УДК 621.3.06

А.А.КУЗНЕЦОВ, канд.техн.наук, ***Ю.А.ИЗБЕНКО***, канд.техн.наук, ***А.А.ЮКАЛЬЧУК*** (г.Харьков)

ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВОЗМОЖНОСТИ РАЗРАБОТКИ КОМБИНИРОВАННОГО МЕТОДА ПОСТРОЕНИЯ ВЫСОКО НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

Наведено теоретичне обгрунтування можливості розробки комбінованого методу побудови високо нелінійних булевих функцій. Обрунтування базується на аналізі відомих методів побудови даних функцій та застосуванні процедур модифікації функцій. Дане обгрунтування дозволяє будувати функції з високими показниками стійкості.

Theoretical basis possibility development of the combination method construction highly nonlinear Boolean functions is presented. The basis is founded on analysis the known methods construction that functions and applaing some procedures modification of functions. This basis allow construction the functions with high criteria strong.

Одной из базовых компонент симметричных криптосистем являются нелинейные преобразования, определяющие стойкость к методам криптоанализа. Как правило, нелинейные преобразования строятся на основе нелинейных булевых функций. Одним из основных показателей их стойкости является нелинейность. Известные методы построения нелинейных булевых функций делятся на: эвристические методы, использующие некоторые интуитивные подходы к построению требуемых функций; систематические методы, использующие некоторые итеративные процедуры модификации некоторых функций. Известно [1], что наивысшей нелинейности достигают функции, построенные на основе применения эвристических методов. Их недостатком является высокая вычислительная сложность и невозможность обсуждения некоторых показателей стойкости. Функции, построенные на основе систематических методов, уступая в нелинейности, позволяют обсуждать остальные показатели стойкости. Поскольку стойкость симметричных схем криптопреобразований определяется, прежде всего, степенью нелинейности, актуальной задачей является теоретическое обоснование возможности разработки комбинированного метода построения нелинейных булевых функций, который, в отличие от известных, объединил бы в себе принципы эвристических и систематических методов и позволил строить высоко нелинейные булевы функции с высокими показателями стойкости. Целью данной статьи является теоретическое обоснование возможности построения данного метода.

Введем основные понятия и определения.

Основными показателями стойкости нелинейных функций являются [1,2]: сбалансированность, нелинейность, критерий распространения (строгий лавинный критерий), алгебраическая степень.

Функция f над $GF(2^n)$ является сбалансированной, если ее выходные значения являются равновероятными: $|\{x \mid f(x) = 0\}| = |\{x \mid f(x) = 1\}| = 2^{n-1}$.

Нелинейность функции N_f - минимальное расстояние Хэмминга N_f между функцией f и всеми аффинными функциями над $GF(2^n)$ [1]:

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

где φ - множество аффинных функций.

Функция f над полем $GF(2^n)$ удовлетворяет [1]:

- критерию распространения относительно вектора α, $KP(\alpha)$, если функция $f(x) \oplus f(x \oplus \alpha)$ является сбалансированной, $x \in V_n$, где $x = (x_1, x_2, \ldots, x_n)$:

$$P(f(x) = f(x \oplus \alpha)) = \frac{1}{2};$$

- критерию распространения степени k, $KP(k)$, если удовлетворяется критерий распространения относительно всех векторов $\alpha \in V_n$ при $1 \le W(\alpha) \le k$:

$$P(f(x) = f(x \oplus \alpha)) = \frac{1}{2} \qquad \forall \alpha : 1 \le W(\alpha) \le k;$$

- строгому лавинному критерию, $СЛК$, если f удовлетворяет критерию распространения степени 1:

$$P(f(x) = f(x \oplus \alpha)) = \frac{1}{2} \qquad \forall \alpha : W(\alpha) = 1.$$

Алгебраическая степень $deg(f)$ является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме. Алгебраической нормальной формой называется выражение вида

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

При теоретическом обосновании возможности построения комбинированного метода в качестве основы взят эвристический метод модификации Себерри-Чжаня (далее – метод модификации) [1] как метод, позволяющий достигать наивысшей нелинейности. Данный метод основан на использовании теории адамаровых матриц [4] и бент-функций [3].

Известно [2], что верхней границы нелинейности над $GF(2^n)$ могут достигать только бент-функции. Данные функции обладают рядом привлекательных свойств: максимальным расстоянием до аффинных функций и линейных структур. Так, для бент-функций справедливы следующие выражения [3]: $d(f_б, A) = N_f = 2^{n-1} - 2^{n/2-1}$ и $d(f_б, £) = 2^{n-2}$, где A и $£$ - множество аффинных функций и линейных структур соответственно. Однако две причины препятствуют использованию бент-функций в прямом виде [3]:

1. Последовательности бент-функций не сбалансированы, что делает их уязвимыми к статистическому анализу $|\{x \mid f(x) = 0\}| \ne |\{x \mid f(x) = 1\}| \ne 2^{n-1}$.

2. Бент-функции существуют лишь на четных векторных пространствах: $f_6(x) \in V_n$, $n = 2k$; нередким требованием при разработке схем преобразования информации является разработка функций с нечетным количеством переменных.

Известно [3,4], что результатом конкатенации строк адамаровой матрицы является бент-последовательность, т.е. последовательность с максимально возможной нелинейностью. Данный факт взят за основу построения метода модификации.

Адамаровой матрицей называется (1, -1) - матрица H порядка n такая, что $HH^t = nI_n$, где H^t – транспонированная матрица H, а I_n – единичная матрица порядка n. Известно, что порядок таких матриц равен 1, 2 или делится на 4. В [1] рассматривается вид адамаровых матриц, именуемый матрицей Сильвестра-Адамара или матрицей Уолша-Адамара. Матрица Сильвестра-Адамара порядка 2^n, обозначаемая как H_n, порождается следующим рекурсивным соотношением

$$H_0 = 1, \qquad H_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_{n-1}, \qquad n = 1,2,\ldots,$$

где символ «⊗» обозначает кронекеровское произведение матриц.

Такие матрицы обладают, в частности, следующими свойствами [3,4].

– Конкатенация строк H_n дает бент-последовательность. Такие последовательности порождаются бент-функциями.

– Каждая строка матрицы H_n – это последовательность линейной функции $h_i = \langle \alpha_i,\ x \rangle$, где α_i – вектор из V_n, чье целочисленное представление равно i, $x = (x_1, x_2, \ldots, x_n)$. И обратное: последовательность любой аффинной функции над V_n – это строка H_n.

Метод модификации основан на использовании данного аппарата и состоит из двух этапов – подготовительного и основного.

В подготовительном этапе конкатенируются строки рассматриваемой матрицы H_n в единую последовательность, в результате чего получают бент-последовательность, т.е. последовательность, обладающую максимально возможной нелинейностью. Полученная последовательность является исходным материалом, используем для получения в основном этапе высоко нелинейной сбалансированной последовательности.

Рассмотрим поле V_{2k}. При четном $n \geq 4$ его можно представить как $n = 4t$, либо $n = 4t+2$, $t \geq 1$.

Лемма [1]. Для любого целого $t \geq 1$ существует

(i) сбалансированная функция f над V_{4t} такая, что $N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t$,

(ii) сбалансированная функция f над V_{4t+2} такая, что $N_f \geq 2^{4t+1} - 2^{2t} - 2^t$.

На основе последнего результата строится итеративная процедура для улучшения нелинейности сбалансированной последовательности. Отметим, что четное $n \geq 4$ можно представить как $n = 2^m$, $m \geq 2$, либо как $n = 2^s(2t + 1)$, где $s \geq 1$ и $t \geq 1$.

Рассматривается случай $n = 2^m$, $m \geq 2$. Начинают с бент-последовательности, полученной конкатенацией строк адамаровой матрицы $H_{2^{m-1}}$. Эта последовательность состоит из $2^{2^{m-1}}$ последовательностей длины $2^{2^{m-1}}$. Затем заменяют ведущую последовательность из всех единиц на бент-последовательность той же длины, полученную конкатенацией строк матрицы $H_{2^{m-2}}$. Длина новой ведущей последовательности становится $2^{2^{m-2}}$. Она заменяется еще одной бент-последовательностью такой же длины. Такой процесс замен продолжается до тех пор, пока длина ведущей последовательности из всех единиц не станет $2^2 = 4$. Для завершения процесса заменяют ведущую последовательность (1,1,1,1) на (1,-1,1,-1). Последняя замена делает всю последовательность сбалансированной.

Процедура модификации для случая $n = 2^s(2t + 1)$, где $s \geq 1$ и $t \geq 1$, строится аналогично за исключением последней замены. Здесь процесс продолжается до тех пор, пока длина ведущей последовательности из всех единиц не станет 2^{2t+1}. Последняя ведущая замена заменяется на $l_0^* = (e_{2^t}, e_{2^t+1}, \ldots, e_{2^{t+1}-1})$, вторую половину бент-последовательности $(e_0, e_1, \ldots, e_{2^{t+1}-1})$, где каждое e_i - строка матрицы H_{t+1}.

Тогда для любого целого $n \geq 4$ существует сбалансированная функция f над V_{4t} такая, что

$$N_f \geq \begin{cases} 2^{2^m-1} - \frac{1}{2}\left(2^{2^m-1} + 2^{2^m-2} + \ldots + 2^{2^2} + 2 \cdot 2^2\right), & n = 2^m, \\ 2^{2^s(2t+1)-1} - \frac{1}{2}\left(2^{2^{s-1}(2t+1)} + 2^{2^{s-2}(2t+1)} + \ldots + 2^{2^{t+1}} + 2^{t+1}\right), & n = 2^s(2t+1) \end{cases}.$$

Для получения сбалансированных функций над V_{2k+1} используются следующие утверждения.

Лемма [1]. Пусть ξ_1 – последовательность f_1 над V_s, и ξ_2 – последовательность f_2 над V_t. Тогда

– $f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t)$ – сбалансированная функция над V_{s+t}, если f_1 или f_2 сбалансированна;

– Кронекеровское произведение $\xi_1 \otimes \xi_2$ – последовательность функции $f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t)$.

Лемма [1]. Пусть ξ_1 – последовательность f_1 над V_s, и ξ_2 – последовательность f_2 над V_t. Также пусть $g(x_1, \ldots, x_s, y_1, \ldots, y_t) = f_1(x_1, \ldots, x_s) \oplus f_2(y_1, \ldots, y_t)$. Полагаем, что $\langle \xi_1,\ l_1 \rangle \leq P_1$ и $\langle \xi_2,\ l_2 \rangle \leq P_2$, где l_1 и l_2 – произвольные аффинные функции длиной 2^s и 2^t соответственно, а P_1 и P_2 – положительные целые. Тогда нелинейность функции g удовлетворяет соотношению

$$N_g \geq 2^{s+t-1} - \frac{1}{2} P_1 \cdot P_2 .$$

Теорема 1 [1]. Нелинейные последовательности, построенные в соответствии с методом модификации над V_n (n представимо как $n = 4t$, либо $n = 4t+2$, $t \geq 1$), являются сбалансированными и обладают нелинейностью $N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t$ либо $N_f \geq 2^{4t+1} - 2^{2t} - 2^t$.

Обсуждая приведенный метод, можно отметить, что полученные последовательности обладают более высокой нелинейностью, чем последовательности, генерируемые функциями, построенными в соответствии с методами систематического конструирования, и, в отличие от известных методов, гарантирует достижение нелинейности, наиболее близкой к верхней границе нелинейности [1]. Существенным недостатком данного метода, накладывающим ограничение на его практическое использование, является то, что он предоставляет лишь высоко нелинейные последовательности и не дает представления о функции, сгенерировавшей данную последовательность. Важным моментом при обсуждении стойкости функций, помимо их нелинейности, является рассмотрение и других показателей стойкости, таких как степень критерия распространения (строгий лавинный критерий), алгебраическая степень [2]. Обсуждение именно этих показателей стойкости для данного метода является затруднительным.

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 [4] представлен способ восстановления образующего полинома по выходной последовательности ξ, использующий следующую лемму.

Лемма1 [4]. Пусть ξ – последовательность некоторой функции f над V_n. Тогда существуют процедуры восстановления полиномиальной формы булевой функции

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

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 полиномиальные формы булевых функций, полученных в процессе применения метода модификации. Наличие полиномиальных форм позволит, в свою очередь, обсуждать такие показатели стойкости, как алгебраическая степень и критерий распространения (строгий лавинный критерий).

Далее, для получения функций с высокими показателями стойкости целесообразным представляется использование следующих леммы и теоремы.

Лемма 2 [1]. Сбалансированность, нелинейность и количество векторов, относительно которых функция удовлетворяет критерию распространения, являются инвариантными относительно аффинных преобразований координат функции.

Теорема 2 [4]. 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 теорем 1,2 и лемм 1, 2 сформулируем следующую теорему.

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

Таким образом, произведено теоретическое обоснование возможности построения комбинированного метода построения высоко нелинейных булевых функций на основе метода модификации с высокими показателями стойкости. Это позволяет применить разработанный подход для построения сбалансированных высоко нелинейных булевых функций, имеющих высокую алгебраическую степень и удовлетворяющих строгому лавинному критерию.

Список литературы: **1**.*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. **2**.*B.Schneier*. Applied Cryptography. 2nd edition, John Wiley & Sons, New York,1996. **3**.*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. **4**.*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.