УДК 681.3.06

КРИТЕРИИ И ПОКАЗАТЕЛИ ЭФЕКТИВНОСТИ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ СИММЕТРИЧНЫХ КРИПТОАЛГОРИТМОВ

А.А. Юкальчук
(Харьковский университет Воздушных Сил им. И. Кожедуба)

Анализируются критерии и показатели эффективности нелинейных преобразований задаваемых аппаратом булевых функций. Исследуется их возможности для адекватной оценки эффективности нелинейных узлов завешивания симметричных криптоалгоритмов. Теоретически обосновывается показатель равномерности минимизации корреляции булевых функций.

критерии, эффективность, нелинейные преобразования, симметричные криптоалгоритмы

Постановка проблемы в общем виде и анализ литературы. Современное развитие информационно-телекоммуникационных систем выдвигает высокие требования к безопасности информационных технологий. Эффективным и наиболее распространенным механизмом обеспечения безопасности являются симметричные криптоалгоритмы.

В соответствии с основными положениями теории секретных систем [1] большинство симметричных криптоалгоритмов строится по принципу многократного выполнения примитивных криптографических преобразований (замешивания и рассеивания), которые реализуются блоками нелинейных (S-box) и линейных (P-box) преобразований [2 – 3]. В классической интерпретации нелинейные узлы замешивания представимы в виде некоторой совокупности специальным образом подобранных нелинейных булевых функций [2 – 4]. Как следствие, эффективность нелинейных преобразований обсуждается в терминах нелинейных булевых функций. Актуальным направлением исследований является анализ и обоснование критериев и показателей их эффективности.

Анализ критериев и показателей эффективности нелинейных преобразований. В настоящее время основными показателями эффективности нелинейных преобразований являются: сбалансированность выходной последовательности, нелинейность функции преобразования, корреляционный иммунитет, критерий распространения, алгебраическая степень функции. Введем основные понятия и определения [4 – 6].

Булевой функцией f от n переменных является функция, осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов $x = (x_1, \ldots, x_n)$ длины n в поле GF(2). Обычно булевы функции представляются в ал-

гебраической нормальной форме и рассматриваются как сумма произведений составляющих координат. Поле $GF(2^n)$ состоит из 2^n векторов α_i: $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1),\ldots,$ $\alpha_{2^n-1} = (1,\ldots,1,1)$, $\alpha_i \in V_n$, где V_n – векторное пространство в $GF(2^n)$.

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.

Эквивалентное определение сбалансированности [4]: функция f над $GF(2^n)$ является сбалансированной, если ее выходные значения являются равновероятными

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

Аффинной функцией f называется функция вида $f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$, где a_j, $c \in GF(2)$, $j = 1, 2,\ldots, n$. 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 N_f – минимальное расстояние Хэмминга N_f между функцией f и всеми аффинными функциями 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

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

Функция f обладает корреляционным иммунитетом порядка k, если выходная последовательность функции $y \in Y$ статистически не зависит от любого подмножества из k входных координат

$$\forall \{x_1, \ldots, x_k\}\ P(y \in Y / \{x_1, \ldots, x_k\} \in X) = P(y \in Y).$$

Эквивалентное определение корреляционного иммунитета в терминах преобразования Уолша [4]: функция f над полем $GF(2^n)$ имеет корреляционный иммунитет порядка k, КИ(k), если ее преобразование Уолша удовлетворяет равенству $F(\omega) = 0$ для всех $\omega \in V_n$ таких, что $1 \le W(\omega) \le k$

$$\forall \omega \in V_n \quad F(\omega) = 0 \quad КИ(f) = k$$

Преобразование Уолша $F(\omega)$ функции f над полем $GF(2^n)$ определяется как принимающая действительные значения функция

$$F(\omega) = 2^{-n} \sum\nolimits_x (-1)^{f(x) \oplus \langle \omega, x \rangle},$$

где $\omega \in V_n$, $f(x)$, $\langle \omega,x \rangle \in N$ ($\langle \omega,x \rangle$ – скалярное произведение $w_1x_1 \oplus \ldots \oplus w_nx_n$).

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

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

$$P(f(x) = f(x \oplus \alpha)) = 0{,}5;$$

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

$$P(f(x) = f(x \oplus \alpha)) = 0{,}5 \quad \forall \alpha : 1 \le W(\alpha) \le k.$$

Алгебраическая степень deg(f) является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме.

Коэффициент корреляции функции со множеством всех аффинных функций определяется как

$$c_i(f, L_w) = 2^{-n} \sum_x (-1)^{f(x)} (-1)^{wx} = 2^{-n} \hat{F}(w). \qquad (2)$$

Функция f над $GF(2^n)$ называется бент-функцией, если

$$2^{-n/2} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1 \qquad (3)$$

для всех $\beta \in V_n$.

Обоснование показателя равномерности минимизации корреляции булевых функций. Известно [4], что верхней границы нелинейности (1) над полем $GF(2^n)$ могут достигать только бент-функции (3). Известно также [3, 4], что при конструировании нелинейных функций разработчики стараются равномерно минимизировать корреляцию данных функций со множеством всех афинных функций, поскольку сумма всех коэффициентов корреляции $c_i(f, L_w)$ (3) всегда будет равняться 1

$$\sum_i c_i \ (f, L_w) = 1. \qquad (4)$$

Анализ выражения (4) позволяет сделать следующие выводы:

– суммарная корреляция не зависит от выбора функции f;

– нулевая корреляция с некоторыми линейными функциями (фазами) влечет за собой более высокую корреляцию с остальными линейными функциями (фазами).

Очевидно естественное требование к нелинейному преобразованию – равномерная минимизация корреляции. Несмотря на очевидность данного условия, до недавнего времени не существовало инструментария для оценки равномерности минимизации корреляции функций.

В [5] предложен показатель, позволяющий оценить степень равномерности минимизации корреляции нелинейной функции. Авторы исходили из того, что на практике равномерная минимизация корреляции достигается выбором такой функции, которая по своим показателям была

как можно ближе к бент-функции, поскольку именно бент-функции имеют минимальные и равномерно распределенные коэффициенты корреляции (заметим, что использованию бент-функций в чистом виде мешает их основной недостаток – их последовательности несбалансированны). Как следствие, при оценке степени равномерности минимизации корреляции функции за отправную точку были взяты корреляционные свойства бент-функций как эталона минимальной корреляции с аффинными функциями.

Так, согласно [5], введенный коэффициент равномерной минимизации кросс-корреляции характеризует равномерную минимизацию коэффициентов кросс-корреляции

$$k_{рм} = \frac{k_{гр}}{r \cdot c_{ср}}, \qquad (5)$$

где $k_{гр}$ – граничный коэффициент кросс-корреляции; r – удельный вес ненулевых значений коэффициентов кросс-корреляции; $c_{ср}$ – среднее значение коэффициента кросс-корреляции.

Приведенные значения имеют следующий вид:

$$r = \left| \frac{B}{2^n} - 2^{n-1} \right|; \qquad (6) \qquad c_{ср} = \sum_{i=1}^{2^n} c_i \Big/ 2^n; \qquad (7)$$

$$k_{гр} = \frac{\left|1 - 2^n\right| \cdot (c_n + c_{n+2})}{2} \quad \text{для } V_{n+1} \quad \text{и} \quad k_{гр} = \left|1 - 2^n\right| \cdot c_n \quad \text{для } V_n, \qquad (8)$$

где B – общее количество ненулевых значений коэффициентов кросс-корреляции; c_i – значение коэффициента кросс-корреляции функции со множеством всех афинных функций L_w; c_n – коэффициент корреляции бент-функции над V_n со множеством всех афинных функций над V_n; c_{n+2} – коэффициент корреляции бент-функции над V_{n+2} со множеством всех афинных функций над V_{n+2}.

Основным недостатком рассмотренного показателя является его высокая вычислительная сложность. Действительно, все расчеты по оценке показателя опираются на предварительное вычисление коэффициентов корреляции бент-функций, поскольку основная идея подобной оценки состоит в исследовании уровня снижения степени корреляции исследуемой функции в сравнении со степенью корреляции бент-функции (как функции-эталона).

Предлагается показатель равномерности минимизации корреляции k_{rm}, который не требует предварительных расчетов и использует при вычислениях только лишь сами коэффициенты кросс-корреляции функции с множеством всех афинных функций L_w, и определяется как среднее значение суммы всех ненулевых значений коэффициентов кросс-корреляции. Аналитически оценку показателя равномерности минимизации корреляции запишем в виде выражения

$$k_{rm} = \sum_{1}^{B} c_i(f, L_w) \Big/ B, \qquad (9)$$

где B – общее количество ненулевых значений коэффициентов корреляции.

Анализ выражения (9) показывает, что для оценки введенного показателя необходимо оценить ненулевые коэффициенты корреляции $c_i(f, L_w)$ функции f с множеством всех афинных функций L_w. Такая оценка не предполагает вычисление коэффициентов корреляции бент-функций, а введенный показатель позволяет эффективно использовать его в качестве инструментария для оценки равномерности минимизации корреляции нелинейных булевых функций.

Выводы. В результате проведенных исследований проведен анализ критериев и показателей эффективности нелинейных преобразований задаваемых аппаратом булевых функций, исследованы их возможности для адекватной оценки эффективности нелинейных узлов завешивания симметричных криптоалгоритмов. Теоретически обоснован показатель равномерности минимизации корреляции булевых функций.

Перспективным направлением является исследование эффективности нелинейных преобразований по рассмотренным критериям и показателям, оценка равномерности минимизации корреляции соответствующих булевых функций.

ЛИТЕРАТУРА

1. *Шеннон К. Теория связи в секретных системах // Шеннон К. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы. – 1963. – С. 333-402.*
2. *Youssef M., Tavares S. On some algebraic structures in the AES round function. – [Электр. ресурс]. – Режим доступа: http://eprint.iacr.org/2002/144.*
3. *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. – [Электр. ресурс]. – Режим доступа: http://eprint.iacr.org/2002/111.*
4. *Maier W., Staffelbach O. Nonlinearity criteria for cryptographic functions // Cryptology – EUROCRYPT'89, Vol. 434, Lecture Notes in Computer Science, Springer-Verlag. – 1990. – P. 549-562.*
5. *Потий А.В., Избенко Ю.А. Обоснование выбора метода построения криптографически стойких булевых функций // Радиотехника. – Х.: ХТУРЭ, 2002. – Вып. 24. – С. 97-102.*

Поступила 27.02.2006

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