УДК 681.3.06

А.А. КУЗНЕЦОВ, д-р техн. наук, А.В. КОВАЛЕНКО, канд. техн. наук, С.А. ИСАЕВ

ФОРМИРОВАНИЕ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН С ИСПОЛЬЗОВАНИЕМ НЕДВОИЧНЫХ КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ

Введение

Регулярные нелинейные криптографические функции (узлы замен) симметричных шифров реализуют отображение n-битных блоков входных данных в m-битные выходные блоки: $F: GF^n(2) \to GF^m(2)$. Традиционный подход к описанию, оцениванию и разработке методов синтеза регулярных нелинейных узлов замен состоит в представлении функции F с помощью ее координатных функций, которые задаются в терминах булевой алгебры [1]. В то же время, как показано в [2, 3], построение нелинейных узлов замен с высокими показателями стойкости через итеративное формирование компонентных булевых функций является непрактичным уже при $n = 6$ и вычислительно недостижимым для $n > 6$. Это предполагает обоснование новых подходов к описанию криптографических узлов замен симметричных шифров, исследование математического аппарата оценивания основных показателей стойкости и построение вычислительно эффективных алгоритмов синтеза.

Представление S-блоков через компонентные булевы функции

Введем основные понятия и определения математического аппарата булевой алгебры, используемые в дальнейшем при описании нелинейных узлов замен через компонентные булевы функции и оценке их криптографических свойств.

Булевой функцией $f(x_1,...,x_n)$ от n переменных является функция, осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов $x = (x_1,...,x_n)$ длины n в поле $GF(2)$ [4]. Обычно булевы функции представляются в алгебраической нормальной форме (АНФ), т.е. рассматриваются как сумма произведений составляющих координат:

$$f(x_1,...,x_n) = \lambda_0 + \lambda_1 x_1 + ... + \lambda_n x_n + +\lambda_{12} x_1 x_2 + \lambda_{13} x_1 x_3 + ... + \lambda_{12...n} x_1 x_2 ... x_n, \qquad (1)$$

где $\lambda_0, \lambda_1, ..., \lambda_{12}, ..., \lambda_{12...n}$ – уникальные двоичные константы, а суммирование и умножение производится в двоичном поле $GF(2)$.

Поле $GF(2^n)$ состоит из 2^n векторов $\alpha_i = (\alpha_1^i, \alpha_2^i, ..., \alpha_n^i)$, $\alpha_j^i \in GF(2)$: $\alpha_0 = (0,...,0,0)$, $\alpha_1 = (0,...,0,1)$, …, $\alpha_{2^n-1} = (1,...,1,1)$, $\alpha_i \in V_n$, где V_n – векторное пространство над $GF(2)$.

Таблицей истинности функции f называется (0,1)-последовательность, определенная как [5]:

$$\left(f(x) \middle| x \in GF^n(2)\right) = \left(f(\alpha_0), f(\alpha_1), ..., f(\alpha_{2^n-1})\right).$$

Последовательностью функции f, обозначаемой $\tilde{f}$, называется (1,-1)-последовательность, определенная как [5]:

$$\left((-1)^{f(x)} \middle| x \in GF^n(2)\right) = \left((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, ..., (-1)^{f(\alpha_{2^n-1})}\right).$$

Рассмотрим криптографические свойства функций, реализующих отображения из $GF^n(2)$ в $GF^m(2)$, где $1 \le m \le n$. Пусть M_n^m есть множество таких функций, а B_n есть множество булевых функций от n переменных, то есть функций, реализующих отображения

из $GF^n(2)$ в $GF(2)$. Тогда любую функцию $F \in M_n^m$ можно рассматривать как состоящую из m булевых функций от n переменных, т.е. m-выходных координатных функций из B_n.

В более общем представлении, компонентная функция $F \in M_n^m$ является ненулевой линейной комбинацией ее координатных функций из B_n.

Таким образом, функцию $F: GF^n(2) \to GF^m(2)$ запишем через множество $F = (f_1(x_1,...,x_n),...,f_m(x_1,...,x_n))$, где $f_i(x_1,...,x_n) \in B_n$.

Алгебраическая степень f [5], обозначаемая $\deg(f)$, определяется как максимальная степень многочлена представленного в АНФ.

Важные свойства булевых функций изучаются с использованием преобразования Уолша – Адамара.

Преобразование Уолша – Адамара функции $f(x_1,...,x_n) \in B_n$ есть вещественная функция $\overline{F}(w)$ [5]:

$$\overline{F}(w) = \sum_{x \in GF^n(2)} (-1)^{f(x)+w \cdot x}, \tag{2}$$

где скалярное произведение векторов x и w определяется как $x \cdot w = x_1 w_1 + ... + x_n w_n$.

Булева функция f сбалансирована, если вероятности событий $f(x) = 1$ и $f(x) = 0$ равны. Используя преобразование Уолша – Адамара, условие сбалансированности функции f запишем в виде $\overline{F}(0) = 0$.

Расстояние по Хеммингу между двумя функциями f и g из B_n определяется как:

$$d_H(f,g) = card\left\{x \mid f(x) \neq g(x), x \in GF^n(2)\right\}. \tag{3}$$

Нелинейность $NL(f)$ функции $f(x_1,...,x_n) \in B_n$ определяется как [5]:

$$NL(f) = \min_{g \in A_n} d_H(f,g), \tag{4}$$

где A_n – множество всех аффинных функций от n переменных,

$$A_n = \left\{ a_0 + \sum_{i=1}^{n} a_i x_i \mid a_i \in GF(2), 0 \le i \le n \right\}. \tag{5}$$

С использованием преобразования Уолша – Адамара нелинейность функции f может быть получена следующим образом:

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{w \in GF^n(2)} \left|\overline{F}(w)\right|. \tag{6}$$

Взаимосвязь показателя нелинейности $NL(f)$ функции $f(x_1,...,x_n) \in B_n$ с преобразованием Уолша – Адамара и вывод формулы (6) легко понять, представив выражение (2) в виде матричного умножения последовательности функции $\left((-1)^{f(x)} \middle| x \in GF^n(2)\right)$, на матрицу Уолша – Адамара H_{2^n} порядка 2^n:

$$\left(\overline{F}(w) \middle| w \in GF^n(2)\right) = \left(\sum_{x \in F_2^n} (-1)^{f(x)+w \cdot x} \middle| w \in GF^n(2)\right) = \left((-1)^{f(x)} \middle| x \in GF^n(2)\right) \cdot H_{2^n}$$

(последовательность функции в данном выражении и далее по тексту представляется в виде вектора-строки, образованной элементами этой последовательности).

Итеративное правило построения матрицы H_{2^n} задается выражением

$$H_1 = |1|,\ H_{2^i} = \begin{vmatrix} H_{2^{i-1}} & H_{2^{i-1}} \\ H_{2^{i-1}} & -H_{2^{i-1}} \end{vmatrix},\ i \in N.$$

Каждая строка матрицы Уолша – Адамара соответствует последовательности некоторой аффинной функции $g_i(x_1,...,x_n)$ из A_n с $a_0 = 0$ в общем представлении (5). Строго говоря, полное множество последовательностей всех аффинных функций с $a_0 = 0$ упорядочены по строкам (столбцам) матрицы Уолша – Адамара естественным образом:

$$A'_n = \left\{ \begin{array}{c} g_1(x_1,...,x_n) = 0 \\ g_2(x_1,...,x_n) = x_1 \\ g_3(x_1,...,x_n) = x_2 \\ ... \\ g_{2^n}(x_1,...,x_n) = x_1 + x_2 + ... + x_n \end{array} \right\},$$

где $g_i(x_1,...,x_n)$ – i-я аффинная функция, из упорядоченного подмножества аффинных функций A'_n с $a_0 = 0$ в (5).

Другими словами, последовательность $\left((-1)^{g_i(x)} \middle| x \in GF^n(2)\right)$ i-й аффинной функции из A'_n соответствует i-й строке матрицы Уолша – Адамара и наоборот.

Тогда выполняется равенство

$$\left((-1)^{f(x)} \middle| x \in GF(2)^n\right) \cdot H_{2^n} = \left((-1)^{f(x)} \middle| x \in GF^n(2)\right) \cdot \left(\begin{array}{c} \left((-1)^{g_1(x)} \middle| x \in GF^n(2)\right) \\ \left((-1)^{g_2(x)} \middle| x \in GF^n(2)\right) \\ ... \\ \left((-1)^{g_{2^n}(x)} \middle| x \in GF^n(2)\right) \end{array} \right)^T =$$

$$= \left(\sum_{x \in GF^n(2)} (-1)^{f(x)+g_i(x)} \middle| x \in GF^n(2),\ g_i(x) \in A'_n \right) = \left(\overline{F}(w) \middle| w \in GF^n(2) \right).$$

Например, для $n = 2$ имеем матрицу Уолша – Адамара H_4:

$$H_4 = \begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{vmatrix},$$

причем

$$\left((-1)^{g_1(x)=0} \middle| x \in GF^2(2)\right) = (1,1,1,1);\ \left((-1)^{g_2(x)=x_1} \middle| x \in GF^2(2)\right) = (1,-1,1,-1);$$

$$\left((-1)^{g_3(x)=x_2}\, x \in GF^2(2)\right) = (1,1,-1,-1);\ \left((-1)^{g_4(x)=x_1+x_2}\,\middle|\, x \in GF^2(2)\right) = (1,1,-1,-1)$$

и матричное произведение $\left((-1)^{f(x)}\middle| x \in GF^2(2)\right)\cdot H_4$ соответствует вычислению вектора значений функции $\overline{F}(w)$ для всех $w \in GF^2(2)$.

Выражение для расчета значений коэффициентов преобразования Уолша – Адамара запишем в виде

$$\overline{F}(w) = \sum_{x \in GF^n(2)} (-1)^{f(x)+g_w(x)}\middle| x \in GF^n(2).$$

Максимальное значение коэффициентов преобразования Уолша – Адамара $\max\limits_{w \in GF^n(2)} \overline{F}(w)$ булевой функции $f(x)$ соответствует максимальному коэффициенту корреляции (похожести) последовательности этой функции и последовательностей всех аффинных функций из множества A'_n:

$$\max_{w \in GF^n(2)} \overline{F}(w) = \max_{w \in GF^n(2)} \left(\sum_{x \in GF^n(2)} (-1)^{f(x)+g_w(x)}\middle| x \in GF^n(2) \right) =$$

$$= \max_{w \in GF^n(2)} \begin{pmatrix} card\left\{x \mid f(x) = g_w(x), x \in GF^n(2)\right\} - \\ -card\left\{x \mid f(x) \neq g_w(x), x \in GF^n(2)\right\} \end{pmatrix}.$$

Последовательности аффинных функций с $a_0 = 1$ в (5) соответствуют инверсии (умножению на «-1») последовательностей функций из A'_n, следовательно, максимум модуля коэффициентов преобразования Уолша – Адамара $\max\limits_{w \in GF^n(2)} \left|\overline{F}(w)\right|$ булевой функции $f(x)$ будет соответствовать максимальному коэффициенту корреляции последовательности этой функции и последовательностей всех аффинных функций из множества A_n.

По определению нелинейности из (4) имеем:

$$NL(f) = \min_{g \in A_n} d_H(f,g) = \min_{g \in A_n} card\left\{x \mid f(x) \neq g(x), x \in GF^n(2)\right\}.$$

Поскольку $card\left\{x \mid f(x) = g(x), x \in GF^n(2)\right\} + card\left\{x \mid f(x) \neq g(x), x \in GF^n(2)\right\} = 2^n$ справедливо равенство

$$\max_{w \in GF^n(2)} \left|\overline{F}(w)\right| = \max_{w \in GF^n(2)} \left| \sum_{x \in GF^n(2)} (-1)^{f(x)+g_w(x)}\middle| x \in GF^n(2)\right| =$$

$$= \max_{w \in GF^n(2)} \left| \begin{matrix} card\left\{x \mid f(x) = g_w(x), x \in GF^n(2)\right\} - \\ -card\left\{x \mid f(x) \neq g_w(x), x \in GF^n(2)\right\} \end{matrix} \right| = \max_{w \in GF^n(2)} \left| 2^n - 2card\left\{x \mid f(x) \neq g(x), x \in GF^n(2)\right.\right.$$

$$= 2^n - 2\min_{g \in A_n} card\left\{x \mid f(x) \neq g(x), x \in GF^n(2)\right\} = 2^n - 2\min_{g \in A_n} d_H(f,g) = 2^n - 2N(f),$$

откуда имеем

$$NL(f) = \frac{2^n - \max\limits_{w \in GF^n(2)} \left|\overline{F}(w)\right|}{2} = 2^{n-1} - \max\limits_{w \in GF^n(2)} \left|\overline{F}(w)\right|.$$

Автокорреляционная функция, обозначаемая $r_{\hat{f}}(\alpha)$, вычисляется по формуле [6]:

$$r_{\hat{f}}(\alpha) = \sum_{x \in GF^n(2)} \hat{f}(x)\hat{f}(x \oplus \alpha),$$

где $\alpha \in GF^n(2)$ и $r_{\hat{f}}(0) = 2^n$. Автокорреляционная функция является вектором, содержащим 2^n действительных значений в диапазоне $[(-2)^n, 2^n]$.

Автокорреляция AC функции f является максимальным абсолютным значением автокорреляционной функции [6]:

$$AC = \max_{\alpha \in GF^n(2), \alpha \neq 0} \left|r(\alpha)\right|.$$

Таким образом, математический аппарат булевых функций является удобным инструментом для описания регулярных нелинейных узлов замен, а использование преобразования Уолша – Адамара дает адекватный механизм оценки основных криптографических показателей стойкости, в частности нелинейности компонентных булевых функций.

В то же время, использование рассмотренного математического аппарата для синтеза регулярных узлов замен через итеративное формирование компонентных булевых функций является непрактичным уже при $n = 6$ и вычислительно недостижимым для $n > 6$ [2, 3]. Перспективным направлением в этом смысле является использование недвоичных криптографических функций, описывающих отображение n-битных блоков входных данных в m-битные выходные блоки в нелинейном узле замен в виде функций отображения $F : GF(2^n) \to GF(2^m)$.

Представление S-блоков через недвоичные криптографические функции

Введем основные понятия и определения предлагаемого математического аппарата для описания нелинейных узлов замен через недвоичные функции.

Недвоичной (над полем $GF(2^{n_1})$) *функцией* $F(X_1,...,X_{n_2})$ от n_2 переменных является функция, осуществляющая отображение из поля $GF((2^{n_1})^{n_2})$ всех векторов $X = (X_1,...,X_{n_2})$ длины n_2 с элементами из $GF(2^{n_1})$ в поле $GF(2^{n_1})$. Как и рассмотренные выше булевы функции, каждая недвоичная функция $F(X_1,...,X_{n_2})$ может быть представлена в АНФ, т.е. как сумма произведений составляющих координат:

$$F(X_1,...,X_{n_2}) = \Lambda_0 + \Lambda_1 X_1 + ... + \Lambda_n X_n + \Lambda_{12} X_1 X_2 + \Lambda_{13} X_1 X_3 + ... + \Lambda_{12...n_2} X_1 X_2 ... X_n, \quad (7)$$

где $\Lambda_0, \Lambda_1, ..., \Lambda_{12}, ..., \Lambda_{12...n_2}$ – уникальные константы из $GF(2^{n_1})$, суммирование и умножение также производится в поле $GF(2^{n_1})$.

Поле $GF((2^{n_1})^{n_2})$ состоит из $2^{n_1 n_2}$ векторов $A_i = (A_1^i, A_2^i, ..., A_{n_2}^i)$, $A_j^i \in GF(2^{n_1})$:

$$A_0 = (0,...,0,0),\ A_1 = (0,...,0,1),\ \ldots,\ A_{2^{n_1}-1} = (0,...,0,2^{n_1}-1),\ A_{2^{n_1}} = (0,...,1,0),$$

$$A_{2^{n_1}+1} = (0,...,1,1),\ \ldots,\ A_{(2^{n_1})^{n_2}-1} = (2^{n_1}-1,...,2^{n_1}-1,2^{n_1}-1),\ \alpha_i \in V_n,$$

где V_{n_2} – векторное пространство над $GF(2^{n_1})$.

Поле $GF((2^{n_1})^{n_2})$ изоморфно полю $GF(2^n)$, $n = n_1 n_2$, т.е. имеем взаимно-однозначное функциональное соответствие множества векторов $A_i = (A_1^i, A_2^i, ..., A_{n_2}^i) \in V_{n_2}$ с элементами из $GF(2^{n_1})$ и двоичных векторов $\alpha_i = (\alpha_1^i, \alpha_2^i, ..., \alpha_n^i) \in V_n$.

Таблицей истинности недвоичной (над полем $GF(2^{n_1})$) функции F называется последовательность с элементами из $GF(2^{n_1})$, определенная как

$$\left(F(X)\middle| X \in GF^{n_2}(2^{n_1})\right) = \left(F(A_0), F(A_1), ..., F(A_{2^{n_1 n_2}-1})\right).$$

Последовательностью недвоичной (над полем $GF(2^{n_1})$) функции F называется последовательность из $2^{n_1 n_2}$ (1,-1)-кортежей длины $2^{n_1}-1$ каждый, определенная как

$$\left((-1)^{w\cdot F(X)}\middle| w \in GF(2^{n_1}), w \neq 0, X \in GF^{n_2}(2^{n_1})\right) =$$

$$= \left(\begin{array}{l} \left((-1)^{w_1\cdot F(A_0)}, (-1)^{w_2\cdot F(A_0)}, ..., (-1)^{w_{2^{n_1}-1}\cdot F(A_0)}\right), \\ \left((-1)^{w_1\cdot F(A_1)}, (-1)^{w_2\cdot F(A_1)}, ..., (-1)^{w_{2^{n_1}-1}\cdot F(A_1)}\right), ..., \\ \left((-1)^{w_1\cdot F(A_{2^{n_1 n_2}})}, (-1)^{w_2\cdot F(A_{2^{n_1 n_2}})}, ..., \right. \\ \left. (-1)^{w_{2^{n_1}-1}\cdot F(A_{2^{n_1 n_2}})}\right) \end{array}\right),$$

где w – накладываемая маска и $w \cdot F(X)$ – скалярное произведение векторных представлений чисел w и $F(X) \in GF(2^{n_1})$ (т.е. числа представлены в виде двоичных последовательностей, с элементами из $GF^{n_1}(2)$).

Например, пусть $n_1 = 2$, $n_2 = 1$ и недвоичная (над $GF(2^2)$) функция задана в АНФ следующим образом:

$$F(X) = 3 + X + 2X^2,$$

где коэффициенты многочлена принадлежат полю $GF(2^2)$: $0 = (0,0)$, $1 = (1,0)$, $2 = (0,1)$, $3 = (1,1)$.

Входными элементами такой функции являются однокоординатные вектора (скаляры) с элементами из $GF(2^2)$: $A_0 = (0)$, $A_1 = (1)$, $A_2 = (2)$, $A_3 = (3)$.

Таблицей истинности функции $F(X) = 3 + X + 2X^2$ является последовательность с элементами из $GF(2^2)$:

$$\left(F(X)\middle| X \in GF^1(2^2)\right) = \left(F(\mathrm{A}_0), F(\mathrm{A}_1), F(\mathrm{A}_2), F(\mathrm{A}_3)\right) = (3, 0, 0, 3).$$

Значения маски w и выхода функции $F(X)$ принадлежат полю $GF(2^2)$: $0 = (0,0)$, $1 = (1,0)$, $2 = (0,1)$, $3 = (1,1)$.

Последовательностью функции $F(X) = 3 + X + 2X^2$ является последовательность из $2^{n_1 n_2} = 4$ (1,-1)-кортежей длины $2^{n_1} - 1 = 3$ каждый:

$$\left\{\left((-1)^{w_1 \cdot F(X)}, (-1)^{w_2 \cdot F(X)}, (-1)^{w_3 \cdot F(X)}\right) \middle| w \in GF(2^{n_1}), w \neq 0, X \in GF^1(2^2)\right\} = \left\{\begin{array}{l}\left((-1)^{w_1 \cdot F(A_0)}, (-1)^{w_2 \cdot F(A_0)}, (-1)^{w_3 \cdot F(A_0)}\right), \\ \left((-1)^{w_1 \cdot F(A_1)}, (-1)^{w_2 \cdot F(A_1)}, (-1)^{w_3 \cdot F(A_1)}\right), \\ \left((-1)^{w_1 \cdot F(A_2)}, (-1)^{w_2 \cdot F(A_2)}, (-1)^{w_3 \cdot F(A_2)}\right), \\ \left((-1)^{w_1 \cdot F(A_3)}, (-1)^{w_2 \cdot F(A_3)}, (-1)^{w_3 \cdot F(A_3)}\right)\end{array}\right\} =$$

$$= \left\{\begin{array}{l}\left((-1)^{(1,0)\cdot(1,1)}, (-1)^{(0,1)\cdot(1,1)}, (-1)^{(1,1)\cdot(1,1)}\right), \\ \left((-1)^{(1,0)\cdot(0,0)}, (-1)^{(0,1)\cdot(0,0)}, (-1)^{(1,1)\cdot(0,0)}\right), \\ \left((-1)^{(1,0)\cdot(0,0)}, (-1)^{(0,1)\cdot(0,0)}, (-1)^{(1,1)\cdot(0,0)}\right), \\ \left((-1)^{(1,0)\cdot(1,1)}, (-1)^{(0,1)\cdot(1,1)}, (-1)^{(1,1)\cdot(1,1)}\right)\end{array}\right\} = \left\{\begin{array}{l}\left((-1)^1, (-1)^1, (-1)^0\right), \left((-1)^0, (-1)^0, (-1)^0\right), \\ \left((-1)^0, (-1)^0, (-1)^0\right), \left((-1)^1, (-1)^1, (-1)^0\right)\end{array}\right\} =$$

$$= \left((-1,-1,1), (1,1,1), (1,1,1), (-1,-1,1)\right).$$

Рассмотрим криптографические свойства функций F', реализующих отображения из $GF^{n_2}(2^{n_1})$ в $GF^m(2^{n_1})$, где $1 \le m \le n_2$. Пусть $M_{n_2}^m$ есть множество таких функций F', а B_{n_2} есть множество недвоичных функций $F(X_1, \ldots, X_{n_2})$ от n_2 переменных, то есть функций, реализующих отображения из $GF^{n_2}(2^{n_1})$ в $GF(2^{n_1})$. Тогда любую функцию из $M_{n_2}^m$ можно рассматривать как состоящую из m недвоичных функций $F(X_1, \ldots, X_{n_2})$ от n_2 переменных, т.е. m-выходных координатных функции из B_{n_2}. В более общем представлении, компонентная функция из $M_{n_2}^m$ является ненулевой линейной комбинацией ее координатных недвоичных функций из B_{n_2}.

Таким образом, функцию отображения $F' : GF^{n_2}(2^{n_1}) \to GF^m(2^{n_1})$, реализующую нелинейный узел замен, запишем через множество

$$F' = (F_1(X_1, \ldots, X_{n_2}), \ldots, F_m(X_1, \ldots, X_{n_2})),$$

где $F_i(X_1, \ldots, X_{n_2}) \in B_{n_2}$.

В данной работе ограничимся рассмотрением функций с $m = 1$, т.е. будем рассматривать только функции $F' = F_i(X_1, \ldots, X_{n_2})$, реализующие отображения из $GF^{n_2}(2^{n_1})$ в $GF(2^{n_1})$.

Введенная формализация функционального отображения $F: GF^{n_2}(2^{n_1}) \to GF(2^{n_1})$ является естественным обобщением рассмотренного выше подхода к представлению регулярных узлов замен в виде совокупности компонентных булевых функций.

Действительно, используя традиционный подход к описанию функционального отображения n-битных блоков входных данных в m-битные выходные блоки, функцию $F: GF^{n}(2) \to GF^{m}(2)$, где $n = n_1 n_2$, $m = n_1$ можно представить в виде кортежа $F = \{f_1(x_1,...,x_n), f_2(x_1,...,x_n),..., f_m(x_1,...,x_n)\}$ из $m = n_1$ булевых функций от $n = n_1 n_2$ булевых переменных каждая.

Для недвоичной функции из предыдущего примера имеем соответствие

$$F(X) = 3 + X + 2X^2 \equiv \begin{Bmatrix} f_1(x_1, x_2) = 1 + x_1 + x_2 \\ f_2(x_1, x_2) = 1 + x_1 + x_2 \end{Bmatrix},$$

где знак тождества означает тождественность правила отображения n = 2-битных блоков входных данных в m = 2-битные выходные блоки.

Важные свойства булевых функций изучаются с использованием преобразования Уолша – Адамара. По аналогии с преобразованием Уолша – Адамара введем спектральное преобразование недвоичных функций следующим образом.

Поскольку нелинейность булевой функции определяется как минимальное расстояние по Хэммингу от рассматриваемой функции ко множеству всех аффинных булевых функций, для недвоичного случая нам необходимо определить множество аффинных недвоичных функций.

Алгебраическая степень F, обозначаемая $\deg(F)$, определяется как максимальная степень многочлена представленного в АНФ.

По аналогии с классическим подходом назовем аффинной функцией недвоичную функция, чья алгебраическая степень $\deg(F) \le 1$. Соответственно, недвоичные функции, имеющие алгебраическую степень $\deg(F) > 1$, назовем нелинейными недвоичными функциями.

Спектральным преобразованием недвоичной функции $F(X_1,..., X_{n_2}) \in B_{n_2}$ есть вещественная функция $\overline{F}(W)$:

$$\overline{F}(W) = \sum_{X \in GF^{n_2}(2^{n_1})} \sum_{i=1}^{n_1} (-1)^{(F(X))_i + (G_W(x))_i}, \qquad (8)$$

где под $G_W(x)$ – понимается W-я недвоичная аффинная функция от n_2 переменных из множества A_n:

$$A_n \quad a_0 \quad \sum_{i\ 1}^{n_2} a_i X_i \mid a_i \quad GF(2^{n_1}), 0 \quad i \quad n \ . \qquad (9)$$

Так же, как и вектор w в случае булевого описания определяет вид линейных двоичных функций $g_w(x)$, в случае недвоичного описания вектор W задает вид недвоичных аффинных функций $G_W(x)$.

Вычислительный метод синтеза регулярных нелинейгых узлов замен

Анализ открытой литературы показал, что на сегодняшний день существуют вычислительные методы синтеза регулярных нелинейных узлов замен, среди которых [2, 8 - 12]: побитовые методы (bit-by-bit methods), методы случайной генерации с фильтрацией (random generation), метод градиентного подъема (hill climbing), генетические алгоритмы (genetic

algorithms), метод имитации отжига (simulated annealing), метод дифференциальной эволюции (differential evolution), метод оптимизации роем частиц (particle swarm optimization) и др. На наш взгляд, наиболее эффективным методом синтеза регулярных S-блоков является метод имитации отжига SA. Так, например, на основе проведенных в работах [10, 13] сравнений показано, что использование метода имитации отжига позволяет реализовать вычислительный поиск криптографических функций с лучшими на сегодняшний день показателями. Описание и алгоритм метода приведены ниже [10].

Поиск начинается с некоторого начального состояния $S = S_0$. Параметр T – некий контрольный параметр, известный как температура. T инициализируется высокой температурой T_0 и постепенно снижается. При каждом значении температуры выполняется определенное число *MIL* (Moves in Inner Loop, шагов во внутреннем цикле) шагов к новым состояниям. Состояние кандидата Y выбирается случайным образом из соседей $N(S)$ текущего состояния. Вычисляется изменение значения функции *cost*, $\delta = cost(Y) - cost(S)$. Если значение $cost(S)$ улучшается (т.е. $\delta < 0$ для задачи минимизации), тогда выполняется шаг относительно этого состояния ($S = Y$); в противном случае – он выполняется с некоторой вероятностью. Чем хуже шаг, тем меньше вероятность того, что он будет принят; чем ниже температура T, тем менее вероятно, что ухудшающий шаг будет принят. Вероятностное принятие решения определяется генерацией случайного числа U в интервале (0…1) и выполнением указанного ниже сравнения.

Вначале температура высокая и принимается почти каждый шаг. Это сделано для того, чтобы поиск носил не локальный, а глобальный характер. По мере того как температура уменьшается, становится все более трудно принимать ухудшающие шаги. В конце концов, допускаются только улучшающие шаги и процесс застывает. Алгоритм прерывается, когда встречается критерий остановки. Общий критерий остановки (который и был применен в нашей работе) – остановка поиска при достижении заданного числа *MaxIL* внутренних циклов, либо когда было выполнено некоторое максимальное число *MUL* последовательных непродуктивных внутренних циклов (т.е. без единого принятого шага). При этом лучшее достигнутое состояние сохраняется, поскольку поиск может выйти из него и впоследствии не найти состояние с подобными показателями. В конце каждого внутреннего цикла температура понижается. В нашей работе использовалось геометрическое охлаждение – умножение на константу охлаждения α в интервале (0…1).

Соседей функции f можно определить следующим образом. Функция g находится по соседству с функцией f, если:

$$\exists x, y \in Z_2^n : \hat{f}(x) \neq \hat{f}(y), \hat{g}(x) = \hat{f}(y), \hat{g}(y) = \hat{f}(x), \forall z \in Z_2^n \setminus \{x, y\} : \hat{g}(z) = \hat{f}(x).$$

Алгоритм имитации отжига *SA*

$S = S_0$;
$T = T_0$;
repeat {
  for (**int** $i = 0$; $i < MIL$; i++)
  {
    выбрать $Y \in N(S)$;
    $\delta = cost(Y) - cost(S)$;
    if ($\delta < 0$) **then** $S = Y$;
    else сгенерировать $U = U(0,1)$;
    if ($U < exp(-\delta/T)$) **then** $S = Y$;
  }
  $T = T \times \alpha$;
}
until (критерий остановки не достигнут).

Поиск начинался со сбалансированной, но при этом случайной функции. Один шаг алгоритма меняет местами два отличных элемента таблицы истинности функции, сохраняя ее сбалансированность.

Рассмотрим процедуры формирования функций стоимости cost (ценовых функций), используемые для синтеза S-блоков через спектральные характеристики булевых функций, введем соответствующие функции стоимости для синтеза S-блоков через спектры недвоичных криптографических функций.

Пусть функция $F(x): GF^n(2) \to GF^m(2)$ задает S-блок размерности *nxm*. Пусть для $\beta \in GF^m(2)$, $F_\beta(x) = \beta_1 f_1(x) \oplus ... \oplus \beta_m f_m(x)$ – линейная комбинация *m* выходов S-блока *F*. Тогда $\hat{F}_\beta(\omega), r_\beta(s)$ – значения преобразования Уолша – Адамара и значения автокорреляции для каждой булевой функции f_β.

Поскольку нелинейность булевой функции $NL(f) = \frac{1}{2}(2^n - \max_\omega |\hat{F}(\omega)|)$, то задача повышения нелинейности может быть представлена как задача минимизации абсолютного максимального значения коэффициента Уолша – Адамара. Изначально в задачах синтеза S-блоков по критерию высокой нелинейности для метода имитации отжига использовалась следующая функция стоимости [10]:

$$cost(f) = WHT_{\max}(f) = \max_\omega |\hat{F}(\omega)|.$$

Поскольку задача понижения автокорреляции представляется как задача минимизации максимального значения автокорреляционной функции, то *cost* функция в дальнейших исследованиях приняла вид [10]:

$$cost(f) = AC(f) = \max_{s \neq 0} |\sum_x \hat{f}(x)\hat{f}(x \oplus s)| = \max_{s \neq 0} |\hat{r}(s)|.$$

Обычно в многокритериальных задачах применяется следующий подход: вычисляется сумма отдельных *cost* функций (по различным критериям), умноженных на весовые коэффициенты. Тогда *cost* функция в задаче синтеза S-блока с высокой нелинейностью и низкой автокорреляцией принимает вид [10]:

$$\cos t(f) = \alpha \cdot WHT_{\max}(f) + \beta \cdot AC(f).$$

Далее были разработаны улучшенные функции, которые основывались на следующем положении.

Известно, что равенство Парсеваля

$$\sum_w (\hat{F}(w))^2 = 2^{2n}$$

ограничивает $WHT_{\max}(f) = \max_w \left|\hat{F}(w)\right|$ значением равным как минимум $2^{n/2}$. Данная граница достигается тогда, когда выполняется равенство $\left|\hat{F}(w)\right| = 2^{\frac{n}{2}}$ для каждого ω. Когда значение некоторого коэффициента $\left|\hat{F}(w)\right|$ меньше этой идеальной границы, теорема Парсеваля утверждает, что другие значения коэффициентов $\left|\hat{F}(w)\right|$ должны быть выше этой границы. Таким образом, попытка ограничить отдаленность абсолютных значений коэффициентов Уолша – Адамара от данной границы является возможным средством достижения высокой

нелинейности. Спектры некоторых функций содержат все значения (по модулю), равные этой идеальной границе. Такие функции называются бент-функциями.

Помимо обладания наивысшей возможной нелинейностью эти функции имеют нулевую автокорреляцию. Следовательно, функция стоимости

$$cost(f) = \sum_{\omega \in GF^n(2)} \left| \left| \hat{F}(\omega) \right| - 2^{\frac{n}{2}} \right|^R \tag{10}$$

является возможным подходом к оптимизации нелинейности и автокорреляции. Ввиду несбалансированности бент-функций приведенная функция стоимости *cost* может быть улучшена для нахождения сбалансированных криптографических функций. В [10] было введено обобщение функции стоимости (10), которое приняло следующий вид:

$$cost(f) = \sum_{\omega \in GF^n(2)} \left| \left| \hat{F}(\omega) \right| - X \right|^R . \tag{11}$$

Параметры X и R, называемые весовыми коэффициентами, обеспечивают свободу для экспериментирования и поиска оптимальных значений.

По аналогии с функциями стоимости относительно спектра Уолша – Адамара вида (11), функции стоимости относительно спектра автокорреляционной функции имеют следующий вид:

$$cost(f) = \sum_{s \in GF^n(2)} \left| \left| r(s) \right| - X \right|^R . \tag{12}$$

Традиционно ценовые функции применяются для оптимизации отдельной булевой функции. Для всего же нелинейного узла замен *cost* функции, основанные на спектре Уолша – Адамара, можно обобщить следующим образом [10]:

$$cost(f) = \sum_{\beta \in GF^m(2)} \sum_{\omega \in GF^n(2)} \left| \left| \hat{F}_\beta(\omega) \right| - X \right|^R \tag{13}$$

и аналогично для *cost* функций, основанных на автокорреляционном спектре:

$$cost(f) = \sum_{\beta \in GF^m(2)} \sum_{s \in GF^n(2)} \left| \left| r_\beta(s) \right| - X \right|^R . \tag{14}$$

Для оптимизации по критериям нелинейности и автокорреляции в [13] использовалась следующая функция стоимости:

$$cost(f) = \sum_{\beta \in GF^m(2)} \sum_{\omega \in GF^n(2)} \left| \left| \hat{F}_\beta(\omega) \right| - X_1 \right|^{R_1} + \sum_{\beta \in GF^m(2)} \sum_{s \in GF^n(2)} \left| \left| r_\beta(s) \right| - X_2 \right|^{R_2} . \tag{15}$$

В первой части проводимых в данной работе исследований использовались функции стоимости вида (12), (13), с заменой спектральных коэффициентов Уолша – Адамара и коэффициентов автокорреляционных спектров булевых функций на предложенные выше коэффициенты соответствующих спектров недвоичных функций.

Вторая часть проводимых исследований состояла в совершенствовании функций стоимости (критерия поиска криптографических функций), которое основывается на следующем положении. Известно, что при оптимизации криптографической функции по нелинейности и автокорреляции она по своим спектральным характеристикам (спектру корреляции с линейными функциями и автокорреляционному спектру) стремится к спектральным характеристи-

кам бент-функций, что и было использовано в предыдущих работах [10, 13] при разработке функций вида (10) – (15). В то же время очевидным недостатком такого подхода является использование одного (фиксированного) значения статического коэффициента, к которому стремятся все спектральные значения оптимизируемой криптографической функции. При этом значения спектральных коэффициентов идеальной функции (или бент-функции) состоят из двух возможных значений для булевых функций, и из трех значений для введенных недвоичных функций. При введении же дополнительных ограничений на сбалансированность количество возможных значений спектральных коэффициентов еще более возрастает.

При разработке новых функций стоимости в (11) – (15) предлагается заменить статический весовой коэффициент X на так называемые динамические весовые коэффициенты, т.е. весовые коэффициенты, принимающие различные значения для различных входных индексов спектра. В данной работе в качестве значений динамических весовых коэффициентов используются спектральные значения бент-функций. Предлагаемые функции стоимости имеют вид:

$$cost(f) = \sum_{\omega \in GF^n(2)} \left| \hat{F}(\omega) - \hat{B}(\omega) \right|^R, \tag{16}$$

$$cost(f) = \sum_{s \in GF^n(2)} \left| r_F(s) - r_B(s) \right|^R, \tag{17}$$

$$cost(f) = \sum_{\omega \in GF^n(2)} \left| \hat{F}(\omega) - \hat{B}(\omega) \right|^{R_1} + \sum_{s \in GF^n(2)} \left| r_F(s) - r_B(s) \right|^{R_2}, \tag{18}$$

где $\hat{B}(\omega), r_B(s)$ – спектральные значения нелинейности и автокорреляции случайной недвоичной бент-функции B.

В основе предлагаемого вычислительного метода синтеза регулярных нелинейных узлов замен симметричных криптоалгоритмов лежит применение математического аппарата недвоичных криптографических функций, методов корреляционного и спектрального анализа, а также предложенных в данной работе усовершенствованных ценовых функций (16) – (18) с использованием динамических весовых коэффициентов $\hat{B}(\omega), r_B(s)$. Усовершенствованный таким образом метод имитации отжига позволяет, как показано ниже, реализовать вычислительный поиск регулярных узлов замен с требуемыми показателями нелинейности и автокорреляции.

Результаты экспериментальных исследований

Для подтверждения достоверности и обоснованности полученных теоретических результатов проведены экспериментальные исследования эффективности предлагаемого вычислительного метода синтеза регулярных нелинейных узлов замен. Первая часть исследований проведена с использованием спектров недвоичных функций со статическими весовыми коэффициентами в функциях стоимости (13) – (15) метода имитации отжига, вторая часть исследований – с использованием динамических коэффициентов $\hat{B}(\omega), r_B(s)$ в функциях стоимости (16) – (18).

Параметры алгоритма для всех исследований были заданы следующими:

- $\alpha = 0.95$ – параметр геометрического охлаждения;
- $MIL = 500$ – число шагов, предпринимаемых во внутреннем цикле;
- $MaxIL = 300$ – максимальное число внутренних циклов поиска;
- $MUL = 50$ – максимальное число последовательных непродуктивных внутренних циклов;
- количество пробегов алгоритма для каждого набора параметров равно 10.

В ходе экспериментов с функциями стоимости вида (13) – (15) использовались различные значения статических коэффициентов X и фиксированное значение $R = 3$.

Формировались S-блоки размерностей 8x2, 4x4, 6x4. Узлы замен выходной размерности 4 представлялись через одну недвоичную функцию над $GF(2^4)$.

Полученные экспериментальные результаты для S-блоков 8x2 приведены в табл. 1. Лучший полученный результат выделен жирным шрифтом.

Таблица 1

Способ построения спектров, критерий отбора	Статические коэффициенты		Динамические коэффициенты	
	NL	*AC*	*NL*	*AC*
WHT, ср.	110	56	114	24
WHT, худш.	108	56	**116**	**24**
ACT, ср.	110	48	114	24
ACT, худш.	112	40	114	24
WHT+*ACT*, худш.	112	40	114	24
WHT+*ACT*, ср.	112	40	114	24

Как видно из полученных результатов, использование функций стоимости с динамическими весовыми коэффициентами позволило повысить показатели стойкости нелинейности и автокорреляции формируемых узлов замен.

В табл. 2 приведено сравнение полученных результатов с лучшими известными результатами, использующими традиционный подход описания S-блока в виде совокупности компонентных булевых функций [8 – 12]. Как видно из таблицы, полученные экспериментальные результаты предлагаемым методом с использованием функций стоимости на основе спектров недвоичных функций и статических весовых коэффициентов хорошо согласуются с экспериментальными результатами вычислительных методов традиционного подхода. Использование динамических весовых коэффициентов позволило получить лучшие известные на сегодняшний день результаты для S-блоков 8x2.

Таблица 2

Метод синтеза	*NL*	*AC*
Случайная генерация	108	56
Генетические алгоритмы	110	48
Имитация отжига (булевы функции)	114	32
Имитация отжига (недвоичные функции)	112	40
Имитация отжига (недвоичные функции, динамические весовые коэффициенты)	**116**	**24**

В табл. 3 приведены лучшие полученные результаты для S-блоков 4x4 и 6x4.

Таблица 3

S-блок	Метод имитации отжига	*NL*	*AC*
4x4	Булевы функции	4	8
4x4	Функции над $GF(2^4)$	4	8
6x4	Булевы функции	22	24
6x4	Функции над $GF(2^4)$	**24**	**24**

Как видно из приведенной таблицы, применение предлагаемого подхода позволяет повысить нелинейность формируемых S-блоков 6x4. Подобные S-блоки (размерности 6x4) применяются в DES-подобных шифрах.

Как показал анализ, S-блоки DES по своим криптографическим показателям нелинейности *NL* и автокорреляции *AC* далеки от оптимальных (см. данные для S1-S8 в табл. 4).

Таблица 4

S-блок	*NL*	*AC*	DDT_{max}
S1	14	48	16
S2	16	56	16
S3	16	48	16
S4	16	64	16
S5	12	**40**	**16**
S6	**18**	48	16
S7	14	52	16
S8	16	48	16
S1*-S8*	**24**	**24**	**10**

Разработанный вычислительный метод предлагается использовать для синтеза DES-подобных S-блоков с улучшенными криптографическими показателями стойкости (в табл. 4 приведены характеристики формируемых узлов замен S1*-S8*).

Следует отметить, что для обеспечения стойкости DES-подобных шифров к дифференциальному и линейному криптоанализу сформированные S-блоки необходимо оценивать не только по показателям нелинейности и автокорреляции, но и с учетом других критериев, учитывающих саму структуру шифра [14]. В этом смысле оценка эффективности формируемых S-блоков с учетом ограничений, накладываемых особенностями основных преобразований БСШ, а также апробация полученных результатов являются перспективным направлением дальнейших исследований.

Заключение

Предложенная математическая модель представления S-блоков через недвоичные функции является новым направлением в области формирования нелинейных узлов замен и представляет собой основу для дальнейших исследований в этом направлении. Введенное теоретическое обобщение и предложенный математический аппарат недвоичных криптографических функций позволил усовершенствовать вычислительный метод формирования нелинейных узлов замен (метод имитации отжига). В результате процесс формирования нелинейных узлов замен с требуемыми криптографическими свойствами упрощен, а именно – существенно сократилось количество оптимизационных спектров в процессе синтеза S-блоков.

Усовершенствованный вычислительный метод реализован программно, полученные экспериментальные результаты с использованием функций стоимости со статическими весовыми коэффициентами хорошо согласуются с экспериментальными результатами вычислительных методов традиционного подхода. Использование динамических весовых коэффициентов в новых разработанных функциях стоимости позволили получить лучшие известные на сегодняшний день результаты для S-блоков 8x2. Для S-блоков 6x4 удалось поднять верхнюю границу показателя нелинейности. Разработанный вычислительный метод предлагается использовать для синтеза DES-подобных S-блоков.

Перспективными направлениями дальнейших исследований являются развитие математического аппарата криптографических недвоичных функций для задач синтеза S-блоков, экспериментальные исследования эффективности предлагаемого подхода для узлов замен больших размерностей, обобщение динамических весовых коэффициентов.

Список литературы: 1. *Сорока, Л.С.* Вероятностная модель формирования нелинейных узлов замен для симметричных криптографических средств защиты информации / Сорока Л.С., Кузнецов А.А., Московченко И.В., Исаев С.А. // Системи обробки інформації. – Х. :ХУВС, 2009. – № 3 (77). – С. 101-104. 2. *O'Connor, L.* An analysis of a class of algorithms for S-box construction / O'Connor L. // J. Cryptology. - 1994. – P. 133-151. 3. *Сорока, Л.С.* Исследование вероятностных методов формирования нели-

нейных узлов замен / Сорока Л.С., Кузнецов А.А., Исаев С.А. // Системи обробки інформації. – 2011. – № 8 (98). – С. 113 – 122. 4. *Булева функция* // Режим доступу: http://ru.wikipedia.org/wiki/Булева_функция. 5. *Dawson, E.* Designing Boolean functions for cryptographic applications / Dawson E., Millan W., Simpson L. // Contributions to General Algebra, Verlag Johannes Heyn, Klagenfurt. – 2000. – 12. – P. 1-22. 6. *Clark, J.A.* Evolving Boolean functions satisfying multiple criteria / Clark J.A., Jacob J.L., Stepney S., Maitra S., Milan W. // Lecture Notes in Computer Science (2551), Springer, Berlin. – 2002. – 2251. – P. 246-259. 7. *Parker, M.G.* Generalised S-Box Nonlinearity / Parker M.G. // NES/DOC/UIB/WP5/020/A. – 2003. 8. *Millan, W.* How to improve the nonlinearity of bijective s-boxes / Millan W. // Information Security and Privacy, ACISP '98, Springer Verlag. – 1998. – volume 1438 of Lecture Notes in Computer Science. – P. 181-192. 9. *Millan, W.* Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes / Millan W., Burnett L., Carter G., Clark A., Dawson E. // Information and communication security, Springer, Heidelberg. – 1999. – Lecture Notes in Computer Science Volume 1726. – P.263-274. 10. *Clark, J.A.* The Design of S-Boxes by Simulated Annealing / Clark J.A., Jacob J.L., Stepney S. // New Generation Computing. – 2005. – 23(3). – P.219–231. 11. *Laskari, C.* Utilizing Evolutionary Computation Methods for the Design of S-Boxes / Laskari C., Meletiou C., Vrahatis N. // Computational Intelligence and Security. – 2006. – Volume 2. – P.1299-1302. 12. *Tesar, P.* A new method for generating high non-linearity S-Boxes / Tesar P. // Radioengineering. – 2010. – Part I of II, Vol. 19 Issue 1. – P.23 -26. 13. *Kavut, S.* Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria / Kavut S., Yücel M.D. // Proc. INDOCRYPT. – 2003. – P.121-134. 14. *Kwangjo, K.* Securing DES S-Boxes against Three Robust Cryptanalysis / Kwangjo K., Sangjin L., Sangjoon P., Daiki L. // Proceedings of the Workshop on Selected Areas in Cryptography, SAC '95. – 1995. – P.145-157.

Харьковский национальный
университет радиоэлектроники

Поступила в редколлегию 14.09.2012