УДК 681.3.06

А.В. ПОТИЙ, канд. техн. наук, Ю.А. ИЗБЕНКО

ОБОСНОВАНИЕ ВЫБОРА МЕТОДА ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИ СТОЙКИХ БУЛЕВЫХ ФУНКЦИЙ

Введение

При конструировании поточных шифров важной задачей является выбор нелинейной функции, которая отвечает за обеспечение требуемой криптографической стойкости формируемого бегущего ключа.

На сегодняшний день наиболее широкое распространение получили два подхода к построению поточных шифров: нелинейный фильтр-генератор, в котором выход линейного рекуррентного регистра (ЛРР) фильтруется выходной функцией нелинейной фильтрации с целью внесения нелинейности, и комбинирующий генератор, в котором нелинейная функция комбинирует выходы нескольких ЛРР.

В качестве нелинейных функций в основном используются нелинейные булевы функции. Задачей данных функций является противостояние криптографическим атакам с целью недопущения просачивания на выход функции информации о ее входных данных. Функции такого рода называются криптографически стойкими функциями (КСФ), отыскание методов конструирования подобных функций является областью активных исследований в криптографии. При построении и выборе таких функций разработчики используют ряд показателей, основными из которых являются [1-6]: 1)сбалансированность, 2)нелинейность, 3)критерий распространения (строгий лавинный критерий), 4)корреляционный иммунитет, 5)алгебраическая степень.

Целью данной статьи является анализ существующих показателей стойкости КСФ; сравнительная оценка на основе проведенного анализа трех классов функций, используемых при построении КСФ, методы построения которых описаны в [1-6]: корреляционно-иммунных функций, эластичных функций, булевых функций на основе бент-функций; формулирование рекомендаций относительно использования основных показателей стойкости и выбора класса методов для построения КСФ. Вводится дополнительный показатель стойкости булевых функций.

1. Основные показатели стойкости криптографически стойких функций

Как указывалось выше, при построении и выборе булевых функций основными показателями стойкости являются:

1. Сбалансированность.
2. Нелинейность.
3. Критерий распространения (строгий лавинный критерий).
4. Корреляционный иммунитет.
5. Алгебраическая степень.

В случае использования корреляционно-иммунных и эластичных функций используются показатели 1, 2, 4, 5, в случае использования булевых функций на основе бент-функций используются показатели 1, 2, 3, 5.

Для дальнейшего рассмотрения вопроса введем некоторые понятия и определения.

Определение 1. Пусть f является функцией на V_n, $V_n=(0,1)^n$, где $\alpha_0=(0,\ldots,0,0)$, $\alpha_1=(0,\ldots,0,1),\ldots,$ $\alpha_{2^n-1}=(1,\ldots,1,1)$ – все векторы на V_n. Тогда (1,-1)-последовательность, определенная как $((1)^{f(\alpha_0)}, (1)^{f(\alpha_1)},\ldots, (1)^{f(\alpha_{2^n-1})})$, называется *последовательностью* функции f.

(0,1)-последовательность, определенная как $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$, называется *таблицей истинности* функции f.

Пример 1. Пусть $f = x_1x_2x_3 \oplus x_1x_3 \oplus x_2 \oplus x_3 \oplus 1$ на V_3.

Тогда $V_3=(0,1)^3$, где $\alpha_0=(0,0,0)$, $\alpha_1=(0,0,1)$, $\alpha_2=(0,1,0)$, $\alpha_3=(0,1,1)$, $\alpha_4=(1,0,0)$, $\alpha_5=(1,0,1)$, $\alpha_6=(1,1,0)$, $\alpha_7=(1,1,1)$ – все векторы на V_n.

Таблица истинности функции f: $f(000)=1$, $f(001)=0$, $f(010)=0$, $f(011)=1$, $f(100)=1$, $f(101)=1$, f(110)=0, f(111)=1. Последовательность функции f: -1,1,1,-1,-1,1,-1.

Определение 2. Функция f на V_n является *сбалансированной* функцией, если ее таблица истинности (последовательность) содержит 2^{n-1} нулей / единиц (единиц / минус единиц).

Пример 2. Пусть $f = x_1x_2 \oplus x_3$ на V_3. Тогда данная функция сбалансирована, т.к. ее таблица истинности имеет вид 0,1,0,1,0,1,1,0 и содержит $2^{3-1} = 4$ нулей / единиц.

Сбалансированность функции является важным показателем, поскольку одним из требований, предъявляемым к поточным шифрам, являются хорошие статистические свойства шифрующей гаммы. Несоблюдение данного критерия делает криптосистему уязвимой к статистическим атакам.

Определение 3. Аффинной функцией f на V_n является 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 $c = 0$.

Пример 3. Аффинная функция на V_3 $f_1 = x_3 \oplus x_1 \oplus 1$, линейная – $f_2 = x_3 \oplus x_1$.

Определение 4. Криптографически слабыми функциями являются аффинные (линейные) функции и функции с линейной структурой, а также нелинейные функции, которые могут быть сведены к вышеназванным функциям с помощью аффинных преобразований.

Определение 5. *Весом Хэмминга* вектора α, обозначаемым как $W(\alpha)$, является количество единиц в векторе. Для данных функций f и g *расстоянием Хэмминга* является $d(f,g) = W(f(x \oplus g(x))$, где $x=(x_1, x_2, \ldots, x_n) \in (0,1)$.

Пример 4. Для $\alpha = (101)$ $W(\alpha) = 2$.

Для $f(x) = x_1x_2$ и $g(x) = x_1 \oplus x_2$ $d(f,g) = W(x_1x_2 \oplus x_1 \oplus x_2) = 3$.

Определение 6. *Нелинейность функции* f -- минимальное расстояние Хэмминга N_f между функцией f и всеми криптографически слабыми функциями на V_n:

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

где φ - множество криптографически слабых функций.

Для произвольной функции f нелинейность N_f на V_n может достигать [5]:

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

Нелинейность функции является важным критерием, поскольку несоблюдение данного критерия делает возможным проведение корреляционных атак, использующих корреляцию данной функции со множеством криптографически слабых функций. При построении КСФ необходимо обеспечить ее минимальную корреляцию со множеством всех криптографически слабых функций, т.е. стремиться, чтобы нелинейность данной функции стремилась к верхней границе нелинейности, определенной в (1).

Определение 7. Пусть f - функция на V_n. Тогда говорят, что f удовлетворяет

1. *критерию распространения относительно вектора* α, *КР(*α*),* если функция $f(x) \oplus f(x \oplus a)$ является сбалансированной, где $x = (x_1,x_2,\ldots,x_n)$ на V_n.
2. *критерию распространения степени k, КР(k),*если удовлетворяется критерий распространения относительно всех векторов $\alpha \in V_n$ при $1 \le W(\alpha) \le k$. При этом функция f является совершенно нелинейной.
3. *строгому лавинному критерию, СЛК,* если f удовлетворяет критерию распространения степени 1.

Пример 5. Пусть $f = x_1x_2 \oplus x_3$ на V_3. Пусть $a = (1,1,0)$, тогда

$$f(x) \oplus f(x \oplus a) = (x_1x_2 \oplus x_3) \oplus ((x_1 \oplus 1)(x_2 \oplus 1) \oplus x_3) = x_1 \oplus x_2 \oplus 1$$

является сбалансированной и удовлетворяет критерию распространения относительно вектора $a = (1,1,0)$.

Пример 6. Пусть $f = x_1 \oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5$ на V_5. Пусть $a = (0,0,1,0,0)$. тогда

$$f(x) \oplus f(x \oplus a) = x_3x_4x_5 \oplus (x_3 \oplus 1)\, x_4x_5 = x_4x_5$$

не является сбалансированной и не удовлетворяет критерию распространения относительно вектора $a = (0,0,1,0,0)$.

Следует отметить, что по сути своей критерий распространения связан с корреляционными свойствами последовательности. Критерий распространения характеризует зависимость выходных значений нелинейной функции от входных векторов с различным весом Хэмминга. Таким образом, критерий распространения является важным конструктивным критерием, пренебрежение которым делает возможным применение статистических атак.

Определение 8. Пусть f - функция на V_n. Тогда говорят, что к*орреляционный иммунитет порядка k, КИ(k),* удовлетворяется в том случае, если случайная величина Y, порождаемая функцией f, статистически не зависит от любого подмножества $X_{i_1}, \ldots X_{i_k}$ ее k входных координат, где X - случайная величина, принимающая значения $x \in V_n$ с равномерной вероятностью 2^{-n}, X_i – случайная величина, соответствующая значению i-ой координаты $x_i \in GF(2)$ [1]. Эквивалентное определение корреляционного иммунитета в терминах преобразования Уолша : функция f над V_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 $1 \le W(\omega) \le k$. Преобразование Уолша $F(\omega)$ функции f над V_n определяется как принимающая действительные значения функция

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

где $\omega \in V_n$. Отметим, что в данной сумме $f(x)$ и $\langle \omega, x \rangle$ рассматриваются как функции, принимающие действительные значения.

Функция, обладающая корреляционным иммунитетом порядка k, называется корреляционно-иммунной k-го порядка. Корреляционно-иммунные функции являются частным случаем эластичных функций.

Как будет показано ниже, данный критерий, по мнению авторов, не является конструктивным.

Определение 9. Алгебраическая степень $\deg(f)$ является степенью самого длинного слагаемого функции, представленной в алгебраической нормальной форме. Высокая алгебраическая степень позволяет противостоять различным аналитическим атакам, призванным свести данную функцию к криптографически слабой.

Пример 7. Пусть $f = x_1 \oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_4x_5 \oplus 1$ на V_5. Тогда $\deg(f) = 3$.

2. Сравнительная оценка используемых классов КСФ

Рассмотрев показатели стойкости КСФ, обратимся к цели нашей статьи. Поскольку наиболее распространенной и эффективной атакой на поточные шифры являются корреляционные атаки, целью которых является выявить зависимость выходной гаммы нелинейной функции от поступающих на нее данных, наше внимание привлек тот факт, что любая булева функция f имеет определенную корреляцию с некоторыми линейными функциями ℓ_i из множества всех линейных функций L. В [7] вводится коэффициент кросс-корреляции $c(f, \ell_i)$, определенный как

$$c(f, \ell_i) = 2^{-n} F(\omega) = 2^{-n} \sum_x (-1)^{f(x) \oplus \langle \omega, x \rangle}. \quad (3)$$

Суммарная корреляция булевой функции f с множеством линейных функций L имеет вид

$$\sum_L c(f, L)^2 = 1, \quad (4)$$

что демонстрирует тот факт, что корреляция с множеством линейных функций существует всегда независимо от выбора функции f. Как видно из (4), коэффициент кросс-корреляции равен нулю в том случае, если $F(\omega) = 0$. Однако это противоречит идее корреляционно-иммунных (эластичных) функций, согласно которой данные функции имеют нулевую корреляцию с линейными функциями. Следовательно, корреляционный иммунитет не является конструктивным критерием стойкости булевых функций. Согласно [7], для совершенно нелинейных функций $| F(\omega) | = 2^{n/2}$. Следовательно, формула (3) принимает вид

$$c(f, \ell_i) = 2^{-n} F(\omega) = 2^{-n} \cdot 2^{n/2} = 2^{-n/2}, \quad (5)$$

из чего следует сделать вывод, что для всех совершенно нелинейных функций абсолютная величина коэффициента кросс-корреляции – величина постоянная, а значит, данный класс функций имеет минимальную корреляцию с линейными функциями. Кроме того, как видно из (5), при расширении векторного пространства $c(f, L)$ будет стремиться к нулю. Для остальных же булевых функций абсолютная величина коэффициента кросс-корреляции с некоторыми линейными функциями будет выше, чем $2^{-n/2}$. Отметим, что нижняя граница коэффициента кросс-корреляции может достигать нуля, но в силу равенства (4) это неизбежно повлечет за собой увеличение корреляции с другими линейными функциями.

В связи с этим в качестве дополнительного показателя стойкости булевых функций предлагается ввести абсолютное значение кросс-корреляции функции

$$C_f = \max | c(f, \ell_i) |, \quad (6)$$

равное максимальному значению коэффициента кросс-корреляции функции f на V_n, $\ell_l \in L$. Критерием для данного показателя будем полагать минимально возможное значение C_f. При прочих равных показателях стойкости некоторых функций данный показатель позволит нам выбрать функцию, минимально коррелирующую с множеством всех аффинных функций.

Известно [5], что совершенной нелинейностью обладают бент-функции. Функция f на V_n называется бент-функцией, если

$$2^{-n/2} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1 \quad \text{для всех } \beta \in V_n. \quad (7)$$

Помимо этого, они обладают максимальной нелинейностью и максимальным расстоянием до линейных структур. Однако две причины препятствуют использованию бент-функций в чистом виде: их последовательности несбалансированны, что делает их уязвимыми к статистическому анализу; они существуют, согласно (7), лишь на четных векторных пространствах.

В качестве примера рассмотрим три булевы функции (рис.1):

1. Типичная бент-функция $f_1(x) = x_1x_2 \oplus x_3x_4$.
2. Сбалансированная функция, построенная на основе бент-функции $f_1(x)$ согласно [5], $f_2(x) = x_1x_2 \oplus x_3x_4 \oplus x_5$.

3. Корреляционно-иммунная функция 2-го порядка, построенная согласно [2], $f_3(x) = x_1x_4 \oplus x_1x_5 \oplus x_2 \oplus x_3 \oplus x_4$.

На рис. 1 представлено распределение абсолютного значения преобразования Уолша, в табл. 1 приведены расчетные показатели стойкости данных функций.

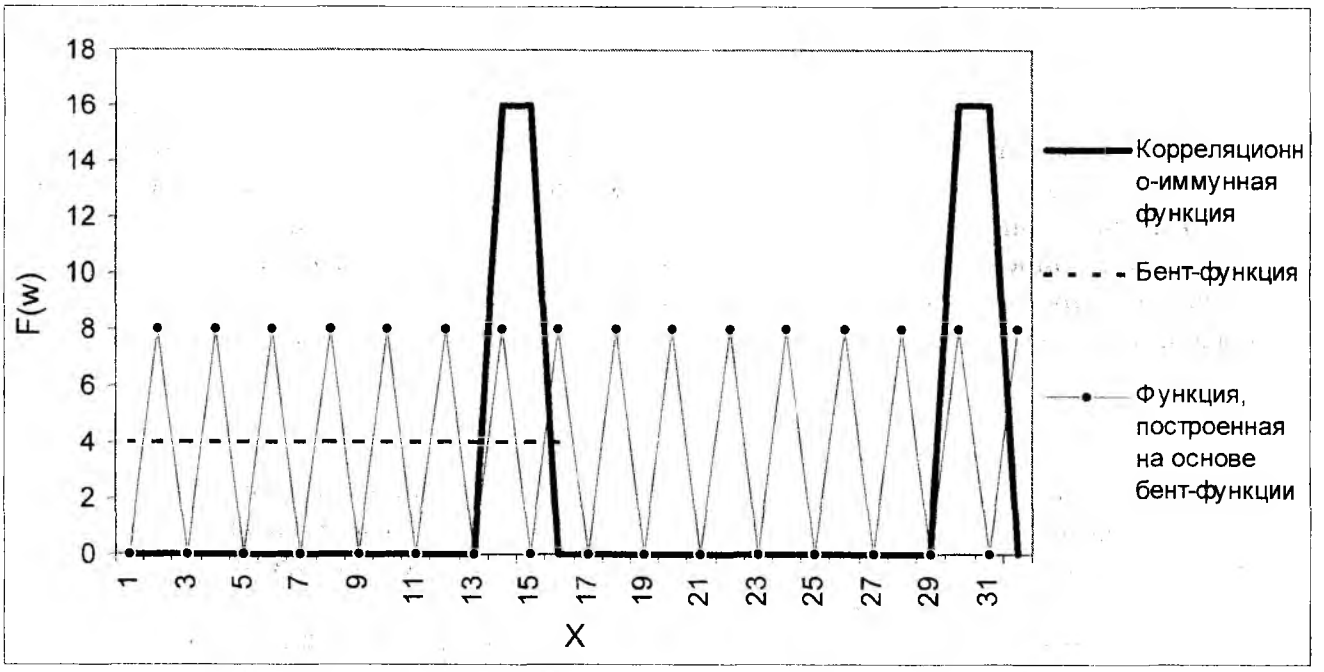

Рис. 1

Таблица 1

	Сбалансированность	N_f		КР(k)	КИ(k)	deg(f)	C_f
		Полученное значение	Верхняя граница				
$f_1(x)$	нет	6	6	4	нет	2	0,25
$f_2(x)$	да	12	12	удовл. всем векторам, кроме (00001)	нет	2	0,25
$f_3(x)$	да	8	12	не удовл. $W(\alpha)$=1,2,3,4, удовл $W(\alpha)$=5	2	2	0,5

Как видно из приведенных результатов, бент-функция $f_1(x)$ имеет в качестве абсолютного значения преобразования Уолша константу, равную $|F(\omega)| = 2^{n/2} = 2^{4/2} = 4$; у функции $f_2(x)$, построенной на основе данной бент-функции, значения $|F(\omega)|$ имеют диапазон 0÷8; у корреляционно-иммунной функции $f_3(x)$ значения $|F(\omega)|$ имеют диапазон 0÷16, нулевая корреляция корреляционно-иммунной функции с некоторыми линейными функциями влечет более высокую корреляцию с остальными линейными функциями. Все функции обладают высокой нелинейностью, причем бент-функция достигает верхней границы нелинейности на заданном пространстве. Приведенные функции не являются криптографически стойкими, однако служат хорошим наглядным материалом для подтверждения наших идей.

Таким образом, на основе выше изложенного, наиболее предпочтительным классом функций, используемых для построения КСФ, является класс совершенных нелинейных функций (бент-функций), так как данный класс функций обладает привлекательными криптографическими свойствами. Из этого следует, что в качестве методов построения КСФ

рекомендуется использовать класс методов, конструирующих высоконелинейные сбалансированные функции на основе бент-функций, так как данный класс методов изначально "стартует" с хорошими криптографическими свойствами, имея в качестве недостатка лишь несбалансированность. При отборе же КСФ на заданном векторном пространстве, помимо основных конструктивных критериев, следует выбирать f насколько возможно близкой к совершенной нелинейной функции с равномерно минимизированной кросс-корреляцией и с минимально-возможным абсолютным значением C_f. Использование классов методов, генерирующих корреляционно-иммунные и эластичные функции, менее предпочтительно, однако они также дают высокие показатели криптостойкости.

Список литературы: **1.** P.Camion, C. Carlet, P. Charpin and N. Sendrier, "On correlation-immune functions," in Lecture Notes in Computer Science vol.576; Advances in Crypology: Crypto '91 3roc., pp 87-100. Berlin: Springer-Verlag, 1991. **2.** J. Seberry, X.M. Zhang and Y. Zheng, "On Constructions and Nonlinearity of Correlation Immune Functions" In T. Helleseth, editor, Advances in Cryptology - Eurocrypt '93, pages 181-199, Springer-Verlag, Berlin, 1994. **3.** P. Camion and A. Canteaut "Construction of t-Resilient Functions over a Finite Alphabet", in Lecture Notes in Computer Science; Advances in Crypology: Eurorypt '96 Proc.,Springer-Verlag 1996, pp. 283-293. **4.** X.-M. Zhang and Y.Zheng, "On nonlinear resilient functions," Advances in Cryptology - Eurocrypt '95, Lecture Notes in Computer Science, vol.921, L.C. Guillou ed., Springer-Verlag, pp. 274-288, 1995. **5.** Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng. Nonlinearity and Propagation Characteristics of Balanced Boolean Functions. Information and Computation, Vol. 119, No 1, pp 1-13, 1995. **6.** B. Preneel, R. Govaerts, and J. Vandewalle, "Boolean functions satisfying higher order propagation criteria" in Lecture Notes in Computer Science 547; Advances in Cryplology: Proc. Eurocrypt'91,1991, pp. 141-152. Berlin: Springer-Verlag. **7.** W.Meier, O.Staffelbach. Nonlinearity criteria for cryptographic functions. Lecture Notes in Computer Science 434, pp.549-562, Springer-Verlag, 1990.

Харьковский военный университет

Харьковский национальный

университет радиоэлектроники

Поступила в редколлегию 19.03.02