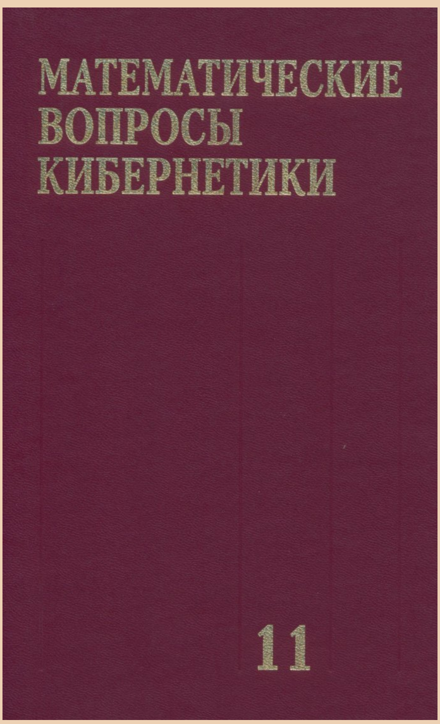
ИПМ им. М.В. Келдыша РАН • Электронная библиотека
Математические вопросы кибернетики • Выпуск 11



П. С. Королёв

Квадратичные булевы функции высокого порядка устойчивости

Рекомендуемая форма библиографической ссылки: Королёв П. С. Квадратичные булевы функции высокого порядка устойчивости // Математические вопросы кибернетики. Вып. 11. — М.: ФИЗМАТЛИТ, 2002. — С. 255–261. URL: http://library.keldysh.ru/mvk.asp?id=2002-255

КВАДРАТИЧНЫЕ БУЛЕВЫ ФУНКЦИИ ВЫСОКОГО ПОРЯДКА УСТОЙЧИВОСТИ

П. С. КОРОЛЁВ

(МОСКВА)

§ 1. Введение

Актуальной задачей в криптографии является построение таких генераторов псевдослучайных последовательностей из нулей и единиц, что по статистическому анализу исходящего сигнала невозможно получить никакой информации о первоначальном ключе.

Одно из решений этой задачи состоит во введении комбинирующей булевой функции $f(x_1, \ldots, x_n)$, которая, используя несколько псевдослучайных генераторов в качестве входов, преобразует их сигналы так, что частота появления на выходе нулей равна частоте появления на выходе единиц как у самой функции f, так и у ее подфункций от не менее чем $n-k$ переменных. Такие комбинирующие функции называются устойчивыми порядка k. Тривиальными устойчивыми функциями являются линейные комбинации входов. Отдельный интерес представляют простейшие нетривиальные устойчивые функции, а именно квадратичные, для которых алгебраическая степень каждой переменной равна двум.

В предлагаемой работе для квадратичных устойчивых функций от n переменных получена, во-первых, точная оценка максимального порядка устойчивости: $k < \lfloor \frac{n}{2} \rfloor$. Во-вторых, получен общий вид всех квадратичных $(n-1)$-устойчивых функций от $2n$ переменных:

$$f(x_1, x_2, \ldots, x_{2n}) = g(x_1 \oplus x_{n+1}, x_2 \oplus x_{n+2}, \ldots, x_n \oplus x_{2n}) \oplus x_1 \oplus x_2 \oplus \ldots \oplus x_n$$

с точностью до перестановки индексов переменных.

§ 2. Обозначения и основные определения

Основным пространством будет являться булев куб $\mathbb{F}_2^n$. Суммирование в нем обозначается $\oplus$. Под словом «функция» далее всегда надо понимать «булева функция».

Весом функции f называется количество наборов, на которых она принимает ненулевое значение:

$$\mathrm{wt}(f) = \sum_{x \in \mathbb{F}_2^n} f(x).$$

Подфункцией функции $f(x_1, \ldots, x_n)$ называется функция f', полученная из f подстановкой констант вместо некоторых переменных. Если вместо

© П. С. Королёв, 2002

переменных $x_{i_1}, \ldots, x_{i_k}$ подставили константы $\sigma_{i_1}, \ldots, \sigma_{i_k}$ соответственно, то полученная подфункция обозначается $f' = f^{\sigma_{i_1}, \ldots, \sigma_{i_k}}_{x_{i_1}, \ldots, x_{i_k}}$.

Функция f на $\mathbb{F}_2^n$ называется *уравновешенной*, если количество наборов, на которых она принимает значение 1, равно количеству наборов, на которых она принимает значение 0. Для такой функции $\mathrm{wt}(f) = 2^{n-1}$.

Функция $f(x_1, \ldots, x_n)$: $\mathbb{F}_2^n \to \mathbb{F}_2$ называется *корреляционно-иммунной порядка* k, $0 \leqslant k \leqslant n$, если для любой ее подфункции f' от $n-k$ переменных выполнено $\mathrm{wt}(f') = \mathrm{wt}(f)/2^k$.

Лемма 1. *Если функция f является корреляционно-иммунной порядка k, то она является корреляционно-иммунной любого меньшего порядка.*

Доказательство. Пусть f' — произвольная подфункция f от $n-k+1$ переменных и x_i — произвольная переменная функции f'. Тогда

$$f' = x_i (f')^1_{x_i} \oplus (x_i \oplus 1)(f')^0_{x_i}.$$

Поскольку f — корреляционно-иммунная порядка k, а $(f')^1_{x_i}$ и $(f')^0_{x_i}$ — ее подфункции от $n-k$ переменных, то

$$\mathrm{wt}(f') = \mathrm{wt}((f')^1_{x_i}) + \mathrm{wt}((f')^0_{x_i}) = \mathrm{wt}(f)/2^k + \mathrm{wt}(f)/2^k = \mathrm{wt}(f)/2^{k-1}.$$

Таким образом, f является корреляционно-иммунной порядка $k-1$ и любого меньшего порядка.

Функция f от n переменных называется *устойчивой порядка k* или *k-устойчивой*, если она является корреляционно-иммунной порядка k и уравновешенной. Множество k-устойчивых функций от n переменных будем обозначать $\mathbb{R}es(n, k)$. Максимальный порядок устойчивости функции будем обозначать $\mathbb{R}es\mathbb{O}rd(f)$. Если функция f не является уравновешенной, то будем считать $\mathbb{R}es\mathbb{O}rd(f) = -1$.

Каждая функция f на $\mathbb{F}_2^n$ однозначно представляется в виде полинома над $\mathbb{F}_2^n$, который называется *полиномом Жегалкина* функции f:

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

где A также функция над $\mathbb{F}_2^n$.

Алгебраической степенью переменной x_i функции $f(x_1, \ldots, x_n)$ называется максимальная степень одночлена, содержащего x_i в полиноме Жегалкина функции f. Обозначать мы ее будем $\deg(f, x_i)$.

Если $\deg(f, x_i) = 0$, то мы говорим, что переменная x_i входит *фиктивно*, если $\deg(f, x_i) = 1$, то x_i входит *линейно*, а если $\deg(f, x_i) = 2$, то x_i входит *квадратично*.

Алгебраической степенью функции f называется величина $\deg(f) = \max\limits_i \deg(f, x_i)$.

Функцию f будем называть *квадратичной*, если алгебраическая степень каждой переменной равна 2, т. е. $\deg(f, x_i) = 2$. Множество всех квадратичных функций будем обозначать $\mathbb{Q}uad$.

Запись

$$f(x_1, \ldots, x_n) \stackrel{\sigma}{=} g(x_1, \ldots, x_n)$$

будет означать, что функции f и g равны с точностью до перестановки индексов переменных.

Лемма 2. *Пусть $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_m) \oplus f(x_{m+1}, \ldots, x_n)$. Тогда*

$$\mathbb{R}es\mathbb{O}rd(f) = \mathbb{R}es\mathbb{O}rd(g) + \mathbb{R}es\mathbb{O}rd(h) + 1.$$

Доказательство. Для того, чтобы функция f была уравновешенной, достаточно, чтобы хотя бы одна из функций g и h была уравновешенной. Пусть уравновешенной является g. Тогда

$$\mathrm{wt}(f) = \sum_{\substack{y\in\mathbb{F}_2^m\\ z\in\mathbb{F}_2^{n-m}}} (g(y)\oplus h(z)) = \sum_{y,z} g(y)(h(z)\oplus 1) + \sum_{y,z}(g(y)\oplus 1)h(z) =$$
$$= \sum_z (h(z)\oplus 1)\sum_y g(y) + \sum_z h(z)\sum_y (g(y)\oplus 1) =$$
$$= \sum_z (h(z)\oplus 1)2^{m-1} + \sum_z h(z)2^{m-1} = 2^{n-1}.$$

Для того, чтобы функция f перестала быть уравновешенной, необходимо подставить в g не менее $\mathbb{R}es\mathbb{O}rd(g)+1$ констант вместо переменных, и в h не менее $\mathbb{R}es\mathbb{O}rd(h)+1$ констант. При этом если подставить чуть меньше констант, то функция f останется уравновешенной. Отсюда

$$\mathbb{R}es\mathbb{O}rd(f) = (\mathbb{R}es\mathbb{O}rd(g)+1) + (\mathbb{R}es\mathbb{O}rd(h)+1) - 1.$$

Лемма 3. *Пусть* $\deg(f)=2$, *тогда*

$$f(x_1,\ldots,x_n) \stackrel{\sigma}{=} g(x_1,\ldots,x_m)\oplus x_{m+1}\oplus\ldots\oplus x_{m+t},$$

где $g\in\mathbb{Q}uad$, *и*

$$\mathbb{R}es\mathbb{O}rd(f) = \mathbb{R}es\mathbb{O}rd(g) + t.$$

§ 3. Порядки устойчивости квадратичных функций

Лемма 4. *Для любой функции g на $\mathbb{F}_2^{n-1}$ функция*

$$f(x_1,x_2,x_3,\ldots,x_n) = g(x_1\oplus x_2, x_3,\ldots,x_n)\oplus x_1$$

является уравновешенной.

Доказательство. Разобьем все множество $\mathbb{F}_2^n$ на пары элементов (y',y''), таких, что y' и y'' отличаются только в первых двух компонентах. Тогда $f(y') = f(y'')\oplus 1$ и

$$\mathrm{wt}(f) = \sum_{(y',y'')} \bigl(f(y')+f(y'')\bigr) = 2^{n-1}.$$

Лемма 5. *Для любой функции $g(y_1,\ldots,y_m)$ на $\mathbb{F}_2^m$ функция*

$$f(x_1,\ldots,x_{2m}) = g(x_1\oplus x_{m+1}, x_2\oplus x_{m+2},\ldots,x_m\oplus x_{2m})\oplus x_1\oplus x_2\oplus\ldots\oplus x_m$$

является $(m-1)$-устойчивой.

Доказательство. Возьмем произвольную подфункцию f', полученную из f подстановкой $m-1$ констант. При этом найдется такое j, что ни вместо x_j, ни вместо x_{m+j} не подставили констант. Тогда f' имеет вид

$$f' = g'(\ldots, x_j\oplus x_{m+j},\ldots)\oplus x_j$$

и по лемме 1 является уравновешенной, следовательно, $f\in\mathbb{R}es(2m, m-1)$.

Теорема 1 [1]. *Пусть $f\in\mathbb{R}es(n, k=n-m)$, $m\geqslant 2$, $\deg(f,x_i)\geqslant 2$ для всех $i=1,\ldots,n$. Тогда*

$$n \leqslant (m-1)2^{\deg(f)-1}.$$

Теорема 2. *Квадратичные k-устойчивые функции от n переменных существуют только при $n \geqslant 3$, $k < \lfloor \frac{n}{2} \rfloor$.*

Доказательство. Подставляя в теорему 1 значение $\deg(f) = 2$, получаем $n \leqslant 2(n-k-1)$, т. е. $k \leqslant \frac{n}{2} - 1$.

При этом множества $\mathbb{R}es(2m, m-1) \cap \mathbb{Q}uad$ непусты при $m \geqslant 2$, и, взяв $f \in \mathbb{R}es(2m, m-1) \cap \mathbb{Q}uad$ и подставив одну константу, получим $f' \in \mathbb{R}es(2m-1, m-2) \cap \mathbb{Q}uad$. Устойчивых функций от 2 переменных нет. Следовательно, множества $\mathbb{R}es(n, k)$ непусты только при $n \geqslant 3$, $k < \lfloor \frac{n}{2} \rfloor$.

§ 4. Коэффициенты Уолша и автокорреляционные коэффициенты

Для булевых функций хорошо известны такие характеристики, как коэффициенты Уолша и автокорреляционные коэффициенты, которые оказываются очень полезными при исследовании устойчивых функций. В этом параграфе приводятся основные факты, известные про коэффициенты Уолша, автокорреляционные коэффициенты и связь между ними.

Коэффициентом Уолша $\widehat{\chi_f}(u)$, $u \in \mathbb{F}_2^n$ называется число

$$\widehat{\chi_f}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + <u, x>},$$

где $<u, x> = \sum_i u_i x_i$ — скалярное произведение.

Теорема 3 (Равенство Парсеваля [2]). *Коэффициенты Уолша удовлетворяют соотношению*

$$\sum_{u \in \mathbb{F}_2^n} \widehat{\chi_f}^2(u) = 2^{2n}.$$

Теорема 4 (Тождество Саркара [2, 4]). *Для любого $w \in \mathbb{F}_2^n$ выполнено*

$$\sum_{\substack{u \in \mathbb{F}_2^n \\ u \preceq w}} \widehat{\chi_f}(u) = 2^n - 2^{|w|+1} \mathrm{wt}(f_w),$$

где f_w — функция, полученная из f подстановкой 0 вместо x_i для всех таких i, что $w_i = 1$.

Теорема 5 [2, 3]. *Функция f на $\mathbb{F}_2^n$ является корреляционно-иммунной порядка k тогда и только тогда, когда $\widehat{\chi_f}(u) = 0$ для всех наборов $u \in \mathbb{F}_2^n$, для которых $1 \leqslant |u| \leqslant k$.*

Теорема 6 [1]. *Для любой функции f на $\mathbb{F}_2^n$, такой, что* $\deg(f, x_i) \geqslant 2$, *выполнено*

$$\sum_{\substack{u \in \mathbb{F}_2^n \\ u_i = 0}} \widehat{\chi_f}^2(u) \geqslant 2^{2n - \deg(f) + 1}.$$

Автокорреляционным коэффициентом функции f на векторе u называется число

$$\Delta_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus u)}.$$

Теорема 7 [2]. $\Delta_f(u) = -2^n + 2^{1-n} \sum_{\substack{x \in \mathbb{F}_2^n \\ <x, u> \equiv 0 \pmod 2}} \widehat{\chi_f}^2(x).$

§ 5. Вид квадратичных функций максимального порядка устойчивости

В этом параграфе, доказав некоторые свойства коэффициентов Уолша и автокорреляционных коэффициентов, мы покажем, что все квадратичные функции от четного числа переменных максимального порядка устойчивости имеют вид

$$g(x_1 \oplus x_{n+1}, \ldots, x_n \oplus x_{2n}) \oplus x_1 \oplus \ldots \oplus x_n, \qquad g \in \mathbb{Q}uad,$$

с точностью до перестановки индексов переменных.

Теорема 8. *Пусть $f \in \mathbb{R}es(N, k) \cap \mathbb{Q}uad$, $N = 2n$, $k = n-1$. Тогда $\widehat{\chi_f}(u) \neq 0$ только при $|u| = n$.*

Доказательство. По теореме 5 получаем, что $\widehat{\chi_f}(u) \neq 0$ только при $|u| \geqslant k+1 = n$.

Выпишем матрицу M, в которой каждая строчка $u \in \mathbb{F}_2^N$ будет встречаться ровно $\widehat{\chi_f}^2(u)$ раз. Согласно равенству Парсеваля, в ней будет $2^{2N} = 2^{4n}$ строчек. В каждой строчке не более n нулей, поэтому во всей матрице не более $n2^{4n}$ нулей.

С другой стороны, по теореме 6 в каждом столбце не менее $2^{2N - \deg(f) + 1} = 2^{4n-1}$ нулей, т. е. во всей матрице не менее $2n2^{4n-1} = n2^{4n}$ нулей.

В результате получаем, что во всей матрице ровно $n2^{4n}$ нулей, и в каждой строчке ровно n нулей и n единиц.

Лемма 6. *Пусть $e_{pq} = (0, \ldots, 0, \underset{p}{1}, 0, \ldots, 0, \underset{q}{1}, 0, \ldots, 0) \in \mathbb{F}_2^n$ и $f \in \mathbb{Q}uad$. Тогда $\Delta_f(e_{pq}) \in \{0, \pm 2^n\}$ и справедливы следующие утверждения:*

$$\Delta_f(e_{pq}) = 2^n \iff f(x) = g(\ldots, x_p \oplus x_q, \ldots),\ \ g \in \mathbb{Q}uad,$$
$$\Delta_f(e_{pq}) = -2^n \iff f(x) = g(\ldots, x_p \oplus x_q, \ldots) \oplus x_p,\ \ g \in \mathbb{Q}uad.$$

Доказательство. Представим функцию f в виде

$$f(x) = \bigoplus_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j \oplus \bigoplus_{1 \leqslant i \leqslant n} b_i x_i \oplus c,$$

где $a_{ij} = a_{ji}$ и $a_{ii} = 0$.

Тогда $\Delta_f(e_{pq}) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{\bigoplus\limits_{i \neq p, q} (a_{pi} \oplus a_{qi}) x_i \oplus a_{pq}(x_p \oplus x_q \oplus 1) \oplus b_p \oplus b_q}$.

Если в выражении $\bigoplus\limits_{i \neq p, q} (a_{pi} \oplus a_{qi}) x_i \oplus a_{pq}(x_p \oplus x_q \oplus 1) \oplus b_p \oplus b_q$ содержится хотя бы один линейный член x_k, то имеем $\Delta_f(e_{pq}) = 0$. Отсутствие линейных членов означает, что для всех i выполнено $a_{pi} = a_{qi}$. Тогда $\Delta_f(e_{pq}) = 2^n(-1)^{b_p \oplus b_q}$ и функцию f можно записать в виде

$$f(x) = \bigoplus_{\substack{i < j \\ i, j \neq p, q}} a_{ij} x_i x_j \oplus \bigoplus_{i \neq p, q} b_i x_i \oplus c \oplus (x_p \oplus x_q) \Bigg(\bigoplus_{i \neq p, q} a_{pi} x_i \oplus b_q \Bigg) \oplus (b_p \oplus b_q) x_p,$$

что и доказывает лемму.

Теорема 9. *Пусть $f(x_1, \ldots, x_{2n}) \in \mathbb{Q}uad$. Тогда*

$$\sum_{1 \leqslant p < q \leqslant 2n} \Delta_f(e_{pq}) = -n2^{2n} \iff f \overset{\sigma}{=} g(x_1 \oplus x_{n+1}, \ldots, x_n \oplus x_{2n}) \oplus x_1 \oplus \ldots \oplus x_n,$$

где $g(y_1, \ldots, y_n) \in \mathbb{Q}uad$.

Доказательство. Возьмем произвольную функцию f на $\mathbb{F}_2^{2n}$. На множестве вершин $V=\{1,\ldots,2n\}$ построим граф $G=(V,E)$ по следующему принципу:

$$(p,q)\in E \overset{\sigma}{\Longleftrightarrow} \Delta_f(e_{pq})\neq 0.$$

Каждая компонента связности $H^t=(V^t,E^t)$ этого графа будет являться полным графом, так как по лемме 6 для всех i имеем

$$(p,q)\in E^t \Longleftrightarrow a_{pi}=a_{qi}.$$

Разобьем V^t на $V_0^t\sqcup V_1^t$ так, что $i\in V_{b_i}^t$ и обозначим $v_0^t:=|V_0^t|$, $v_1^t:=|V_1^t|$.

Тогда для $\{p,q\}\subset V_0^t$ или $\{p,q\}\subset V_1^t$ имеем $\Delta_f(e_{pq})=2^{2n}$, а для $p\in V_0^t$, $q\in V_1^t$ имеем $\Delta_f(e_{pq})=-2^{2n}$.

Оценим сумму

$$\sum_{(p,q)\in E^t}\Delta_f(e_{pq})=2^{2n}\left(\frac{v_0^t(v_0^t-1)}{2}+\frac{v_1^t(v_1^t-1)}{2}\right)-2^{2n}v_0^tv_1^t=$$
$$=2^{2n-1}((v_0^t-v_1^t)^2-(v_0^t+v_1^t))\geqslant -2^{2n-1}|V^t|,$$

причем равенство достигается только при $v_0^t=v_1^t=v^t$.

Следовательно,

$$\sum_{1\leqslant p<q\leqslant 2n}\Delta_f(e_{pq})\geqslant -2^{2n-1}\sum_t|V^t|=-n2^{2n},$$

причем равенство для всех t достигается только при $v_0^t=v_1^t$.

Таким образом, если у нас имеется равенство $\sum\Delta_f(e_{pq})=-n2^{2n}$, то множество всех переменных можно разбить на пары (i_k^t,j_k^t), где $i_k^t\in V_0^t$, $j_k^t\in V_1^t$, и тогда функция будет представима в виде

$$f(x_1,\ldots,x_{2n})=g(x_{i_1^1}\oplus x_{j_1^1},\ldots,x_{i_v^1}\oplus x_{j_v^1},\ldots)\oplus x_{i_1^1}\oplus\ldots\oplus x_{i_v^1}\oplus\ldots,$$

т. е. в нужном нам виде.

Если же функция уже имеет вид

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

то при построении графа G и разбиении его на компоненты будет при всех i, $i\leqslant n$, выполнено $i\in V_{b_i}^t$ и $i+n\in V_{b_i\oplus 1}^t$, откуда следует, что $v_0^t=v_1^t$ для всех t.

Теорема 10. *Пусть* $f(x_1,\ldots,x_{2n})\in\mathbb{R}es(2n,n-1)\cap\mathbb{Q}uad$. *Тогда существует такая функция* $g(y_1,\ldots,y_n)\in\mathbb{Q}uad$, *что*

$$f(x_1,\ldots,x_{2n})\overset{\sigma}{=}g(x_1\oplus x_{n+1},\ldots,x_n\oplus x_{2n})\oplus x_1\oplus\ldots\oplus x_n.$$

Доказательство. Подставим выражение из теоремы 7 в теорему 9:

$$\sum_{1\leqslant p<q\leqslant 2n}\Delta_f(e_{pq})=\sum_{p<q}\left(-2^{2n}+2^{1-2n}\sum_{\substack{x\in\mathbb{F}_2^{2n}\\ <x,e_{pq}>\equiv 0\pmod 2}}\widehat{\chi_f}^2(x)\right)=$$
$$=-n(2n-1)2^{2n}+2^{1-2n}\sum_{p<q}\sum_{x_p=x_q}\widehat{\chi_f}^2(x).$$

По теореме 8 при $|x| \neq n$ имеем $\widehat{\chi_f}(x) = 0$, следовательно,

$$\sum_{p<q} \sum_{x_p = x_q} \widehat{\chi_f}^2(x) = \sum_{p<q} \sum_{\substack{x_p = x_q \\ |x| = n}} \widehat{\chi_f}^2(x) = \sum_{|x|=n} \left(\widehat{\chi_f}^2(x) \sum_{\substack{p<q \\ x_p = x_q}} 1 \right) = \\ = (n^2 - n) \sum_{|x|=n} \widehat{\chi_f}^2(x) = (n^2 - n)2^{4n}.$$

Поэтому

$$\sum_{1 \leqslant p < q \leqslant 2n} \Delta_f(e_{pq}) = -n(2n-1)2^{2n} + 2^{1-2n}(n^2-n)2^{4n} = -n2^{2n}.$$

Отсюда по теореме 9 получаем, что все функции из $\mathbb{R}es(2n, n-1) \cap \cap \mathbb{Q}uad$ имеют заданный вид.

СПИСОК ЛИТЕРАТУРЫ

1. Таранников Ю. В. Об автокорреляционных свойствах корреляционно-иммунных функций // Материалы VII Международного семинара «Дискретная математика и ее приложения» (29 января — 2 февраля 2001 г.), М.: Из-во центра прикладных исследований при механико-мататематическом факультете МГУ, 2001. — Ч. III. — С. 331–333.
2. Таранников Ю. В. Числовые характеристики булевых функций // Дискретная математика и ее приложения. Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. М.: Из-во центра прикладных исследований при механико-мататематическом факультете МГУ, 2001. — Ч. I. — С. 129–144.
3. Guo-Zhen Xiao, Massey J. A spectral characterization of correleation-immune combining functions // IEEE Transactions on Information Theory. — V. 34, № 3, May 1988. — P. 569–571.
4. Sarkar P. Spectral domain analysis of correlation immune and resilient Boolean functions // Cryptology e-print archive (http://eprint.iacr.org/), Report 2000/049, September 2000.

Поступило в редакцию 15 I 2002