УДК 681.3.06

МЕТОД ПОСТРОЕНИЯ ВЫСОКО НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

А.А.Кузнецов, Ю.А. Избенко, А.А. Юкальчук
(Харьковский университет Воздушных Сил им. И. Кожедуба)

Исследуются методы построения нелинейных преобразований для симметричных криптоалгоритмов. Предлагается метод построения сбалансированных высоко нелинейных булевых функций, удовлетворяющих строгому лавинному эффекту.

нелинейные преобразования для симметричных криптоалгоритмов

Постановка проблемы в общем виде и анализ литературы. Анализ критериев и показателей эффективности криптографических функций [1, 2] показывает, что наиболее обоснованным подходом к описанию нелинейных преобразований симметричных криптоалгоритмов является аппарат нелинейных булевых функций [3, 4] основанный на развитом математическом аппарате булевой алгебры.

Основные показатели эффективности нелинейных преобразований выражаются в терминах булевых функций как показатели сбалансированности, нелинейности, корреляционного иммунитета, распространения, алгебраической степени. При этом под показателем нелинейности N_f понимается минимальное расстояние Хэмминга между последовательностью функции f и последовательностями всех аффинных функций над $GF(2^n)$:

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

где φ – множество аффинных функций.

Для произвольной функции f нелинейность N_f над $GF(2^n)$ может достигать:

$$N_f \le 2^{n-1} - 2^{n/2-1}. \qquad (1)$$

© А.А.Кузнецов, Ю.А. Избенко, А.А. Юкальчук

В [5, 6] теоретически обоснована возможность построения булевых функций, достигающих предельного показателя нелинейности для сбалансированных функций:

$$N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t,\ n = 4t, \qquad (2)$$

удовлетворяющих строгому лавинному критерию и имеющих высокую алгебраическую степень, равную deg(f) = n – 1, где n – размерность векторного пространства. **Целью данной статьи** является разработка метода построения булевых функций, удовлетворяющих перечисленным показателям и критериям эффективности.

Разработка метода построения высоко нелинейных булевых функций. Предлагаемый метод построения высоко нелинейных булевых функций является дальнейшим развитием эвристического метода модификации с применением процедур систематического конструирования и сочетает в себе конструктивные подходы обоих методов. Данный метод основан на использовании свойств ортогональных массивов, отличается от известных введением дополнительных процедур восстановления и модификации полиномиальных форм булевых функций, и позволяет строить нелинейные булевы функции с высокими показателями стойкости.

Предлагаемый метод структурно состоит из трех этапов.

- На *первом этапе* используется метод модификации Себерри-Чжаня [5], позволяющий получить высоко нелинейную последовательность

$$\xi = \varepsilon_0 \varepsilon_1 \cdots \varepsilon_{2^n - 1},$$

где n – размерность векторного пространства.

Согласно метода модификации конкатенируются строки матрицы Адамара H_n в единую последовательность, в результате чего получают бент-последовательность, т.е. последовательность, обладающую максимально возможной нелинейностью. Полученная последовательность является исходным материалом для получения высоко нелинейной сбалансированной последовательности. Результатом этого этапа являются сбалансированные высоко нелинейные последовательности ξ. Показатель нелинейности последовательности ξ удовлетворяет условию

$$N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t,\ n = 4t,$$

где n – размерность векторного пространства.

- На *втором этапе* используется процедура восстановления образующего полинома по выходной последовательности ξ. Использование данной процедуры позволяет по известной последовательности $\xi = \varepsilon_0 \varepsilon_1 \cdots \varepsilon_{2^n - 1}$ восстановить исходную полиномиальную форму булевой функции

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

путем решения системы линейных уравнений

$$\begin{cases} a & = \varepsilon_0; \\ a+b & = \varepsilon_1; \\ a+c & = \varepsilon_2; \\ a+b+c+d & = \varepsilon_3; \\ \vdots & \vdots \\ a+b+c+d+\ldots+z & = \varepsilon_{2^n-1}, \end{cases}$$

где $B = \{a,b,c,d,\ldots,z\}$ – некоторый алфавит, мощность которого $|B| = 2^n-1$.

Данная система может быть решена матричным способом

$$[abcd..z] = [\varepsilon_0 \varepsilon_1 \varepsilon_2 \varepsilon_3 \cdots \varepsilon_{2^n}] \begin{bmatrix} \ell_{11} & \ell_{12} & \ell_{13} & \cdots & \ell_{1,2^n} \\ \ell_{21} & \ell_{22} & \ell_{23} & \cdots & \ell_{2,2^n} \\ \vdots & \vdots & \vdots & & \\ \vdots & \vdots & \vdots & & \\ \ell_{2^n,1} & \ell_{2^n,2} & \ell_{2^n,3} & \cdots & \ell_{2^n,2^n} \end{bmatrix}^{-1},$$

где матрица

$$C = \begin{bmatrix} \ell_{11} & \ell_{12} & \ell_{13} & \cdots & \ell_{1,2^n} \\ \ell_{21} & \ell_{22} & \ell_{23} & \cdots & \ell_{2,2^n} \\ \vdots & \vdots & \vdots & & \\ \vdots & \vdots & \vdots & & \\ \ell_{2^n,1} & \ell_{2^n,2} & \ell_{2^n,3} & \cdots & \ell_{2^n,2^n} \end{bmatrix}$$

представлена в виде 2^n строк, каждая из которых является таблицей истинности одной из возможной функций, представленных в мономиальной форме:

$$\{1, x_1, x_2, x_1x_2, x_3, x_1x_3, x_2x_3, x_1x_2x_3, x_4, \ldots\}.$$

Полученные в ходе решения ненулевые значения

$$e_i,\ e_i \in A\{a,b,c,d,\ldots,z\},$$

отождествляются с соответствующими мономами

$$m_i,\ m_i \in M\{1, x_1, x_2, x_1x_2, x_3, x_1x_3, x_2x_3, x_1x_2x_3, x_4, \ldots\}.$$

Сумма полученных мономов представляет собой исходную полиномиальную форму булевой функции, сгенерировавшей выходную последовательность ξ.

- На *третьем,* заключительном *этапе*, используется процедура модификации полиномиальной формы булевой функции f(x), позволяющая при сохранении основных показателей стойкости нелинейного преобразования (сбалансированности и нелинейности) путем применения аффинных преобразований f(xA) изменить вид образующего полинома

$$f^*(x) = f(xA),$$

где A – специальным образом подобранная ортогональная матрица, что позволит улучшить динамические свойства нелинейного преобразования.

Действительно, согласно [1, 2], сбалансированность, нелинейность и количество векторов, удовлетворяющих критерию распространения, являются инвариантными относительно аффинного преобразования координат. Это свидетельствует о том, что степень критерия распространения может быть улучшена путем соответствующим образом подобранного аффинного преобразования координат.

Формирование матрицы *A* осуществляется следующим образом:

– проверяется, удовлетворяет ли функция f(x) критерию распространения относительно вектора a_i, $a_i \in V_n$, $i = 0, \ldots, 2^n - 1$;

– из множества всех векторов, относительно которых f(x) удовлетворяет критерию распространения, формируется несингулярная матрица $A_{n \times n}$.

Далее каждому x_i, $i = 1, \ldots, n$, полиномиальной формы функции f(x) согласно матрице A ставится в соответствие сумма ненулевых элементов x_j i-го столбца, $j = 1, \ldots, n$. После окончания процедуры постановки соответствия

$$x_i \leftrightarrow \Sigma\, x_j,\ x_j \neq 0,$$

осуществляется процедура аффинных преобразований путем подстановки в полиномиальную форму вместо каждого x_i соответствующей ему суммы x_j с последующим приведением подобных. Другими словами, осуществляется операция f*(x) = f(xA).

Полученная в результате аффинных преобразований функция f*(x) является сбалансированной, имеет нелинейность, равную нелинейности функции f(x), и удовлетворяет критерию распространения первой степени (строгому лавинному критерию).

Выводы. Таким образом, использование разработанного метода построения булевых функций позволяет формировать нелинейные булевы функции с высокими показателями стойкости: данные функции будут сбалансированными, обладать максимально достижимым показателем нелинейности (для сбалансированных функций) $N_f \geq 2^{4t-1} - 2^{2t-1} - 2^t$, n = 4t, удовлетворять строгому лавинному критерию и иметь высокую алгебраическую степень, равную deg(f) = n – 1, где n – размерность векторного пространства.

Перспективным направлением дальнейших исследований является построение булевых функций в соответствии с разработанным методом, исследование дополнительных показателей стойкости формируемых нелинейных преобразований (коэффициент равномерной минимизации корреляции и абсолютное значение корреляции функции).

ЛИТЕРАТУРА

1. *Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Advances in Cryptology – EUROCRYPT'89. – Lecture Notes in Computer Science, Springer-Verlag, 1990. – Vol. 434. – P. 549-562.*
2. *Fuller J., Millan W. On linear redundancy in S-boxes // Proceedings of Fast Software Encryption – FSE'03 (T. Johansson, ed.), Lecture Notes in Computer Science, Springer-Verlag, 2003. – Earlier version available at http://eprint .iacr.org/2002/111/.*
3. *Кузнецов А.А., Избенко Ю.А., Юкальчук А.А. Анализ известных методов построения высоко нелинейных булевых функций // Вісник НТУ "ХПІ": Збірник наукових праць. – Х.: НТУ "ХПІ", 2004. – № 18. – С. 91-96.*
4. *Потий А.В., Избенко Ю.А. Обоснование выбора метода построения криптографически стойких булевых функций // Радиотехника. – Х.: ХТУРЭ, 2002. – Вып. 24. – С. 97-102.*
5. *Кузнецов А.А., Избенко Ю.А., Юкальчук А.А. Теоретическое обоснование возможности разработки комбинированного метода построения высоко нелинейных булевых функций // Вісник НТУ "ХПІ": Збірник наукових праць. – Х.: НТУ "ХПІ", 2004. – № 19. – С. 115-120.*
6. *Кузнецов О.О., Ізбенко Ю.А., Юкальчук А.А. Метод побудови високо нелінійних булевих функцій // IV науково-технічна конференція молодих вчених Харківського військового університету 16-17 квітня 2004 р. – Х.: ХВУ, 2004. – С. 60.*

Поступила 3.04.2006

Рецензент: доктор технических наук, профессор Ю.В. Стасев,
Харьковский университет Воздушных Сил им. И. Кожедуба.