom{\frac{t+j-4}{2}}{j-1} l_1(1) + a_2 l_2 + \ldots + a_j l_j$$

if $(t+j)$ even and

$$l_j(t) = \binom{\frac{t+j-3}{2}}{j} l_0(1) + \binom{\frac{t+j-3}{2}}{j-1} l_1(2) + a_2 l_2 + \ldots + a_j l_j$$

if $(t+j)$ odd where $a_2, \ldots, a_j$ — some numbers and arguments of $l_2, \ldots, l_j$ are 1 or 2 (it depends on the parity). For initial matrices A_1 and A_2 introduced above we have $l_0(1) = 0$, $l_0(2) = 1$, $l_1(1) = l_1(2) = 1$, $l_j(1) = l_j(2) = 0$ for $j \geq 2$. Therefore,

$$l_j(t) = \binom{\frac{t+j-2}{2}}{j} + \binom{\frac{t+j-4}{2}}{j-1}$$

if $(t+j)$ even and

$$l_j(t) = \binom{\frac{t+j-3}{2}}{j-1}$$

if $(t+j)$ odd.

It follows

$$\frac{\sum\limits_{j=k_0(t,\alpha)+1}^{t} l_j(t)}{s(t)} \leq \frac{\sum\limits_{j=k_0(t,\alpha)+1}^{t} \left(\binom{\lceil\frac{t+j-2}{2}\rceil}{j} \cdot 1 + \binom{\lceil\frac{t+j-3}{2}\rceil}{j-1} \cdot 1\right)}{\text{const } \cdot \left(\frac{\sqrt{5}+1}{2}\right)^t} \leq$$

(by Lemma 4 for $k_0(t,\alpha) = \left\lfloor \frac{t}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2}\right) + \frac{1}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right) - 1\right\rfloor$)

$$\text{const } \frac{(t - k_0(t,\alpha))\binom{\lceil\frac{t+k_0(t,\alpha)-1}{2}\rceil}{k_0(t,\alpha)+1}}{\left(\frac{\sqrt{5}+1}{2}\right)^t} \leq$$

(denoting $v = \log_2\left(\frac{\sqrt{5}+1}{2}\right)$ and using the Stirling formula),

$$\leq \text{ const } \cdot t \frac{\sqrt{\frac{\frac{1}{2}t\left(1+\frac{v}{\alpha}\right)}{\frac{tv}{\alpha}\cdot\frac{1}{2}t\left(1-\frac{v}{\alpha}\right)}} \frac{\left(\frac{1}{2}t\left(1+\frac{v}{\alpha}\right)\right)^{\frac{1}{2}t\left(1+\frac{v}{\alpha}\right)}}{\left(\frac{tv}{\alpha}\right)^{\frac{tv}{\alpha}}\left(\frac{1}{2}t\left(1-\frac{v}{\alpha}\right)\right)^{\frac{1}{2}t\left(1-\frac{v}{\alpha}\right)}}}{\left(\frac{\sqrt{5}+1}{2}\right)^t} =$$

$$\text{const}\;\cdot\sqrt{t}\frac{\left(1+\frac{v}{\alpha}\right)^{\frac{1}{2}t\left(1+\frac{v}{\alpha}\right)}}{\left(\frac{2v}{\alpha}\right)^{\frac{tv}{\alpha}}\left(1-\frac{v}{\alpha}\right)^{\frac{1}{2}t\left(1-\frac{v}{\alpha}\right)}\left(\frac{\sqrt{5}+1}{2}\right)^{t}} =$$

$$\text{const}\;\cdot\sqrt{t}\left(\frac{\left(1+\frac{v}{\alpha}\right)^{\frac{1}{2}\left(1+\frac{v}{\alpha}\right)}}{\left(\frac{\sqrt{5}+1}{2}\right)^{1+\frac{1}{\alpha}}\left(\frac{v}{\alpha}\right)^{\frac{v}{\alpha}}\left(1-\frac{v}{\alpha}\right)^{\frac{1}{2}\left(1-\frac{v}{\alpha}\right)}}\right)^{t}.$$

It is easy to check that the expression in the parentheses increases monotonically on α for $\log_2\left(\frac{\sqrt{5}+1}{2}\right) = 0.6942\ldots < \alpha \le \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right) = 1.5523\ldots$ and takes the value 1 for $\alpha = \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right)$. Therefore this expression takes values less than 1 for $\log_2\left(\frac{\sqrt{5}+1}{2}\right) < \alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right)$. It follows that $\frac{\sum_{j=k_0(t,\alpha)+1}^{t} l_j(t)}{s(t)} \overset{t\to\infty}{\longrightarrow} 0$ for $\log_2\left(\frac{\sqrt{5}+1}{2}\right) < \alpha < \sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right)$.

Thus, in the matrix A_t the number of rows that contain more than $k_0(t,\alpha)$ ones is asymptotically small with respect to the total number of rows. We eliminate from the matrix A_t all rows that contain more than $k_0(t,\alpha)$ ones. For sufficiently large t the number of such rows is smaller than $2^{k(t)}$ where $k(t) = \lfloor \log_2 s(t)\rfloor - 1$; therefore the obtained matrix will contain at least $2^{k(t)}$ rows. Now the matrix satisfies the property (iii) of a proper matrix (see Definition 1) for $k_0 = k_0(t,\alpha)$, $k = k(t)$. Next, we eliminate if necessary some rows more to obtain the matrix with exactly $2^{k(t)}$ rows. As a result, we have constructed the proper $(k_0(t,\alpha), k(t), p, t)$-matrix for some p. Thus, for the sequence of proper $(k_0(t,\alpha), k(t), p, t)$-matrices constructed above we have

$$\frac{t}{t+k(t)} = \frac{t}{t+\left\lfloor t\log_2\left(\frac{\sqrt{5}+1}{2}\right)+\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)-1\right\rfloor} \quad \overset{t\to\infty}{\longrightarrow} \quad \frac{1}{\log_2(\sqrt{5}+1)}$$

and

$$\frac{k(t)}{k_0(t,\alpha)} = \frac{\left\lfloor t\log_2\left(\frac{\sqrt{5}+1}{2}\right)+\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)-1\right\rfloor}{\left\lfloor \frac{t}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2}\right)+\frac{1}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)-1\right\rfloor} \quad \overset{t\to\infty}{\longrightarrow} \quad \alpha,$$

moreover, if $\alpha > 1$ then $\frac{k(t)}{k_0(t,\alpha)} > \alpha$ for the infinite sequence of t.

The conclusion of the Theorem follows.

$\square$

Remark. Note that in the construction in the proof of Theorem 3 in fact we have $p = 1$ for $t = 1$ and $p = t-1$ for $t > 1$.

7 Constructions of new record highly nonlinear resilient Boolean functions

In this Section by means of proper matrices constructed in the previous Section we construct m-resilient n-variable functions with maximum possible nonlinearity $2^{n-1}-2^{m+1}$ for $m=\frac{1}{\log_2(\sqrt{5}+1)}n+O(\log_2 n)=0.5902\ldots n+O(\log_2 n)$. Until now such functions with maximum possible nonlinearity $2^{n-1}-2^{m+1}$ were known only for $m\ge 0.6n-1$ [11] and some small set of concrete parameters n and m.

Lemma 5. *For any positive integer k there exists a proper $(1,k,2^k+1,2^k+1)$-matrix.*

Proof. We form the quadratic matrix B of order 2^k+1 writing in its rows all possible cyclic shifts of the row $(1\underbrace{22\ldots2}_{2^{k-1}}\underbrace{**\ldots*}_{2^{k-1}})$. It is easy to check that in this matrix for any two different rows there exists a column such that one of these two rows has one in this column, and the second row has two in this column. The sum of numbers in each row of B is exactly 2^k+1. Eliminating any row from B we obtain a proper $(1,k,2^k+1,2^k+1)$-matrix $B_{1,k,2^k+1,2^k+1}$. □

Lemma 6. *For given positive integer k and infinite sequence of positive integer n there exist proper $S_{n,m,k,1}$-systems of Boolean functions for some m.*

Proof. By Lemma 1 there exists an $S_{2,-1,2,1}$-system of Boolean functions. Using Lemma 5 we apply

$$S_{2,-1,2,1}\left(T_{1,1,1,2}\right)^h T_{1,k,2^k+1,2^k+1}.$$

By Theorem 1 this construction is valid if $2+3h\ge 2^k+1$. Therefore for all h provided $h\ge\frac{2^k-1}{3}$ we construct $S_{2^k+k+3h+3,2^k+2h,k,1}$-system of Boolean functions. □

Note that the constructions in Lemmas 5 and 6 are obviously nonoptimal from the practical point of view but more easy for the proof.

Theorem 4. *It is possible to construct m-resilient n-variable function with maximum possible nonlinearity $2^{n-1}-2^{m+1}$ for $m=\frac{1}{\log_2(\sqrt{5}+1)}n+O(\log_2 n)$.*

Proof. We use proper $(k_0(t,\alpha),k(t),p,t)$-matrices constructed in the proof of Theorem 3. Note that by Remark after the proof of Theorem 3 we have $p=t-1$ for $t\ge 2$. We choose $1<\alpha<\sqrt{5}\log_2\left(\frac{\sqrt{5}+1}{2}\right)=1.5523\ldots$ and form the sequence $t_0,t_1,t_2,\ldots$ recursively. By Theorem 3 for given α beginning with sufficiently large t the matrices constructed in the proof of Theorem 3 are proper $(k_0(t,\alpha),k(t),p,t)$-matrices. We denote this sufficiently large t by t_0 (we can assume that $t_0\ge 2$). Suppose that t_i and $k(t_i)$ are already defined positive integers. Then we define t_{i+1} as the maximal positive integer such that

$$k_0(t_{i+1},\alpha)=\left\lfloor\frac{t_{i+1}}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2}\right)+\frac{1}{\alpha}\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)-1\right\rfloor=k(t_i). \quad (3)$$

It is easy to see that $k_0(t,\alpha)$ is nondecreasing on t and $k_0(t+1,\alpha)-k_0(t,\alpha)\le 1$, therefore this definition of t_{i+1} is correct. Finally, we put

$$k(t_{i+1})=\left\lfloor t_{i+1}\log_2\left(\frac{\sqrt{5}+1}{2}\right)+\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)-1\right\rfloor. \qquad (4)$$

The recursive definition is completed.

For defined t_0 by Lemma 6 we construct $S_{n_0,m_0,k(t_0),1}$-system of Boolean functions such that $n_0\ge t_1-2$. After this we define recursively:

$$S_{n_i,m_i,k(t_i),1}T_{k(t_i),k(t_{i+1}),t_{i+1}-1,t_{i+1}}=S_{n_{i+1},m_{i+1},k(t_{i+1}),1},\quad i=0,1,2,\dots$$

Here $n_{i+1}=n_i+k(t_{i+1})+t_{i+1}$, $m_{i+1}=m_i+t_{i+1}$.

By Theorem 1 this construction is valid if $n_i\ge 2p_{i+1}-t_{i+1}=t_{i+1}-2$ for all i. We prove this statement by induction on i. We have $n_0\ge t_1-2$ by construction. Next, suppose that $n_i\ge t_{i+1}-2$. Then using (3) and (4) we have

$$n_{i+1}-t_{i+2}+2=n_i+k(t_{i+1})+t_{i+1}-t_{i+2}+2\ge k(t_{i+1})+2t_{i+1}-t_{i+2}\ge$$
$$t_{i+1}\log_2\left(\frac{\sqrt{5}+1}{2}\right)(2-\alpha)+\sqrt{5}\left(\log_2\left(\frac{\sqrt{5}+1}{2}\right)-\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)-1\right)+$$
$$\frac{\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)}{\log_2\left(\frac{\sqrt{5}+1}{2}\right)}\ge t_{i+1}\cdot 0.3107\ldots-0.3123\ldots>0$$

since $t_{i+1}\ge 2$. Thus, we use the Theorem 1 correctly.

After q steps we have $n_q=n_0+\sum_{i=1}^{q}(k(t_i)+t_i)$, $m_q=m_0+\sum_{i=1}^{q}t_i$. From (4) we have

$$\frac{1}{\log_2\left(\frac{\sqrt{5}+1}{2}\right)}\left(k(t_i)-\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)\right)<t_i\le$$
$$\frac{1}{\log_2\left(\frac{\sqrt{5}+1}{2}\right)}\left(k(t_i)-\log_2\left(\frac{\sqrt{5}+1}{2\sqrt{5}}\right)+1\right).$$

It follows that

$$\frac{m_q}{n_q}=\frac{m_0+\sum_{i=1}^{q}t_i}{n_0+\sum_{i=1}^{q}(k(t_i)+t_i)}=\frac{\frac{1}{\log_2\left(\frac{\sqrt{5}+1}{2}\right)}\sum_{i=1}^{q}k(t_i)+O(q)}{\left(1+\frac{1}{\log_2\left(\frac{\sqrt{5}+1}{2}\right)}\right)\sum_{i=1}^{q}k(t_i)+O(q)}=$$
$$\frac{1}{\log_2\left(\sqrt{5}+1\right)}+O\left(\frac{q}{n_q}\right).$$

It is easy to see that $q=O(\log_2 n_q)$. Therefore, $m_q=\frac{1}{\log_2(\sqrt{5}+1)}n_q+O(\log_2 n_q)$. $\square$

8 Constructions of proper matrices by means of cyclic matrices

The construction of proper matrices in Section 6 gives the best limit value for the ratio $\frac{t}{t+k}$ but in general does not give the best possible matrices for concrete parameters. In this Section we discuss the method that probably gives the best possible in some sence concrete proper matrices.

We denote by $S(t)$ the maximum possible number of rows in matrices that satisfy properties (i) and (ii) of proper (t,k,p,t)-matrices but the number of rows in these matrices is not necessary power of two. By the proof of Theorem 2 we have $S(t) \le \left(\frac{\sqrt{5}+1}{2}\right)^t$. Below we show that $S(t) = \left\lfloor \left(\frac{\sqrt{5}+1}{2}\right)^t \right\rfloor$ at least for $1 \le t \le 10$. We search desired matrices for odd t in the class of matrices with $p = t$ that contain with each its row also all possible cyclic shifts of this row.

Theorem 5. $S(t) = \left\lfloor \left(\frac{\sqrt{5}+1}{2}\right)^t \right\rfloor$ *for* $1 \le t \le 10$.

Proof. For $t = 1,3,5,7,9$ we give the desired matrices M_t directly. Below we give in the matrices only one row from each class of cyclic shifts.

$$M_1 = \{1\},\ M_3 = \left\{\begin{matrix} 2 & 1 & * \\ 1 & 1 & 1 \end{matrix}\right\},\ M_5 = \left\{\begin{matrix} 1 & 2 & 2 & * & * \\ * & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{matrix}\right\},$$

$$M_7 = \left\{\begin{matrix} 1 & 2 & 2 & 2 & * & * & * \\ 1 & 2 & 1 & * & 1 & 2 & * \\ 1 & 1 & * & * & 1 & 2 & 2 \\ 2 & 1 & 1 & 1 & 1 & * & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}\right\},\ M_9 = \left\{\begin{matrix} 1 & 2 & 2 & 2 & 2 & * & * & * & * \\ 1 & 1 & * & 2 & * & 1 & 2 & 2 & * \\ 1 & 2 & 1 & * & * & 1 & 2 & 2 & * \\ 1 & 2 & 1 & 2 & * & * & 1 & * & 2 \\ 1 & 2 & * & 1 & 2 & * & 1 & 2 & * \\ 2 & * & * & 1 & 1 & 2 & 1 & 1 & 1 \\ 2 & 2 & * & 1 & 1 & 1 & 1 & * & 1 \\ * & 2 & 1 & 2 & 1 & 1 & 1 & * & 1 \\ 2 & 1 & 1 & * & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}\right\}.$$

For $t = 2$ we put $M_2 = \begin{pmatrix} 2 & * \\ 1 & 1 \end{pmatrix}$ (here we do not use cyclic shifts). Thus, $S(1) = 1$, $S(2) = 2$, $S(3) = 4$, $S(5) = 11$, $S(7) = 29$, $S(9) = 76$. If t is even, $t > 2$, then $\left\lfloor \left(\frac{\sqrt{5}+1}{2}\right)^t \right\rfloor = \left\lfloor \left(\frac{\sqrt{5}+1}{2}\right)^{t-1} \right\rfloor + \left\lfloor \left(\frac{\sqrt{5}+1}{2}\right)^{t-2} \right\rfloor$. Therefore if t is even, $t > 2$, and desired matrices M_{t-2} and M_{t-1} are constructed already then the matrix M_t can be constructed in the form

$$M_t = \begin{pmatrix} M_{t-1} & \vec{\mathbf{1}}^T \\ M_{t-2}\,\vec{*}^T & \vec{\mathbf{2}}^T \end{pmatrix}.$$

Thus, $S(4) = 6$, $S(6) = 17$, $S(8) = 46$, $S(10) = 122$. $\square$

Hypothesis. $S(t) = \left\lfloor \left(\frac{\sqrt{5}+1}{2}\right)^t \right\rfloor$.

Note that if $k_0 < t$ then a proper (k_0, k, p, t)-matrix can be obtained from M_t by the cancelling all rows where the number of ones is greater than k_0 and some rows up to the nearest power of two.

Using the matrices M_9 and M_{10} as initial in the recursive construction of Theorem 3 we have constructed the 172-variable 102-resilient function with maximum possible nonlinearity as

$$S_{2,-1,2,1}T_{2,2,2,4}T_{2,4,7,8}T_{4,5,7,8}T_{5,6,9,9}T_{6,9,14,14}T_{9,10,15,15}$$
$$T_{10,11,16,16}T_{11,11,16,16}T_{11,9,13,13} = S_{172,102,9,1}.$$

These are the smallest parameters that we have found improving the bound in [11].

References

1. 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.
2. R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz, A. Sahai, Exposure-resilient functions and all-or-nothing transforms, In Advanced in Cryptology: Eurocrypt 2000, Proceedings, Lecture Notes in Computer Science, V. 1807, 2000, pp. 453–469.
3. B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, R. Smolensky, The bit extraction problem or t-resilient functions, IEEE Symposium on Foundations of Computer Science, V. 26, 1985, pp. 396–407.
4. C. Ding, G. Xiao, W. Shan, The stability theory of stream ciphers, Lecture Notes in Computer Science, V. 561, Springer-Verlag, 1991.
5. E. Pasalic, T. Johansson, Further results on the relation between nonlinearity and resiliency for Boolean functions, IMA Conference on Cryptography and Coding, Lecture Notes in Computer Science, Vol. 1746, 1999, pp. 35–44.
6. E. Pasalic, S. Maitra, T. Johansson, P. Sarkar, New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity, WCC2001 International Workshop on Coding and Cryptography, Paris, January 8–12, 2001, Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.
7. P. Sarkar, S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties, In Advanced in Cryptology: Eurocrypt 2000, Lecture Notes in Computer Science, V. 1807, 2000, pp. 485–506.
8. 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.
9. 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.
10. Yu. Tarannikov. On resilient Boolean functions with maximal possible nonlinearity, Proceedings of Indocrypt 2000, Lecture Notes in Computer Science, V. 1977, pp. 19-30, Springer-Verlag, 2000.

11. Yu. Tarannikov. New constructions of resilient Boolean functions with maximal nonlinearity, Preproceedings of 8th Fast Software Encryption Workshop, Yokohama, Japan, April 2-4, 2001, pp. 70-81, also available at Cryptology ePrint archive (http:// eprint.iacr.org/), Report 2000/069, December 2000, 11 pp.
12. Y. Zheng, X. M. Zhang, Improved upper bound on the nonlinearity of high order correlation immune functions, Selected Areas in Cryptography, 7th Annual International Workshop, SAC2000, Lecture Notes in Computer Science, V. 2012, pp. 264–274, Springer-Verlag, 2001.