УДК 621.34

УСЛОВИЯ ПОСТРОЕНИЯ НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

д.т.н, проф. Ю.В. Стасев, Ю.А. Избенко, В.Н. Ткаченко, А.А. Смирнов

Рассматривается один из показателей стойкости булевых функций – нелинейность, а также определяются условия построения нелинейных булевых функций.

Наиболее распространенным способом построения поточных шифров является комбинация нескольких регистров сдвига с линейной обратной связью, выходы которых подвергаются преобразованию некоторой криптографически стойкой булевой функцией.

Одним из наиболее весомых показателей стойкости булевых функций является нелинейность. Нелинейность – минимальное расстояние Хэмминга от функции **f** до множества криптографически слабых функций [1]. Нелинейность криптографических булевых функций является фундаментально важным качеством, поскольку данный показатель определяет стойкость метода шифрования.

Целью данной статьи является определение условий построения нелинейных булевых функций для поточных шифров.

Введем некоторые определения. Рассматривается $\mathbf{V_m}$ - векторное пространство **m** - грамм с элементами из **GF(2)**. Отметим, что имеется естественное взаимно - однозначное соответствие между векторами из $\mathbf{V_m}$ и целыми числами из $\mathbf{[0, 2^m - 1]}$. Это позволяет упорядочить данные векторы в соответствии с их целочисленными значениями. Для удобства, как $\boldsymbol{\alpha_i}$ будет обозначаться вектор, чье целочисленное представление равно **i**.

Пусть **f** - функция из $\mathbf{V_m}$ в **GF(2)** (или просто функция над $\mathbf{V_m}$). Поскольку **f** может быть выражена как уникальный полином от **m** переменных $\mathbf{x_1, x_2, \ldots, x_m}$, то будем идентифицировать **f** с помощью ее уникального многочлена **f(x)**, где $\mathbf{x = (x_1, x_2, \ldots, x_m)}$. Функция **f** называется *аффинной функцией*, если принимает вид $\mathbf{f(x) = a_1x_1 \oplus \ldots \oplus a_m x_m \oplus c}$, где $\mathbf{a_j, c \in GF(2)}$. В частности, **f** – *линейная функция*, если $\mathbf{c = 0}$.

Таблица истинности функции **f** - это **(0, 1)** - последовательность, задаваемая как $\mathbf{(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^m-1}))}$. *Последовательность функции* **f**, $\boldsymbol{\xi_f}$ - это **(1,-1)** - последовательность, задаваемая как $\mathbf{((-1)^{f(\alpha 0)}, (-1)^{f(\alpha 1)}, \ldots, (-1)^{f(\alpha 2^m - 1)})}$. В случае, если $\boldsymbol{\alpha,\beta} \in \mathbf{V_m}$, то $\mathbf{\langle \alpha,\beta \rangle = a_1b_1 \oplus \ldots \oplus a_m b_m}$, где сложение и умножение выполняются над **GF(2)**.

Если α и β – **(1,-1)** - последовательности, то $\langle \alpha, \beta \rangle = \sum_{i=1}^{m} a_i b_i$, где сложение и умножение выполняется над действительными числами.

Весом Хэмминга $W(\alpha)$ вектора $\alpha \in V_m$ называется число единиц в таблице истинности. Расстояние Хэмминга **d(f, g)** между двумя функциями **f** и **g** на V_m есть вес Хэмминга побитовой суммы последовательностей функций, определяемое как $d(f, g) = W(f(x) \oplus g(x))$, где $x = (x_1, \ldots, x_m)$.

В качестве меры нелинейности функции принимают расстояние до набора криптографически слабых функций: функций, легко вскрываемых методами криптоанализа. Расстояние между двумя двоичными функциями **f** и **g** определяется как

$$d(f, g) = |\{x \in \{0, 1\}^n : f(x) \neq g(x)\}|. \quad (1)$$

Пусть **f** и **g** имеют последовательности $\xi_f = (a_0, \ldots, a_{2^m-1})$ и $\xi_g = (b_0, \ldots, b_{2^m-1})$ соответственно. Согласно (1), расстояние между функциями **f** и **g** определяется как расстояние Хэмминга между функциями: $d(f, g) = W(f(x) \oplus g(x))$. Другими словами, это количество несовпадений соответствующих позиций последовательностей ξ_f и ξ_g: $a_i \neq b_i$. Тогда, если **d(f, g)** – количество несовпадений, то количество совпадений $a_i = b_i$ равно $2^m - d(f, g)$. Дисбаланс между $2^m - d(f, g)$ и **d(f, g)** есть, по определению, произведение последовательностей ξ_f и ξ_g. Тогда:

$$\langle \xi_f, \xi_g \rangle = 2^m - 2d(f, g);$$
$$2d(f, g) = 2^{m-1} - \langle \xi_f, \xi_g \rangle / 2. \quad (2)$$

Таким образом, можно сделать вывод о том, что расстояние Хэмминга между двумя функциями тем больше, чем больше дисбаланс между количеством несовпадений и совпадений в соответствующих позициях $a_i = b_i$ последовательностей функций (таблиц истинности) в сторону несовпадений.

Пример. Пусть $f(x) = x_2$, $g(x) = x_1x_2$, $x \in V_2$; $z(x) = x_1x_2x_3$, $r(x) = x_1 \oplus x_2x_3$, $x \in V_3$. Тогда таблицы истинности и последовательности функций имеют следующий вид:

	f(x)	g(x)	f(x)⊕g(x)	ξ_f	ξ_g
00	0	0	0	1	1
01	1	0	1	-1	1
10	0	0	0	1	1
11	1	1	0	-1	-1

Видно, что **d(f, g) = 1**, **d(z, r) = 5**.

	z(x)	r(x)	z(x)⊕r(x)	ξ_z	ξ_r
000	0	0	0	1	1
001	0	0	0	1	1
010	0	0	0	1	1
011	0	1	1	1	-1
100	0	1	1	1	-1
101	0	1	1	1	-1
110	0	1	1	1	-1
111	1	0	1	-1	1

Аналогично, используя (2), выведем:

$$\mathbf{d(f, g)=2^{2-1} - \frac{1}{2}\langle(1,-1,1,-1)(1,1,1,-1)\rangle = 2- \frac{1}{2}\, 2=1};$$

$$\mathbf{d(z, r)=2^{3-1} - \frac{1}{2}\langle(1,1,1,1,1,1,1,-1)\ (1,1,1,-1,-1,-1,-1,1)\rangle = 4 - \frac{1}{2}\,(-2) = 5}.$$

В качестве показателей, определяющих меру нелинейности функции, в [2] предлагается использовать два показателя: минимальное расстояние до аффинных функций и минимальное расстояние до линейных структур.

Используя преобразование Уолша и теорему Парсеваля, авторы показали, что если **Ă** и **Ł** – множество аффинных функций и множество функций с линейной структурой соответственно, **f** – произвольная функция, то

$$\mathbf{d(f, Ă) \le 2^{\,m-1} - 2^{\,m/2-1}}; \tag{3}$$

$$\mathbf{d(f, Ł) \le 2^{\,m-2}}. \tag{4}$$

В [1] нелинейность $\mathbf{N_f}$ определяется как минимальное расстояние Хэмминга между произвольной функцией **f** и всеми аффинными функциями φ на $\mathbf{V_m}$:

$$\mathbf{N_f = min\ \{d(f, \varphi)\}}\ . \tag{5}$$

Используя теорию адамаровых матриц и теорему Парсеваля, авторы получили ту же верхнюю границу нелинейности, что была получена в [2]:

$$\mathbf{N_f\ \le 2^{\,m-1} - 2^{\,m/2-1}}\ . \tag{6}$$

Очевидно, что использование критериев нелинейности из [2] позволит по сравнению с использованием критерия из [1] избежать использования множества потенциально слабых функций – функций с линейной структурой.

По определению, функция **f(x)** имеет линейную структуру при $\mathbf{a \in F_2^n}$, если существует такое $\mathbf{a \in F_2^n}$, что для всех $\mathbf{x \in F_2^n}$ выполняется либо равенство **f(x) = f(x⊕a)**, либо неравенство **f(x) ≠ f(x⊕a)**. Произвольная функция с линейной структурой не обязательно является аффинной. В качестве примера можно привести нелинейную функцию $\mathbf{f(x) = x_1x_2 \oplus x_2 \oplus x_2x_3}$, имеющую линейную структуру при **a = (1,0,1)**.

В [2] введена идея совершенной нелинейности. По определению, функция является совершенной нелинейной, если

$$\mathbf{(\forall\ a\neq 0)\ \ |\{x\in\{0,1\}^n : f(x) = f(x\oplus a),\ \}| = |\{x\in\{0,1\}^n : f(x) \neq f(x\oplus a),\ \}| = 2^n/2}, \tag{7}$$

т.е., если для каждого ненулевого вектора **a** значения **f(x)** и **f(x⊕a)** совпадают точно для половины аргументов **x** и отличаются для другой по-

ловины. Доказано, что класс функций с такими свойствами совпадает с классом функций, известным в комбинаторике как “бент - функции”. Функция **f** на $\mathbf{V_m}$ называется бент - функцией, если

$$2^{-m/2} \sum_{x \in V_m} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1 \quad \text{для всех } \beta \in \mathbf{V_m}. \qquad (8)$$

Показано, что класс совершенных нелинейных функций (бент - функций) является оптимальным относительно обоих расстояний, при четном **m** они одновременно имеют максимальное расстояние $2^{m-1} - 2^{m/2-1}$ до всех аффинных функций и максимальное расстояние 2^{m-2} до всех функций с линейной структурой.

Как видно из (8), бент - функции существуют лишь при четном **m**. Помимо этого, выходные последовательности таких функций несбалансированы, т.е. нулевое и единичное выходные значения неравновероятны, что делает их уязвимыми к криптоанализу.

Из вышеизложенного следует сделать вывод, что при конструировании криптографически стойких булевых функций с высокой нелинейностью необходимо соблюдение следующих условий:

– в соответствии с (2) отбор функций, последовательности которых имеют максимальное расстояние Хэмминга до множества последовательностей криптографически слабых функций;

– отсев нелинейных функций с линейной структурой;

– использование бент - функций на произвольном пространстве $\mathbf{V_m}$ лишь при четном **m**.

ЛИТЕРАТУРА

1. Seberry J., Zhang X.M. Hadamard Matrices, Bent Functions and Cryptography. – *http:/www.cs.uow.edu.au/people/jennie.*

2. Meier W., Staffelbach O. Nonlinearity criteria for cryptographic functions / Lecture Notes in Computer Science 434. – Springer - Verlag, 1990. – P. 549 - 562.

Поступила в редколлегию 27.08.2001