УДК 519.7

М. В. Наумов

ГЕНЕРАЦИЯ ЧАСТИЧНО БЕНТ-ФУНКЦИЙ

Для булевых функций в криптографии важны следующие характеристики: сбалансированность, нелинейность, критерий распространения, корреляционная иммунность, степень и отсутствие ненулевых линейных структур. Частично бент-функции – это класс булевых функций, которые представляют интерес, поскольку могут обладать ценными криптографическими свойствами.

Предлагаются два алгоритма генерации частично бент-функций. Эти алгоритмы были реализованы и исследованы; второй из них позволяет улучшать криптографические свойства генерируемых функций.

Ключевые слова: булевы функции, частично бент-функции, корреляционная иммунность.

В работе использованы следующие обозначения.

$Z_2 = \{ 0, 1 \}$; $n \in N$, $G = \{ 0, 1 \}^n$ – множество всех двоичных векторов длины n;

$\oplus$ – сумма по модулю 2, $u \oplus v$ – вектор, каждый бит которого равен сумме по модулю 2 соответствующих бит векторов u и v;

$(u, v) = u_1 v_1 \oplus \ldots \oplus u_n v_n$ – скалярное произведение векторов u и v из G;

$f: G \to \{0, 1\}$ – булева функция от n переменных;

$w(f) = |\{ s \in G : f(s) \neq 0 \}|$ – вес функции f;

$P_2(n)$ – множество булевых функций от n переменных;

$W_f(s) = \sum_{x \in G} (-1)^{f(x)+(x,s)}$ – преобразование Уолша–Адамара функции f, $W_f: G \to Z$;

NW_f – количество ненулевых значений функции $W_f(s)$;

$\Delta_f(s) = \sum_{x \in G} (-1)^{f(x)+f(x \oplus s)}$ – функция автокорреляции, $\Delta_f : G \to Z$;

$N\Delta_f$ – количество ненулевых значений функции автокорреляции;

$d(f, g) = |\{ s \in G : f(s) \neq g(s) \}| = w(f \oplus g)$ – расстояние по Хэммингу между f и g из $P_2(n)$;

$d(f, T) = \min_{g \in T} d(f, g)$ – расстояние между функцией $f \in P_2(n)$ и множеством $T \subset P_2(n)$;

$x^0 = 1, x^1 = x$, $f(x_1, \ldots, x_n) = \bigoplus_{(i_1, \ldots, i_n) \in G} a_{i_1, \ldots, i_n} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ – представление функции $f \in P_2(n)$ в виде алгебраической нормальной формы (АНФ), $a_{i_1, \ldots, i_n} \in \{0, 1\}$;

$\deg (x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}) = \sum_{k=1}^{n} i_k$ – степень монома $x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$, число входящих в него переменных;

$\deg f$ – степень функции f, наибольшая из степеней мономов ее АНФ;

$A(n) = \{ (a, x) \oplus a_0 : a \in G, a_0 \in \{0, 1\} \}$ – класс аффинных функций, $A(n) \subset P_2(n)$;

$N_f = d(f, A(n))$ – нелинейность функции f;

КИ(m) – корреляционная иммунность порядка m;

КР(m) – критерий распространения порядка m.

Основные понятия. Для генерации частично бент-функций применяются обычные бент-функции.

Бент-функцией называется функция $f \in P_2(n)$, у которой $W_f(s) = \pm 2^{n/2}$ для всех $s \in G$.

Утверждение [1]. f – бент-функция, если и только если для всех $s \in G$, $s \neq 0$ выполняется условие $\Delta_f(s) = 0$.

Бент-функции существуют только для четного n, так как W_f – целочисленная функция.

Бент-функции можно генерировать с помощью следующей теоремы.

Теорема (*конструкция Мейорана–МакФарланда*) [2]. Пусть h – любая перестановка на $Z_2^{n/2}$, g – произвольная булева функция от $n/2$ переменных. Тогда функция $f(u', u'') = (u', h(u'')) \oplus g(u'')$ является бент-функцией от n переменных.

Функция $f \in P_2(n)$ называется корреляционно-иммунной порядка m (КИ(m)), если любая ее подфункция от $(n - m)$ переменных, полученная фиксацией остальных m переменных, имеет вес $\frac{w(f)}{2^m}$. Очевидно, что если функция КИ(m), то она КИ(k) для любого $k < m$.

Известно, что $f(x)$ – КИ(m), если и только если $W_f(s) = 0$ для всех $s \in G$ таких, что $1 \le w(s) \le m$.

Корреляционная иммунность позволяет противостоять корреляционной атаке.

К сожалению, бент-функции не могут быть корреляционно-иммунными и сбалансированными, поэтому изучаются различные расширения бент-функций.

Говорят, что функция f удовлетворяет критерию распространения (КР) по направлению a, если $\Delta_f(a) = 0$, т. е. производная $D_a f = f(x) \oplus f(x \oplus a)$ сбалансирована.

Выполнение критерия распространения по направлению a приводит к тому, что $f(x) = f(x \oplus a)$ с вероятностью 0,5, т. е. знание значения $f(x \oplus a)$ не поможет нам узнать $f(x)$.

Говорят, что функция f удовлетворяет критерию распространения порядка m (КР(m)), если $\Delta_f(s) = 0$ для всех $s \in G$ таких, что $1 \le w(s) \le m$.

Критерий распространения – это свойство, которое характеризует поведение функции в момент, когда некоторые ее координаты инвертированы. Это свойство булевой функции подобно свойству диффузии для криптосистемы. Функции, применяемые в блочных шифрах, должны иметь высокий порядок КР.

Частично бент-функции. Функция $f \in P_2(n)$ называется частично бент-функцией, если $NW_f \cdot N\Delta_f = 2^n$.

Для любой бент-функции по определению $NW_f = 2^n$, а по критерию Ротхауза $N\Delta_f = 1$, поэтому класс бент-функций содержится в классе частично бент-функций.

Частично бент-функции представляют интерес в криптографии, потому что для них произведение $NW_f \cdot N\Delta_f$ имеет минимальное значение, что дает основание надеяться на то, что число ненулевых значений преобразования Уолша–Адамара и функции автокорреляции также мало, однако это совсем не гарантирует КИ и КР, ведь может оказаться $W_f(s) \neq 0$ или $\Delta_f(s) \neq 0$ на единственном векторе s веса 1. Очевидно, частично бент-функции могут удовлетворять критерию распространения по многим направлениям (в зависимости от $N\Delta_f$), важному свойству безопасности.

Обычные бент-функции используются в стандарте связи CDMA, в блоках замены (S-boxes), в некоторых шифрах, хэш-функциях [3]. Возможно, частично бент-функции можно использовать в тех же самых областях.

Генератор частично бент-функций 1. Генерировать частично бент-функции можно с помощью следующей теоремы.

Теорема 1 [4]. Функция $f \in P_2(n)$ является частично бент-функцией тогда и только тогда, когда существует невырожденная матрица A с элементами из Z_2 и вектор $\beta \in Z_2^n$ такие, что $f(xA \oplus \beta) = g(x_0) \oplus (x_1, t)$, где $x = (x_0\, x_1),\ x \in Z_2^n,\ x_0 \in Z_2^{2h},\ x_1 \in Z_2^{n-2h},\ t \in Z_2^{n-2h}$; g – бент-функция.

Опишем этот генератор и вспомогательный генератор невырожденной матрицы. Бент-функции будем строить с помощью конструкции Мейорана–МакФарланда.

Генератор невырожденной матрицы

Вход: $n \in N$.

Выход: невырожденная матрица A размерности $n \times n$.

1. Будем представлять матрицу A как множество строк. Возьмем в качестве ее первой строки произвольный ненулевой вектор e_1 длины n, $A = \{e_1\}$. Пусть $M = \{0, e_1\}$. Под M будем понимать линейную оболочку строк матрицы A.

2. Если в A есть n строк, т. е. $M = G$, то возвращаем A.

3. Берем произвольный вектор $e \in G \setminus M$.

4. $A = A \cup e,\ M = M \cup \{m \oplus e : m \in M\}$.

5. Идем на шаг 2.

Генератор частично бент-функций 1

Вход: $n \in N$, $0 \le h \le \lfloor n/2 \rfloor$.

Выход: $r \in P_2(n)$ – частично бент-функция или ответ «не существует».

1. Если $n = 2h$, то генерируем бент-функцию $r \in P_2(n)$ и возвращаем ее.

2. Генерируем бент-функцию $g(x_0)$ на Z_2^{2h} и произвольный вектор $t \in Z_2^{n-2h}$.

3. Для всех $x = (x_0\, x_1) \in G$ полагаем $f(x) = g(x_0) \oplus (x_1, t)$.

4. Генерируем невырожденную матрицу A и вектор $\beta \in Z_2^n$.

5. Для всех $x \in G$ полагаем $r(x) = f(xA \oplus \beta)$. Возвращаем r.

Замечание. Нелинейность функции $r(x)$ равна $N_r = 2^{n-1} - 2^{n-h-1}$. Такая же нелинейность у функций, которые выдает генератор 2. Это следует из теорем, которые приводятся в [5].

Определенные на подпространстве бент-функции. Следующие три определения взяты из [6].

Пусть $S \subset G$. Функция $f : S \to \{0, 1\}$ называется частично определенной булевой функцией. Обозначать такие функции мы будем $f|_S$, а называть просто – функциями, определенными на S.

Неполным преобразованием Уолша–Адамара для f называется функция $W_f^S(\upsilon) = \sum_{u \in S} (-1)^{f(u)+(u,\upsilon)}$, определенная на G.

Функция f – частично определенная бент-функция, если для всех $\upsilon \in G$ выполняется $W_f^S(\upsilon) = \pm\sqrt{|S|}$. Мы будем называть f бент-функцией, определенной на S.

Пусть E' – подпространство G и f – функция, определенная на E'. Введем функцию $\Delta_f^{E'}(\upsilon) = \sum_{u \in E'} (-1)^{f(u)+f(u \oplus \upsilon)}$, определенную на E', и назовем ее функцией автокорреляции для f на подпространстве E' (определение из [7]).

Приведенное ниже утверждение 2 будет использовано в генераторе 2 частично бент-функций.

Утверждение 1 [7] (характеризация определённых на подпространстве бент-функций). Пусть E' – подпространство G с базисом $\{e_1, \ldots, e_{2h}\}$ и f – частично определенная функция на нем.

f – частично определенная бент-функция на E', если и только если для всех $s' \in E',\ s' \neq 0$ выполняется $\Delta_f^{E'}(s') = 0$.

Сформулируем и докажем следующее утверждение.

Утверждение 2 (о бент-функции, определённой на подпространстве). Пусть E' – подпространство G

с базисом $\{e_1, \ldots, e_{2h}\}$ и f – функция, определенная на E'.

Определим булеву функцию g от $2h$ переменных так:

$$\forall x = x_1 \ldots x_{2h} \in Z_2^{2h}, \quad g(x) = f(x_1 e_1 \oplus \ldots \oplus x_{2h} e_{2h}).$$

Тогда

$\forall s' \in E', s' \neq 0, \quad \Delta_f^{E'}(s') = 0 \quad \Leftrightarrow \quad g$ – бент-функция.

$$\triangleright \quad x' = x_1 e_1 \oplus \ldots \oplus x_{2h} e_{2h}, \; s' = s_1 e_1 \oplus \ldots \oplus s_{2h} e_{2h},$$

$$\Delta_f^{E'}(s') = \sum_{x' \in E'} (-1)^{f(x') + f(x' \oplus s')} = \sum_{x \in Z_2^{2h}} (-1)^{g(x) + g(x \oplus s)} = \Delta_g(s),$$

$$\forall s' \in E', \; s' \neq 0;$$

$$\Delta_f^{E'}(s') = 0 \quad \Leftrightarrow \quad \forall s \in Z_2^{2h}, \; s \neq 0;$$

$$\Delta_g(s) = 0. \quad \triangleleft$$

Как видим, утверждение 2 дает нам способ построения определенной на подпространстве бент-функции с помощью обычной бент-функции.

Генератор частично бент-функций 2. В [5] было впервые введено понятие частично бент-функции и сформулирована приведенная ниже теорема.

Теорема 2. Любая функция $f \in P_2(n)$ удовлетворяет неравенству $NW_f \cdot N\Delta_f \geq 2^n$.

Следующие утверждения эквивалентны:

а) функция f – частично бент-функция;

б) $\exists z \in G, \quad \forall s \in G, \; \Delta_f(s) = 0 \vee \Delta_f(s) = (-1)^{(s,z)} 2^n$;

в) G разлагается в прямую сумму подпространств $E = \{x \in G : \; \Delta_f(x) \neq 0\}$ *и* E' (E' четной размерности) так, что $f|_{E'}$ – бент-функция и $\forall x \in E, \quad \forall y \in E', \quad f(x \oplus y) = f(y) \oplus (x, z)$. Здесь z – любое из тех, которые могут быть выбраны в пункте (*б*).

Поскольку вектор z встречается и далее в теореме 3, назовем его базовым вектором аффинной части для частично бент-функции f.

Следующий генератор основан на теореме 2 и утверждении 2:

Вход: $n \in N$, $0 \leq h \leq \lfloor n/2 \rfloor$.

Выход: $f \in P_2(n)$, $N_f = 2^{n-1} - 2^{n-h-1}$ или ответ – «не существует».

1. Если $n = 2h$, то генерируем бент-функцию $f \in P_2(n)$ и возвращаем ее.

2. Генерируем бент-функцию $g \in P_2(2h)$ и произвольный вектор $z \in G$.

3. Генерируем базисы пространств E' и E, в прямую сумму которых раскладывается G. Это n линейно независимых булевых векторов длины n, $\{e_1, \ldots, e_{2h}\}$ – базис E', $\{e_{2h+1}, \ldots, e_n\}$ – базис E. Базисы получаем так: генерируем невырожденную матрицу A размерности $n \times n$, ее первые $2h$ строчек – базис E', остальные – базис E.

4. Для всех $x = (x_1, \ldots, x_n) \in Z_2^n$ полагаем $f(\overset{n}{\underset{i=1}{\oplus}} x_i e_i) = g(x_1, \ldots, x_{2h}) \oplus \overset{n}{\underset{i=2h+1}{\oplus}} x_i (e_i, z)$.

Анализ работы генераторов частично бент-функций. Время работы генераторов примерно одинаково, поскольку они похожи по построению. В генераторе 2 $f(\overset{n}{\underset{i=1}{\oplus}} x_i e_i) = f(xA)$, т. е. генерация невырожденной матрицы используется в обоих генераторах частично бент-функций и занимает 50…60 % всего времени их работы.

В дальнейшем имеет смысл использовать генератор 2, поскольку он позволяет явно задавать пространство E и вектор z, с помощью определенного выбора которых можно попытаться улучшить КИ и КР, задать сбалансированность. Для этого используется следующая теорема.

Теорема 3 [5]. Пусть f – частично бент-функция, z – вектор из пункта (*ii*) теоремы 2, $E = \{x \in G : \; \Delta_f(x) \neq 0\}$. Функция f является:

а) сбалансированной $\Leftrightarrow f|_E \neq \text{const}$;

б) несбалансированной $\Leftrightarrow f|_E = \text{const}$ и $w(f) = 2^{n-1} \pm 2^{n-h-1}$, где $\dim E = n - 2h$, $0 \leq h \leq \lfloor n/2 \rfloor$;

в) корреляционно-иммунной порядка $k \Leftrightarrow$ смежный класс $z \oplus E^{\perp}$ содержит только векторы веса больше k или нулевого;

г) сбалансированной корреляционно-иммунной порядка $k \Leftrightarrow$ класс $z \oplus E^{\perp}$ содержит только векторы веса больше k;

д) удовлетворяет критерию распространения РС(k) $\Leftrightarrow E$ не содержит векторов веса w, $1 \leq w \leq k$.

В этой теореме $E^{\perp} = \{x \in G : \forall e \in E \quad (x, e) = 0\}$. Используя теорему 2, можно пытаться улучшать порядок КИ и КР частично бент-функций.

Улучшение порядка КИ и КР. О работе генератора 2 без улучшений можно судить по следующей таблице (табл. 1).

В генераторе 2 есть возможность напрямую задавать для частично бент-функции базовый вектор аффинной части z и пространство линейных структур E. Это означает, что можно попытаться улучшить порядок КИ и КР для генерируемой функции, так как из теоремы 2 известно, что порядок КИ определяется смежным классом $z \oplus E^{\perp}$, а порядок КР – пространством E.

Начнем с критерия распространения. Выдаваемая функция удовлетворяет КР(k) тогда и только тогда, когда все ненулевые векторы пространства E имеют вес больше k. Нужно сконструировать E таким образом, чтобы число k было как можно больше.

Если $\dim E = n - 2h = 1$, т. е. базис пространства E состоит из единственного вектора, то мы берем в качестве этого вектора вектор из всех единиц. Он обеспечивает максимально возможный порядок КР, равный $2h$. Например, улучшенный генератор 2 выдает в этом случае (n = 15, h = 7) функцию с порядком КИ, равным единице, и порядком КР, равным 14.

Множество {1, 2, …, n} можно разбить на dim E непересекающихся множеств K_i с числом элементов, превосходящим или равным $\lfloor n/\dim E \rfloor$. С каждым множеством K_i сопоставим вектор длины n, в котором единицы стоят только в позициях из K_i. Очевидно, эти dim E векторов линейно независимы. Таким образом, всегда можно добиться порядка КР, равного $\lfloor n/\dim E \rfloor - 1$.

Пусть p – порядок КР. Начиная с p = 1 (или $\lfloor n/\dim E \rfloor - 1$, если это не нуль) и до $p = 2h$ пробуем строить пространство E, обеспечивающее КР(p), с помощью описанного ниже алгоритма; если построить E удается – увеличиваем p, иначе выходим из цикла и E остается тем, что было построено для предыдущего p.

Алгоритм построения пространства E

Вход: n, dim E, p – требуемый порядок КР.

Выход: базис E или ответ – «не найден».

1. Если dim E = 1, то возвращаем базис E – вектор из всех единиц.

2. Берем в качестве e_1 случайный вектор. Если он не подошел, т. е. его вес $\le p$, то генерируем случайное число t от p + 1 до n и пусть e_1 – это вектор, у которого первые t позиций заполнены единицами. Полагаем $M = \{0, e_1\}$, $K = G \setminus M$, i = 2. Здесь M – линейная оболочка построенных векторов базиса E, K – множество кандидатов на место e_i.

3. Строим e_i. Сначала пробуем на место e_i случайный вектор. Если он подходит, идем на шаг 4, иначе вычеркиваем этот вектор из K. Перебираем векторы из K с начала или с конца до тех пор, пока не найдем подходящий вектор; неподходящие векторы вычеркиваем. Если нашли подходящий вектор (его вес больше p, и он не приводит к появлению в M ненулевых векторов веса $\le p$), то идем на шаг 4, иначе ответ – «не найден».

4. $M = M \cup \{m \oplus e_i : m \in M\}$,

$K = K \setminus \{m \oplus e_i : m \in M\}$.

5. Если базис E размерности dim E еще не построен, то увеличиваем i на единицу и идем на шаг 3, иначе возвращаем базис E.

Функция с n = 15, h = 5 генерируется с использованием алгоритма построения E примерно за три секунды. Для n = 21, h = 7 время работы этого алгоритма неизвестно; оно слишком велико. Ниже приводятся характеристики функций, построенных с применением этого алгоритма (табл. 2).

Как видим, порядок КР действительно улучшился. Функции, для которых он был меньше четырех, перестали выдаваться вообще.

После построения пространства E находим для него произвольное прямое дополнение, это будет пространство E'. Функцию вычисления прямого дополнения нетрудно реализовать на основе предложенного ранее генератора невырожденной матрицы.

Вычисление прямого дополнения E′ пространства E

Вход: E, dim E.

Выход: базис E'.

1. $M = E$, i = 1.

2. Если $i > n - \dim E$, то возвращаем $\{e_1, \ldots, e_{n-\dim E}\}$ – базис E'.

3. Берем в качестве e_i произвольный вектор из $G \setminus M$.

4. Расширяем M: $M = M \cup \{m \oplus e_i : m \in M\}$, $i = i +$ 1. Идем на шаг 2.

Этот алгоритм, так же как и генератор невырожденной матрицы, можно немного улучшить: если мы нашли последний вектор, то линейную оболочку остальных векторов M расширять не нужно, поскольку она больше не понадобится.

Таблица 1

1 000 функций, выданных генератором 2: n = 15, h = 5; сбалансированных – 966

	не РС(1)	РС(1)	РС(2)	РС(3)	РС(4)	РС(5)
не КИ(1)	6	27 (3)	107 (8)	170 (6)	42	3
КИ(1)	–	45	213 (5)	253 (9)	60 (3)	–
КИ(2)	3	11	14	9	–	–

Примечание. Здесь и далее в таблицах: без скобок – число сбалансированных функций, в скобках – несбалансированных.

Таблица 2

1 000 функций, выданных генератором 2 с улучшенным КР: n = 15, h = 5; сбалансированных – 966

	не КР(1)	КР(1)	КР(2)	КР(3)	КР(4)	КР(5)	КР(6)
не КИ(1)	–	–	–	–	–	338 (2)	109
КИ(1)					4 (1)	391 (21)	102
КИ(2)					–	16 (2)	6
КИ(3)					–	–	(8)

Из базисов E и E' составляется матрица A (см. генератор 2).

Теперь попробуем улучшить порядок КИ. На пространство $E^{\perp}$ повлиять не можем, так как уже построили E; $E^{\perp}$ вычисляем как множество векторов из G, каждый из которых ортогонален всем векторам базиса E. Осталось перебрать все значения z и выбрать среди них то, которое обеспечивает самый высокий порядок КИ. Пишем вспомогательную функцию, которая по z и $E^{\perp}$ определяет, какой порядок КИ обеспечивает смежный класс $z \oplus E^{\perp}$. Для этого проверяем, принадлежат ли $z \oplus E^{\perp}$ векторы веса 1, 2 и т. д.

Можно перебирать все значения z из G, однако это необязательно, поскольку $z_1 \oplus E^{\perp} = z_2 \oplus E^{\perp}$, если и только если $z_2 \oplus z_1 \in E^{\perp}$. Очевидно, достаточно перебрать все значения z из пространства E_1 – прямого дополнения $E^{\perp}$; $\dim E_1 = n - \dim E^{\perp} = \dim E = n - 2h$. Как находить прямое дополнение, нам известно. Базис $E^{\perp}$ находится примерно так же, как базис G в генераторе невырожденной матрицы. Для тех значений n и h, которые мы использовали ранее, перебор z не занимает существенного времени – функция генерируется примерно за то же время. О влиянии улучшения z на характеристики генерируемой функции можно судить по приведенным ниже таблицам (табл. 3, 4). Большое число несбалансированных функций в них объясняется тем, что перебор значений z начинается с нуля, а остальные значения z улучшения КИ не дают.

Также была сделана попытка одновременного улучшения КИ и КР.

Выясним, как можно улучшить порядок КИ функции с помощью аффинной добавки.

Влияние аффинной добавки на значения преобразования Уолша–Адамара такое: если $\tilde{f}(x) = f(x) \oplus (x,t) \oplus t_0$, где $t \in G, t_0 \in \{0,1\}$, то $W_{\tilde{f}}(s) = W_f(s \oplus t)$, т. е. аффинная добавка приводит к сдвигу значений преобразования Уолша–Адамара. Пусть f является частично бент-функцией, тогда

$$W_{\tilde{f}}(s) \neq 0 \Leftrightarrow W_f(s \oplus t) \neq 0 \Leftrightarrow$$

$$\Leftrightarrow s \oplus t \in z \oplus E^{\perp} \Leftrightarrow s \in z \oplus t \oplus E^{\perp},$$

т. е. аффинная добавка к частично бент-функции приводит лишь к изменению z. Улучшить КИ частично бент-функции с помощью аффинной добавки – это значит перебрать все значения вектора z. Как это можно сделать, мы уже знаем.

Предложенный ниже алгоритм может применяться для улучшения КИ любой булевой функции. На практике он не исследовался.

Алгоритм улучшения порядка КИ функции с помощью аффинной добавки

Вход: n, $f \in P_2(n)$.

Выход: $t \in G$ или ответ – «нельзя улучшить».

1. Находим вес функции f. Если f является константой или ее вес нечетный, то ответ – «нельзя улучшить».

2. Находим все значения преобразования Уолша–Адамара функции f, вычисляем множество $E = \{s \in G : W_f(s) \neq 0\}$ и k – порядок КИ функции f.

3. Если функция несбалансированная, то вычисляем максимальное m такое, что для всех $s \in G$ выполняется $2^{m+1} \mid W_f(s)$, иначе вычисляем максимальное m такое, что для всех $s \in G$ выполняется $2^{m+2} \mid W_f(s)$. По теореме о необходимом условии КИ [1] мы не сможем получить порядок КИ выше m. Если $k = m$, то ответ – «нельзя улучшить».

4. $i = 1$. $T = G$. T – это множество возможных значений вектора t.

5. Нам известно, что для функции $\tilde{f}(x) = f(x) \oplus (x,t) \oplus t_0, t_0 \in \{0,1\}$ множество $t \oplus E = \{s \in G : W_{\tilde{f}}(s) \neq 0\}$. Для каждого $t \in T$ и каждого $j \in \{j \in G : w(j) = i\}$ проверяем: если $t \oplus j \in E$, то $T = T \setminus t$. В итоге в T остаются только те значения t, которые обеспечивают КИ(i) для $\tilde{f}$. Если T не пусто, то берем любое $t \in T$, в противном случае поступаем так: если $i = 1$ или $i - 1 \leq k$, то ответ – «нельзя улучшить», иначе возвращаем t.

6. Если $i = m$, то возвращаем t. $i = i + 1$. Идем на шаг 4.

Таблица 3

1 000 функций, выданных генератором 2 с улучшенным КИ: $n = 15$, $h = 5$; сбалансированных – 328

	не КР(1)	КР(1)	КР(2)	КР(3)	КР(4)	КР(5)	КР(6)
не КИ(1)	–						
КИ(1)	–	–	(142)	48 (291)	44 (190)	–	–
КИ(2)	–	–	189 (49)	47	–	–	–

Таблица 4

1 000 функций, выданных генератором 2 с улучшенным КИ и КР: $n = 15$, $h = 5$; сбалансированных – 277

	не КР(1)	КР(1)	КР(2)	КР(3)	КР(4)	КР(5)	КР(6)
не КИ(1)	–	–	–	–	–	–	–
КИ(1)					(1)	8 (435)	–
КИ(2)					1	268 (51)	–
КИ(3)					–	–	(236)

Если этот алгоритм выдает t, то функция $\tilde{f}$ будет иметь более высокий порядок КИ, нежели f. Известно, что аффинная добавка никак не влияет на порядок КР.

Итак, изложены результаты реализации и исследования двух генераторов частично бент-функций, описаны возможности по улучшению порядков КИ и КР таких функций. Работоспособность алгоритмов проверена на практике, изучены свойства генерируемых функций.

Автор выражает благодарность И. А. Панкратовой и К. В. Сафонову за постоянное внимание к работе и ценные замечания.

Библиографические ссылки

1. Carlet C. Boolean Functions for Cryptography and Error Correcting Codes [Electronic resource] // INRIA. 2010. URL: http://www-rocq.inria.fr/codes/Claude.Carlet/chap-fcts-Bool-corr.pdf. (дата обращения: 08.06.2010).

2. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ // Прикл. дискретная математика. 2009. № 1 (3). С. 15–36.

3. Bent-function [Electronic resource] // Wikipedia. 2010. URL: http://en.wikipedia.org/wiki/Bent_function (дата обращения: 08.06.2010).

4. Zheng Y., Zhang X. M. Plateaued functions // ICICS'99. Lecture Notes in Computer Science. 1999. Vol. 1726. P. 284–300.

5. Carlet C. Partially-bent functions // Design, Codes and Cryptography. 1993. Vol. 3. №. 2. P. 135–145.

6. Токарева Н. Н. Обобщения бент-функций. Обзор работ // Дискрет. анализ и исследование операций. 2010. Т. 17. № 1. С. 34–64.

7. Агафонова И. В. Криптографические свойства нелинейных булевых функций [Electronic resource] // Семинар по дискретному гармоническому анализу и геометрическому моделированию DHA & CAGD. 2007. URL: http://dha.spb.ru/PDF/cryptoBOOLEAN.pdf (дата обращения: 08.06.2010).

M. V. Naumov

THE GENERATION OF PARTIALLY-BENT FUNCTIONS

Most important characteristics of cryptographic functions are balancedness, nonlinearity, propagation criterion, correlation immunity, degree and non-existence of nonzero linear structure. Partially-bent functions form super-class of the class of bent functions. These functions may achieve desirable characteristics.

Two algorithms for generation of partially-bent functions were supposed and studied. Second algorithm may improve cryptographic characteristics of generated functions.

Keywords: Boolean functions, partially-bent functions, correlation immunity.

УДК 519.62

В. А. Нестеров

ПОПЕРЕЧНЫЕ КОЛЕБАНИЯ ПЛАСТИНЫ, ПОДАТЛИВОЙ ПРИ ТРАНСВЕРСАЛЬНОМ СДВИГЕ

Рассматривается конечно-элементный модальный расчет пластины с низкой трансверсальной сдвиговой жесткостью. В каждом из четырех узлов прямоугольного конечного элемента пластины в качестве основных кинематических параметров присутствуют углы трансверсального сдвига. На примере анализа собственных колебаний композитной пластины показана актуальность разработанной конечно-элементной модели. Представлены результаты численного исследования влияния граничных условий неклассического вида на величины частот собственных колебаний.

Ключевые слова: пластина, метод конечных элементов, трансверсальный сдвиг, модальный анализ.

Композитные конструкции, обладающие высокой степенью весового совершенства, часто используются в производстве космической техники. Композитные пластины отличаются низкой сдвиговой жесткостью по отношению к трансверсальным напряжениям. Учет указанной особенности при реализации численного расчета приводит к повышению порядка разрешающих уравнений за счет введения в рассмотрение углов трансверсального сдвига.

Разрешающие уравнения теории метода конечных элементов (МКЭ) для задачи о собственных колебаниях пластины с низкой трансверсальной сдвиговой жесткостью получим вариационным способом. Для этого запишем выражение полной энергии колеблющейся пластины