

МЕТОД ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ БУЛЕВЫХ ФУНКЦИЙ С КОНТРОЛИРУЕМОЙ АЛГЕБРАИЧЕСКОЙ СТЕПЕНЬЮ

Ю.А. Избенко, А.В. Ивашкин
(представил д.т.н., проф. И.Д. Горбенко)

В статье предложен метод построения криптографически стойких булевых функций, позволяющий повысить стойкость схем преобразования информации к методам криптоанализа.

Стойкость различного рода криптографических систем в значительной степени зависит от свойств составных частей данных систем. Нелинейные преобразования, осуществляемые булевыми функциями, определяют стойкость криптопреобразований в блочных шифрах, поточных шифрах и хэш-функциях. Одними из основных показателей стойкости булевых функций являются сбалансированность и нелинейность, в качестве одного из дополнительных показателей рассматриваются алгебраическая степень функции и алгебраическая степень каждой координаты.

Рассмотрим некоторые понятия и определения. Пусть мы имеем некоторую функцию f над V_n , где V_n является векторным пространством, каждый вектор которого состоит из n элементов из $GF(2)$. Такая функция называется булевой функцией и может быть представлена в виде полинома из n координат. Обычно булевы функции представляются в алгебраической нормальной форме и рассматриваются как сумма произведений составляющих координат.

Пусть $V_n = (0, 1)^n$, f является функцией над V_n , где $\alpha_0 = (0, \dots, 0, 0)$, $\alpha_1 = (0, \dots, 0, 1)$, ..., $\alpha_{2^n-1} = (1, \dots, 1)$ – все векторы над V_n . Тогда $(1, -1)$ -последовательность, определенная как $((-1)^{f(\alpha_0)}, \dots, (-1)^{f(\alpha_{2^n-1})})$, называется последовательностью функции f . $(0, 1)$ -последовательность, определенная как $(f(\alpha_0), f(\alpha_1), \dots, f(\alpha_{2^n-1}))$, называется таблицей истинности функции f . $(1, -1)$ -последовательность $((1, -1)$ -последовательность) называется сбалансированной, если она содержит одинаковое количество нулей и единиц (единиц и минус единиц). Функция является сбалансированной, если сбалансирована ее последовательность.

Аффинной функцией f над V_n является функция вида $f = a_1x_1 \oplus \dots \oplus a_nx_n \oplus c$, где $a_j, c \in GF(2)$, $j = 1, 2, \dots, n$. Функция f называется линейной, если $c = 0$.

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 функции f – минимальное расстояние Хэмминга N_f между функцией f и всеми аффинными функциями над V_n [2]:

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

где φ – множество аффинных функций.

Для произвольной функции f нелинейность N_f над V_n может достигать:

$$N_f \leq 2^{n-1} - 2^{n/2-1}.$$

Алгебраическая степень $\deg(f)$ является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме. Алгебраической степенью $\deg(f, x_i)$ координаты x_i является степень самого длинного слагаемого функции, в котором присутствует координата x_i .

В настоящее время наиболее распространенными методами построения нелинейных булевых функций являются методы конкатенации и модификации бент-последовательностей. В целом метод модификации бент-последовательностей позволяет конструировать функции с большей нелинейностью, чем метод конкатенации, однако он является вычислительно сложным и на практике малоприменимым. Гораздо больший интерес представляет метод конкатенации, относящийся к методам систематического конструирования нелинейных функций, поскольку, в отличие от метода модификации, помимо меньшей вычислительной сложности позволяет обобщать показатели стойкости полученных функций.

Рассмотрим известные методы построения нелинейных функций, основанные на конкатенации булевых функций. В [1] представлен метод построения высоконелинейных сбалансированных булевых функций, в котором для выполнения построения используется булева функция f над заданным векторным пространством V_n . При этом процесс построения состоит из следующих двух этапов: выбора нелинейной функции f , имеющей нулевые значения в спектре Уолша, результатом которого является промежуточная булева функция; конкатенация подходящей линейной функции h над V_n , результатом которой является высоконелинейная сбалансированная булева функция. Алгебраическая степень полученной функции аналогична алгебраической степени начальной функции f . Данный метод имеет высокую вычислительную сложность за счет необходимости нахождения нелинейных функций с нулевыми значениями в спектре Уолша и поиска необходимой линейной функции h , которая может быть найдена путем полного перебора всех линейных функций

над V_n .

В [2] представлен метод построения высоконелинейных сбалансированных булевых функций, в котором построение состоит из выполнения конкатенации булевых функций, полученных путем модификации бент-функций, результатом которой есть высоконелинейная сбалансированная булева функция. Процедура выполнения конкатенации двух булевых функций над V_{2k+1} , где $k \geq 1$, полученных путем модификации бент-функций, описывается следующим выражением:

$$g(x_1, x_2, \dots, x_{2k+1}) = (I \oplus x_1) f_1(x_2, \dots, x_{2k+1}) \oplus x_1 f_2(x_2, \dots, x_{2k+1}), \quad (1)$$

где f_1, f_2 – бент-функции над V_{2k} ; g – полученная высоконелинейная сбалансированная булева функция над V_{2k+1} .

Процедура выполнения конкатенации четырех булевых функций над V_{2k} , где $k \geq 1$, полученных путем модификации бент-функций, описывается следующим выражением:

$$g(y, x) = \bigoplus_{i=0}^3 D_{\alpha_i}(y) f_i(x), \quad (2)$$

где $f_i(x)$ – бент-функции над V_{2k-2} ; $y = (y_1, y_2)$, $x = (x_1, \dots, x_{2k-2})$ и α_i – вектор над V_2 , чье целочисленное представление равно i ; $g(y, x)$ – полученная высоконелинейная сбалансированная булева функция над V_{2k} .

Функция, вычисленная над V_{2k+1} , является сбалансированной, имеет нелинейность $N_g \geq 2^{2k} - 2^k$, функция, вычисленная над V_{2k} , является сбалансированной, имеет нелинейность $N_g \geq 2^{2k-1} - 2^{2k}$. Алгебраическая степень обеих функций равна $\deg(g) = \max_i \{ \deg(f_i(x)) \} + 1$. Данный метод

требует много времени для построения криптографически стойких булевых функций над V_{2k} за счет необходимости построения четырех бент-функций с необходимыми свойствами; кроме того, максимальную алгебраическую степень координат $\deg(g, x_i)$, равняющуюся алгебраической степени полученных функций $\deg(g)$, имеют лишь те координаты x_i , которые находятся в наиболее длинном слагаемом функций, представленных в алгебраической нормальной форме, остальные координаты имеют меньшую алгебраическую степень, которая снижает криптографическую стойкость к атаке криптоанализа методом дифференциалов высших порядков.

Целью статьи является создание метода построения высоконелинейных сбалансированных булевых функций с контролируемой алгебраической степенью, позволяющих строить высоконелинейные сбалансированные булевы функции с низкими временными затратами и контролируемой алгебраической степенью каждой координаты.

Данная цель может быть достигнута, если в методе построения высоконелинейных сбалансированных булевых функций с контролируемой

алгебраической степенью, основанном на выполнении конкатенации булевых функций, полученных путем модификации бент-функций, результатом которой есть криптографически стойкая функция, процедуру конкатенации трех булевых функций над V_{2k+1} , где $k \geq 1$, выполняют в соответствии с выражением

$$g(x_1, x_2, \dots, x_{2k+1}) = x_1(f_1(x_2, \dots, x_{2k+1}) \oplus f_2(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1})) \oplus f_2(x_2, \dots, x_{2k+1}) \oplus h(x_2, \dots, x_{2k+1}), \quad (3)$$

где f_1, f_2 – бент-функции над V_{2k} ; h – неконстантная аффинная функция над V_{2k} ; g – полученная высоконелинейная сбалансированная булева функция над V_{2k+1} , а процедуру конкатенации трех булевых функций над V_{2k} , где $k \geq 1$, выполняют в соответствии с выражением

$$g(x_1, x_2, \dots, x_{2k}) = x_1(f_1(x_3, \dots, x_{2k}) \oplus f_2(x_3, \dots, x_{2k}) \oplus h(x_3, \dots, x_{2k})) \oplus x_2(f_1(x_3, \dots, x_{2k}) \oplus f_2(x_3, \dots, x_{2k}) \oplus h(x_3, \dots, x_{2k})) \oplus f_2(x_3, \dots, x_{2k}) \oplus h(x_3, \dots, x_{2k}), \quad (4)$$

где f_1, f_2 – бент-функции над V_{2k-2} ; h – неконстантная аффинная функция над V_{2k-2} ; g – полученная высоконелинейная сбалансированная булева функция над V_{2k} .

Функция g над V_{2k+1} является сбалансированной, имеет нелинейность $N_g \geq 2^{2k} - 2^k$ и алгебраическую степень каждой координаты

$$\deg(g) = (\deg(f_1(x)) = \deg(f_2(x))) + 1 = \deg(g, x_i), \quad i = 1, \dots, 2k + 1.$$

Функция g над V_{2k} является сбалансированной, имеет нелинейность

$$N_g \geq 2^{2k-2} - 2^{2k}$$

и алгебраическую степень каждой координаты

$$\deg(g) = (\deg(f_1(x)) = \deg(f_2(x))) + 1 = \deg(g, x_i), \quad i = 1, \dots, 2k.$$

Метод построения высоконелинейных сбалансированных булевых функций над V_{2k+1} с контролируемой алгебраической степенью каждой координаты может быть реализован следующим образом. Выполняется построение бент-функции $f_1(x_2, \dots, x_{2k+1})$ над V_{2k} таким образом, что выбирается произвольная квадратичная бент-функция с добавлением нелинейного слагаемого вида $x_2 x_4 \dots x_{2k}$ и считается количество "0" и "1" в ее выходной последовательности. Выполняется построение бент-функции $f_2(x_2, \dots, x_{2k+1})$ над V_{2k} таким образом, что выбирается произвольная квадратичная бент-функция с добавлением нелинейного слагаемого вида $x_3 x_5 \dots x_{2k+1}$. Далее случайным

образом фиксируется неконстантная аффинная функция $h(x_2, \dots, x_{2k+1})$ над V_{2k} и считается количество "0" и "1" в выходной последовательности конкатенации функций $f_2 \oplus h$. Если количество "0" и "1" в выходной последовательности f_1 равняется количеству "0" и "1" в выходной последовательности $f_2 \oplus h$, то функция h комплементируется единицей: $h = h \oplus 1$, иначе – не комплементируется. После определения f_1 , f_2 и h выполняется применение процедуры построения булевых функций над V_{2k+1} в соответствии с выражением (3). Результатом применения (3) есть функция g с высокими криптографическими показателями стойкости. Над V_{2k} построение высоконелинейных сбалансированных булевых функций с контролируемой алгебраической степенью каждой координаты может быть реализовано следующим образом. Выполняется построение бент-функции $f_1(x_3, \dots, x_{2k})$ над V_{2k-2} таким образом, что выбирается произвольная квадратичная бент-функция с добавлением нелинейного слагаемого вида $x_3 x_5 \dots x_{2k-1}$ и считается количество "0" и "1" в ее выходной последовательности. Выполняется построение бент-функции $f_2(x_3, \dots, x_{2k})$ над V_{2k-2} таким образом, что выбирается произвольная квадратичная бент-функция с добавлением нелинейного слагаемого вида $x_4 x_6 \dots x_{2k}$. Далее случайным образом фиксируется неконстантная аффинная функция $h(x_3, \dots, x_{2k})$ над V_{2k-2} и считается количество "0" и "1" в выходной последовательности конкатенации функций $f_2 \oplus h$. Если количество "0" и "1" в выходной последовательности f_1 равняется количеству "0" и "1" в выходной последовательности $f_2 \oplus h$, то функция h комплементируется единицей: $h = h \oplus 1$, иначе – не комплементируется. После определения f_1 , f_2 и h выполняется применение процедуры построения булевых функций над V_{2k} в соответствии с выражением (4). Результатом применения (4) есть функция g с высокими криптографическими показателями стойкости.

В качестве примера рассмотрим следующую конструкцию, построенную согласно (2):

$$g(x) = x_1 x_4 x_6 x_8 \oplus x_1 x_6 x_7 x_8 \oplus x_1 x_2 x_6 \oplus x_1 x_2 x_7 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_6 \oplus x_1 x_4 x_7 \oplus \\ \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_8 \oplus x_1 x_7 x_8 \oplus x_4 x_6 x_8 \oplus x_2 x_6 \oplus x_3 x_4 \oplus x_5 x_6 \oplus x_7 x_8 \oplus x_2,$$

на основе бент-функций:

$$f_1(x) = x_3 x_4 \oplus x_5 x_6 \oplus x_7 x_8 \oplus x_4 x_6 x_8; \\ f_2(x) = x_3 x_4 \oplus x_5 x_6 \oplus x_7 x_8 \oplus x_4 x_6 x_8 \oplus x_6 \oplus 1; \\ f_3(x) = x_3 x_6 \oplus x_4 x_7 \oplus x_5 x_8 \oplus x_6 x_7 x_8; \\ f_4(x) = x_3 x_6 \oplus x_4 x_7 \oplus x_5 x_8 \oplus x_6 x_7 x_8 \oplus x_7 \oplus 1$$

над V_8 , и конструкцию, построенную согласно (4):

$$g(x) = x_1 x_4 x_6 x_8 \oplus x_1 x_3 x_5 x_7 \oplus x_2 x_4 x_6 x_8 \oplus x_2 x_3 x_5 x_7 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_6 \oplus x_1 x_4 x_7 \oplus \\ \oplus x_1 x_5 x_6 \oplus x_1 x_5 x_8 \oplus x_1 x_7 x_8 \oplus x_2 x_3 x_4 \oplus x_2 x_3 x_6 \oplus x_2 x_4 x_7 \oplus x_2 x_5 x_6 \oplus x_2 x_5 x_8 \oplus$$

$\oplus x_2x_7x_8 \oplus x_3x_5x_7 \oplus x_1x_7 \oplus x_2x_7 \oplus x_3x_6 \oplus x_4x_7 \oplus x_5x_8 \oplus x_1 \oplus x_2 \oplus x_7 \oplus I$,
на основе бент-функций:

$$f_1(x) = x_3x_4 \oplus x_5x_6 \oplus x_7x_8 \oplus x_4x_6x_8; f_2(x) = x_3x_6 \oplus x_4x_7 \oplus x_5x_8 \oplus x_3x_5x_7$$

и аффинной функции $h = x_7 \oplus I$.

Приведенные функции являются сбалансированными, обладают нелинейностью $N_g=240$. Функция, построенная в соответствии с (2), имеет алгебраическую степень $\deg(g) = 4$, максимальной алгебраической степени достигают координаты x_1, x_4, x_6, x_7, x_8 : $\deg(g) = \deg(g, x_i) = \deg(g, x_4) = \deg(g, x_6) = \deg(g, x_7) = \deg(g, x_8) = 4$. Функция, построенная в соответствии с (4), имеет алгебраическую степень $\deg(g) = 4$, максимальной алгебраической степени достигают все координаты x_i : $\deg(g) = \deg(g, x_i) = 4, i = 1, \dots, 2k$.

Таким образом, представленный метод гарантированно представляет функции с контролируемой алгебраической степенью каждой координаты. Достижение максимальной алгебраической степени (алгебраической степени функции) каждой координаты осуществляется за счет использования нелинейных слагаемых $x_2 x_4 \dots x_{2k}$ и $x_3 x_5 \dots x_{2k+1}$, содержащих все используемые координаты над V_{2k+1} , и использования нелинейных слагаемых $x_3 x_5 \dots x_{2k-1}$ и $x_4 x_6 \dots x_{2k}$, также содержащих все используемые координаты над V_{2k} . Выполнение процедуры конкатенации булевых функций с помощью предложенных выражений позволяет сократить время, необходимое для построения высоконелинейных сбалансированных булевых функций над V_{2k} в 2 раза за счет построения двух бент-функций вместо четырех согласно (2), и повысить стойкость к атаке криптоанализа методом дифференциалов высших порядков за счет контроля алгебраической степени каждой координаты.

ЛИТЕРАТУРА

1. B.Preenel, R.Govaerts, J.Vandewalle. Boolean functions satisfying high order propagation criteria. In *Advances in Cryptology – EUROCRYPT'91*, vol.547, *Lecture Notes in Computer Science*, Springer-Verlag, pp.141-152, 1991.
2. J.Seberry, X.M.Zhang, Y.Zheng. Highly Nonlinear Balanced Boolean Functions Satisfying High Degree Propagation Criterion. In *Advances in Cryptology – EUROCRYPT'93*, vol.765, *Lecture Notes in Computer Science*, Springer-Verlag, pp.153 – 167, 1994.

Поступила 2.12.2002

ИЗБЕНКО Юрий Анатоліевич, ад'юнкт Харківського військового університету. В 1998 году окончил ХВУ. Область научных интересов – криптографическая защита информации.

ИВАШКИН Александр Викторович, старший научный сотрудник научно-исследовательской лаборатории Харківського військового університету. В 1997 году окончил ХВУ. Область научных интересов – криптографическая защита информации.