

ПОСТРОЕНИЕ КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДА ГРАДИЕНТНОГО СПУСКА

А.А.Кузнецов, Ю.А.Избенко, И. Московченко

Исследуются методы построения криптографических булевых функций. Теоретически обосновывается возможность формирования сбалансированных криптографических булевых функций с высокими показателями нелинейности и алгебраической степени, удовлетворяющих строгому лавинному критерию.

1. Постановка проблемы в общем виде и анализ литературы. Безопасность информации в современных АСУ обеспечивается механизмами криптографического преобразования данных [1,2]. Построение эффективных криптоалгоритмов описывается в терминах булевой алгебры криптографическими булевыми функциями [3].

Как показывает анализ открытой литературы [4-7], известные методы построения криптографических функций с требуемыми показателями стойкости можно условно разделить на три класса: методы случайной генерации; алгебраические методы; эвристические методы.

К первому классу относятся методы, основанные на процедурах случайной генерации с последующим отбором функций, удовлетворяющих заданным показателям [4]. Их достоинство состоит в очевидной простоте практической реализации. Существенным недостатком является быстрый рост вычислительной сложности – поиск функций от восьми и более переменных вычислительно недоступен.

Ко второму классу [6-9] относятся методы, использующие итеративные процедуры построения, основанные на алгоритмах модификации булевых функций, удовлетворяющих определенным требованиям (например, бент-функций). Достоинством алгебраических методов является низкая вычислительная сложность. Их основным недостатком является снижение в процессе итеративного поиска некоторых других показателей стойкости, например, показателя нелинейности [9].

В основе эвристических методов [10-14] лежат интуитивные подходы к построению криптографических булевых функций. Большинство известных эвристических подходов обладает всеми преимуществами процедур случайного поиска и алгебраических методов [13]. Действительно, все эвристические методы позволяют конструировать функции с нелинейностью, максимально приближенной к верхней границе. Так, в классе эвристических методов генетические методы [11] и методы имитации отжига [12] позволяют строить функции с наивысшими показателями стойкости. Ограничением на практическое применение данных методов может служить только их высокая вычислительная сложность. Следовательно, актуальной научно-технической задачей является разработка метода построе-

ния криптографических булевых функций, обладающего низкой вычислительной сложностью на основе дальнейшего совершенствования эвристических методов. Наибольшим потенциалом обладает метод градиентного подъема как способ, являющийся базовым для всех остальных методов данного класса [10,14]. Целью статьи является обоснование подхода к построению криптографических булевых функций на основе градиентного поиска.

2. Обоснование подхода к построению криптографических булевых функций на основе градиентного поиска. Рассмотрим основные положения булевой алгебры применительно к построению криптографических булевых функций, введем основные определения и обозначения [3].

Булевой функцией f от n переменных является функция [3], осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов $x = (x_1, \dots, x_n)$ длины n в поле $GF(2)$. Обычно булевы функции представляются в алгебраической нормальной форме и рассматриваются как сумма произведений составляющих координат. Поле $GF(2^n)$ состоит из 2^n векторов α_i : $\alpha_0 = (0, \dots, 0, 0)$, $\alpha_1 = (0, \dots, 0, 1), \dots, \alpha_{2^n-1} = (1, \dots, 1, 1)$, $\alpha_i \in V_n$, где V_n – векторное пространство в $GF(2^n)$. *Последовательностью функции* f называется $(1,-1)$ -последовательность, определенная как $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \dots, (-1)^{f(\alpha_{2^n-1})})$. *Таблицей истинности функции* f называется $(0,1)$ -последовательность, определенная как $(f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{2^n-1}))$. Последовательность функции f является *сбалансированной*, если ее $(0,1)$ -последовательность $((1,-1)$ -последовательность) содержит одинаковое количество нулей и единиц (единиц и минус единиц). Функция f является сбалансированной, если сбалансирована ее последовательность. *Весом Хэмминга* вектора α ($(0,1)$ -последовательности α), обозначаемым как $W(\alpha)$, является количество единиц в векторе (последовательности). *Расстоянием Хэмминга* $d(f,g)$ между последовательностями двух функций f и g является количество позиций, в которых различны последовательности этих функций. *Нелинейность* N_S преобразования – минимальное расстояние Хэмминга между выходной последовательностью S и всеми выходными последовательностями аффинных функций над некоторым полем:

$$N_S = \min \{d(S, \varphi)\},$$

где φ – множество аффинных функций.

Нелинейность функции N_f – минимальное расстояние Хэмминга N_f между функцией f и всеми аффинными функциями над $GF(2^n)$ [3].

$$N_f = \min \{d(f, \varphi)\},$$

где φ – множество аффинных функций.

При разработке предлагаемого подхода в качестве основы взят эвристический метод градиентного подъема В.Миллана, Э.Кларка, Э.Доусона, 1997 г [10] (далее – метод градиентного подъема). Данный метод основан на преобразовании выходных последовательностей нелинейных функций.

Суть метода градиентного подъема состоит в повышении нелинейности произвольной булевой функции путем комплементации некоторой позиции в таблице истинности данной функции. Каждая позиция таблицы истинности соответствует уникальным входным данным функции. Метод позволяет создать полный список/перечень таких входных данных функции, что комплементация любой соответствующей данному входу выходной позиции в таблице истинности будет увеличивать нелинейность данной функции. Список/перечень таких позиций в таблице истинности обозначим как $1 - Improvement Set$ функции $f(x)$, или $1 - IS_f$.

Определение 1 [10]. Пусть $g(x) = f(x) \oplus 1$ для $x = x_a$ и $g(x) = f(x)$ для всех остальных x . Если $N_g > N_f$ то $x_a \in 1 - IS_f$.

Возможны случаи, когда данное множество будет пустым, и тогда функция $f(x)$ обозначается как функция с максимальной нелинейностью и техника, используемая в описываемом методе, является не применимой. Поскольку все бент-функции являются глобально-максимальными, их $1 - Improvement Set$ множество является пустым. Существует также субоптимальный локальный максимум, который может быть найден посредством использования методов градиентного подъема. Решение данной задачи является вычислительно трудоемким, поскольку используется принцип инвертирования позиций таблицы истинности функции случайным образом, нахождения новых значений WHT (Walsh – Hadamar transform – преобразование Уолша-Адамара) и определения множества $1 - IS_f$. В [10] представлен быстрый систематический метод определения множества $1 - IS_f$ заданной булевой функции путем использования ее таблицы истинности и преобразований Уолша-Адамара. Ниже представлены определения, на которых базируется метод определения того, является ли вход x элементом множества $1 - IS_f$.

Для нахождения множества $1 - IS_f$ заданной булевой функции необходимо сначала определить значения коэффициентов преобразования Уолша-Адамара, которые соответствовали бы величинам, близким к абсолютному значению максимального коэффициента, WH_{max} .

Определение 2. Пусть $f(x)$ является булевой функцией с преобразованием Уолша-Адамара $F(w)$, где WH_{max} обозначает максимальное абсолютное значение $F(w)$. Тогда будут существовать одна или более линейных функций $L_w(x)$, имеющих минимальное расстояние до функции $f(x)$, и для данных w будет справедливо равенство $|F(w)| = WH_{max}$.

Определяется следующее множество:

$$W_1^+ = \{ w: F(w) = WH_{max} \} \text{ и}$$

$$W_1^- = \{ w: F(w) = - WH_{max} \}.$$

Определяются множества w для которых WHT приближены к максимуму:

$$W_2^+ = \{ w: F(w) = WH_{max} - 2 \},$$

$$W_2^- = \{ w: F(w) = - (WH_{max} - 2) \},$$

$$W_3^+ = \{ w: F(w) = WH_{max} - 4 \} \text{ и}$$

$$W_3^- = \{ w: F(w) = -(WH_{max} - 4) \}.$$

Когда таблица истинности изменяется ровно в одном месте, все *WHT* значения изменяются на +2 или -2. Из этого следует, что для увеличения нелинейности все *WHT* значения в множестве W_1^+ должны быть изменены на -2, все *WHT* значения в множестве W_1^- должны быть изменены на 2 а также все *WHT* значения в множестве W_2^+ должны быть изменены на -2, все *WHT* значения в множестве W_2^- должны быть изменены на 2. Если первые два условия являются очевидными, то следующие два условия требуются для того, чтобы все другие значения $|F(w)|$ оставались меньшими, чем WH_{max} . Данные условия могут быть представлены в виде простых тестов.

Теорема 1 [10]. Пусть дана некоторая булева функция $f(x)$ с *WHT* $F(w)$, и определены множества $W^+ = W_1^+ \cup W_2^+$ и $W^- = W_1^- \cup W_2^-$. Тогда для некоторого входа x существует элемент из *Improvement Set* и выполняются следующие два условия:

- (i) $f(x) = L_w(x)$ для всех $w \in W^+$, и
- (ii) $f(x) \neq L_w(x)$ для всех $w \in W^-$.

Если функция $f(x)$ не сбалансирована, понижение несбалансированности может быть достигнуто использованием дополнительного ограничения:

- (iii) если $F(0) > 0$, $f(x) = 0$, иначе $f(x) = 1$.

Рассмотрим следующий *пример*. Пусть дана таблица истинности (см. столбец 2 таблицы 1) некоторой булевой функции, а также соответствующие значения преобразования Уолша-Адамара *WHT* (см. столбец 3 таблицы 1). Необходимо, если это возможно, повысить нелинейность заданной последовательности.

Таблица 1. – Демонстрация метода градиентного подъема

x/w	$f(x)$	$F(w)$	$L_{0101}(x)$	$L_{1110}(x)$	$x \in 1 - IS_f$
0000	0	0	0	0	√
0001	1	4	1	0	
0010	0	0	0	1	
0011	1	4	1	1	√
0100	1	4	1	1	√
0101	1	8	0	1	
0110	1	-4	1	0	
0111	0	0	0	0	√
1000	0	-4	0	1	
1001	1	0	1	1	√
1010	0	-4	0	0	√
1011	0	0	1	0	
1100	0	0	1	0	
1101	0	4	0	0	√
1110	1	8	1	1	√

1111	1	-4	0	1	
------	---	----	---	---	--

Как видно из приведенной таблицы, максимальное значение $WH_{max} = 8$ достижимо для $w = 0101$ и $w = 1110$. Значений преобразований, равных $WH_{max} - 2 = 6$, не существует, поэтому $W_1^+ = \{0101, 1110\}$ и $W_1^- = W_2^+ = W_2^- = \phi$. Тогда согласно теореме 1 значениями-кандидатами для множества $1 - IS_f$ будут такие значения x , для которых $L_{0101}(x) = L_{1110}(x) = f(x)$. Таким образом, $1 - IS_f = \{0000, 0011, 0100, 0111, 1001, 1010, 1101, 1110\}$ и комплементация любого бита в соответствующей позиции таблицы истинности (столбец 2) повлечет за собой увеличение нелинейности с $N_f = 0,5(2^n - WH_{max}) = 4$ до $N_f = 5$.

Таким образом, теорема 1 дает конструктивный механизм повышения нелинейности исходной булевой функции посредством итеративной пошаговой комплементации позиций в таблице истинности. Кроме того, замечание (iii) дает механизм понижения несбалансированности рассматриваемой последовательности. Как видно из приведенного примера использование результатов теоремы 1 позволяет за конечное число шагов повысить нелинейность булевой функции при сохранении ее сбалансированности.

Обсуждая приведенный метод, можно отметить, что полученные последовательности обладают более высокой нелинейностью, чем последовательности, генерируемые функциями, построенными в соответствии с алгебраическими методами, и, наравне с другими эвристическими методами, рассмотренный подход гарантирует достижение нелинейности, наиболее близкой к верхней границе нелинейности. В то же время данный метод обладает меньшей вычислительной сложностью по сравнению с другими эвристическими методами и является их составной частью как метод, позволяющий добиваться высокой нелинейности.

Анализ эвристических методов показывает, что основные вычислительные затраты происходят за счет повторяющихся итеративных процедур, призванных повысить определенные показатели стойкости. Соответственно, понизить данные вычислительные затраты можно за счет уменьшения количества соответствующих процедур. Как следствие, это подразумевает что исходными данными для этих методов должны быть функции, уже имеющие достаточно высокие показатели стойкости.

Однако все эвристические методы предполагают, что исходными данными являются произвольно выбранные функции, другими словами, это в лучшем случае случайным образом сбалансированные нелинейные последовательности. Именно за счет многошаговой процедуры повышения нелинейности эвристические методы становятся столь трудоемкими, не гарантируя при этом успешной модификации каждой входной последовательности.

Эффективным путем решения данной проблемы, с нашей точки зрения, является использование в качестве входных данных не последовательностей, сгенерированных случайным образом, а бент – последовательностей (бент - функций), что позволит качественным образом понизить

вычислительную сложность данных методов и добиться высоких показателей стойкости.

Для аргументации изложенного используем следующие рассуждения. Известно, что стойкость преобразований в симметричных схемах преобразования информации определяется, прежде всего, степенью нелинейности преобразований. При этом верхней границы нелинейности N_f над $GF(2^n)$ могут достигать только бент-функции [4]. Данные функции обладают рядом привлекательных свойств [4]: бент-функции обладают максимальной нелинейностью; бент-функции удовлетворяют критерию распространения $KP(n)$; бент-функции имеют нулевые значения автокорреляции. Так, для бент-функций справедливы следующие выражения [4]:

$$d(f_0, A) = N_f = 2^{n-1} - 2^{n/2-1}, \quad (1)$$

$$d(f_0, \mathcal{L}) = 2^{n-2}, \quad (2)$$

$$AC(f) = 0. \quad (3)$$

где A и \mathcal{L} - множество аффинных функций и линейных структур соответственно.

Однако использованию бент-функций в чистом виде препятствует тот факт, что их последовательности не сбалансированы, что делает их уязвимыми к статистическому анализу [4]:

$$|\{x \mid f(x) = 0\}| \neq |\{x \mid f(x) = 1\}| \neq 2^{n-1}.$$

Поскольку бент-функции обладают тремя максимально достижимыми показателями стойкости, представляется целесообразным найти способы преобразования бент-последовательностей в сбалансированные последовательности с минимально возможными потерями относительно других показателей.

Утверждение 1 [4]. Пусть задана бент-последовательность длины 2^n , содержащая $2^{n-1} + 2^{n/2-1}$ единиц и $2^{n-1} - 2^{n/2-1}$ нулей, либо наоборот. Тогда комплементарное дополнение $2^{n/2-1}$ позиций в бент-последовательности приводит к сбалансированной функции над V_n , имеющей нелинейность по крайней мере

$$N_f \leq 2^{n-1} - 2^{n/2}. \quad (4)$$

Отметим, что данная нелинейность является удовлетворительной, однако предложенный способ не предоставляет эффективного инструментария, использование которого обеспечивало бы не только получение сбалансированных последовательностей, но и последовательностей, нелинейность которых была бы максимально приближенной к теоретически достижимой; сама по себе сбалансированность еще не свидетельствует о том, что и другие показатели стойкости будут высокими.

Концепция построения нашего метода базируется на развитии идей, предложенных в [4] и [10]. В качестве входных данных рассматриваются бент-последовательности, обладающие заведомо привлекательными криптографическими свойствами. Для преобразования бент-последовательностей в сбалансированные последовательности используется идея Майера-Штаффельбаха [4], согласно которой необходимо комплементировать $2^{n/2-1}$ позиций в бент-последовательности. В качестве инст-

рументария, позволяющего эффективно осуществлять данную комплементацию, используется идея Миллана-Кларка [10]. Основной отличительной чертой предложенного метода от метода Миллана-Кларка (метода градиентного подъема) является то, что он позволяет не повышать, а понижать нелинейность функций, обладающих максимальной нелинейностью. Целью метода является минимально-возможное понижение нелинейности при каждой из $2^{n/2-1}$ обязательных комплементаций последовательности. Понижение нелинейности функции, заведомо имеющие высокие показатели стойкости, путем приведения ее к сбалансированному виду за счет пошагового градиентного спуска позволяет при минимальных потерях нелинейности получить криптографически стойкую функцию с высокими показателями стойкости.

Теорема 1. Булева функция, соответствующая последовательности, образованной комплементарным дополнением $2^{n/2-1}$ позиций в бент-последовательности над векторным пространством V_n является сбалансированной криптографической функцией с показателем нелинейности, удовлетворяющем выражению (4).

Доказательство. В соответствии с утверждением 1 последовательность, образованная комплементарным дополнением $2^{n/2-1}$ позиций в бент-последовательности над векторным пространством V_n является сбалансированной последовательностью с показателем нелинейности, удовлетворяющей выражению (4). В соответствии с определением нелинейность булевой функции определяется нелинейностью соответствующей последовательности и наоборот. Следовательно, булева функция, соответствующая последовательности, образованной комплементарным дополнением $2^{n/2-1}$ позиций в бент-последовательности является криптографической сбалансированной функцией с показателем нелинейности, удовлетворяющей (4).

Теорема 1 дает конструктивный механизм определения криптографических булевых функций путем понижения степени нелинейности бент-последовательности для приведения ее к сбалансированному виду. Совокупность выполняемых процедур и операций в дальнейшем будем называть *методом градиентного спуска*.

Выходными данными этапа приведения функции к сбалансированному виду являются высоконелинейные сбалансированные последовательности. В связи с этим при наличии высоко нелинейных последовательностей $\xi = \varepsilon_0 \varepsilon_1 \dots \varepsilon_{2^n-1}$ где n – размерность векторного пространства, представляет интерес восстановление внешнего вида функции, сгенерировавшей заданную последовательность, с целью обсуждения других показателей стойкости и, в случае необходимости, последующей модификации функции с целью улучшения ее стойкости, а также возможности отбора функций с наилучшими показателями стойкости.

В рамках предложенного метода выходные данные этапа приведения функции к сбалансированному виду приводятся к алгебраической нормальной форме способом, указанным в [16], после чего полученные функ-

ции преобразуются функции, удовлетворяющие критерию распространения посредством способа, указанного в [1].

Так, в [16] представлен способ восстановления алгебраической нормальной формы функции по её выходной последовательности ξ . Данный способ основан на использовании следующей леммы.

Лемма 1 [16]. Пусть ξ – последовательность некоторой функции f над V_n . Тогда существуют процедуры восстановления алгебраической нормальной формы функции

$$f(x_1, \dots, x_n) = a_0 \oplus \bigoplus_{i=1}^n a_i x_i \oplus \bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n$$

по известной последовательности $\xi = \varepsilon_0 \varepsilon_1 \dots \varepsilon_{2^n-1}$.

Таким образом, использование леммы 1 позволит нам, при наличии некоторых высоко нелинейных последовательностей, восстанавливать алгебраически нормальные формы булевых функций, полученных в процессе применения предложенного метода. Наличие алгебраических нормальных форм позволит, в свою очередь, обсуждать такие показатели стойкости, как алгебраическая степень и критерий распространения (строгий лавинный критерий).

Далее, для получения функций, удовлетворяющих критерию распространения целесообразным представляется использование следующих леммы и теоремы.

Лемма 2 [17]. Сбалансированность, нелинейность и количество векторов, относительно которых функция удовлетворяет критерию распространения, являются инвариантными относительно аффинных преобразований координат функции.

Теорема 2 [17]. Пусть f является функцией над V_n и A является несингулярной матрицей порядка n над $GF(2)$. Если $f(x) \oplus f(x \oplus \gamma)$ является сбалансированной для каждой строки γ матрицы A , то $\psi(x) = f(xA)$ удовлетворяет строгому лавинному критерию.

Таким образом, лемма 2 и теорема 2 свидетельствуют о том, что при наличии некоторой нелинейной булевой функции возможна модификация данной функции путем аффинных преобразований, результатом которых, при фиксированной нелинейности, сбалансированности и количестве векторов, удовлетворяющих критерию распространения, будет являться функция, удовлетворяющая строгому лавинному критерию.

На основании изложенных теорем и лемм сформулируем следующую теорему.

Теорема 4. Функции, построенные на основе использования метода градиентного спуска с последующим применением процедур восстановления алгебраической нормальной формы булевой функции и аффинных преобразований, являются сбалансированными, обладают нелинейностью $N_f \geq 2^{n-1} - 2^{n/2}$, удовлетворяют строгому лавинному критерию и имеют высокую алгебраическую степень, равную $deg(f) \leq n - 1$, где n – размерность векторного пространства.

Доказательство. В соответствии с теоремой 1 булевы функции, полученные в результате выполнения градиентного спуска являются сбалансированными и имеют нелинейность, удовлетворяющую соотношению (2.4). Конструктивность процедуры восстановления алгебраической нормальной формы функции задается леммой 1, при этом степень функции, соответствующая модифицированной бент-последовательности удовлетворяет соотношению $deg(f) \leq n - 1$, где n – размерность векторного пространства. Лемма 2 устанавливает инвариантность нелинейности относительно аффинных преобразований, а теорема 2 гарантирует при этом приведение функции к виду, удовлетворяющему строгому лавинному критерию. Следовательно, функции, построенные на основе использования метода градиентного спуска с последующим применением процедур восстановления алгебраической нормальной формы булевой функции и соответствующих аффинных преобразований помимо сбалансированности и высокой нелинейности будут удовлетворять строгому лавинному критерию, что и завершает доказательство.

3. Выводы. Таким образом, теоретически обоснована возможность формирования сбалансированных криптографических булевых функций с высокими показателями нелинейности и алгебраической степени, удовлетворяющих строгому лавинному критерию. Сформулирована и доказана теорема 4, которая устанавливает параметры криптографических булевых функций, формируемых в результате предлагаемого подхода. Важным направлением дальнейших исследований является разработка практических алгоритмов реализующих предложенный подход.

ЛИТЕРАТУРА

1. Барсуков В.С., Дворянкин С.В., Шеремет И.И. Технологии электронных коммуникаций: В 20 т. Т.20: Безопасность связи в каналах телекоммуникаций – М.: Электронные знания, 1992. – 122 с.
2. Захист інформації в комп'ютерних системах від несанкціонованого доступу. / За ред. С.Г. Лаптева. – К., 2001. – 321 с.
3. Горбенко И.Д., Потий А.В., Избенко Ю.А. Исследование аналитических и статистических свойств булевых функций криптоалгоритма Rijndael (FIPS 197). Радиотехника. Всеукраинский межведомственный научно-технический сборник. - 2004. - № 126. - С. 132 - 138.
4. W.Maier, O.Staffelbach. Nonlinearity criteria for cryptographic functions. In Advances in Cryptology – EUROCRYPT'89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, pp.549-562,1990.
5. Кузнецов А.А., Избенко Ю.А., Юкальчук А.А. Анализ известных методов построения высоко нелинейных булевых функций // Вісник НТУ "ХПІ". Збірник наукових праць.- Харків: НТУ "ХПІ". – 2004. - №18. –С. 91-96.
6. S.Maitra, E.Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. Accepted in SETA, May, 2001, Norway.

7. E.Pasalic, T.Johansson. Further Results on the Relation Between Nonlinearity and Resiliency for BF. *IEEE Trans. on Information Theory*, Vol 48, No. 7, July 2002, 1825-1834
8. E.Pasalic, T.Johansson, S.Maitra, P.Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds of nonlinearity. In Workshop of Coding and Cryptography, Electronic Notes in Discrete Mathematics. Elsevier, January 2001.
9. S. Maity and T. Johansson. Construction of Cryptographically Important Boolean Functions. In INDOCRYPT 2002, Volume 2551 in Lecture Notes in Computer Science, pages 234–245, Springer Verlag, 2002.
10. W. Millan, A. Clark and E. Dawson, "Smart Hill Climbing Finds Better Boolean Functions", Workshop on Selected Areas in Cryptography 1997 (SAC'97), page 50, Workshop Record.
11. W. Millan, A. Clark and E. Dawson. An effective genetic algorithm for finding highly nonlinear Boolean functions. In First International Conference on Information and Communications Security, number 1334 in Lecture Notes in Computer Science, pages 149–158. Springer Verlag, 1997.
12. J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan, "Evolving of Boolean functions satisfying multiple criteria", proceedings of INDOCRYPT'02, LNCS vol 2551, pages 246-259, Springer, 2002.
13. W. Millan, A. Clark and E. Dawson. Heuristic Design of Cryptographically Strong Balanced Boolean Functions. In Advances in Cryptology EUROCRYPT'98, pages 489–499. Springer Verlag LNCS 1403, 1998.
14. W. Millan, A. Clark and E. Dawson. Boolean function design using hill climbing methods. In 4th Australasian Conference on Information, Security and Privacy, number 1587 in Lecture Notes in Computer Science, pages 1–11. Springer Verlag, April 1999.
15. Потий А.В., Избенко Ю.А. Обоснование выбора метода построения криптографически стойких булевых функций. Всеукр.начно-тех.сборник "Радиотехника", Харьков, 2002, вып.126, стр.132-137.
16. J. Seberry and X. Zhang. Hadamar Matrices, Bent Functions and Cryptography // In J.H.Dinitz and D.R. Stinson, editors, Contemporary Design Theory: A Collection of Surveys, chapter 11, pages 431-559, John Wiley and Sons, Inc, 1995.
17. J. Seberry, X.-M. Zhang and Y. Zheng. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions // In Information and Computation, Vol. 119, No 1, pp. 1 - 13, 1995.