

НЕДВОИЧНЫЕ КРИПТОГРАФИЧЕСКИЕ ФУНКЦИИ ДЛЯ ГЕНЕРАЦИИ БЛОКОВ ПОДСТАНОВОК СИММЕТРИЧНЫХ ШИФРОВ

Никита Гончаров, Татьяна Кузнецова, Александр Кузнецов

Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина
worldxdark@gmail.com, kuznetsova.tatiana17@gmail.com, kuznetsov@karazin.ua

Рецензент: Сергей Толупа, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, ул. М. Ломоносова 81, г. Киев, 03189, Украина.
tolupa@i.ua

Поступила: Январь 2020.

Аннотация: Важным элементом современных симметричных криптоалгоритмов являются нелинейные узлы замен (блоки подстановок, S-блоки). Свойства этих блоков непосредственно влияют на показатели криптографической стойкости алгоритмов шифрования. Например, стойкость симметричных шифров к дифференциальному и линейному криптоанализу непосредственно зависит от показателей нелинейности S-блоков и их корреляционных свойств. В данной статье исследуются способы математического описания регулярных нелинейных узлов замен, вычислительные техники их генерации и оценки криптографических показателей. Рассматривается традиционный подход, в котором для описания внутренней структуры S-блоков используется совокупность компонентных булевых функций. Исследуются недвоичные функции, с помощью которых формируются регулярные нелинейные узлы замены. Приводятся результаты вычислительного поиска S-блоков с использованием предлагаемого подхода. Для генерации регулярных S-блоков использовались методы имитации отжига, применительно к недвоичным функциям с улучшенными ценовыми функциями (настраиваемый элемент метода имитации отжига). Показано, что по нелинейности и автокорреляции, сформированные узлы замен обладают улучшенными свойствами.

Ключевые слова: симметричный криптоалгоритм; нелинейный узел замен; нелинейность; автокорреляция; спектральное преобразование; криптографическая функция; имитация отжига; ценовая функция.

1 Введение

Регулярные нелинейные криптографические функции (узлы замен, блоки подстановок, S-бок) симметричных шифров реализуют отображение n -битных блоков входных данных в m -битные выходные блоки: $F : GF^n(2) \rightarrow GF^m(2)$. Традиционный подход к описанию, генерации и оценке показателей стойкости и регулярных S-блоков состоит в представлении функции F с помощью ее координатных функций, которые задаются в терминах булевой алгебры [1]. В тоже 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 математическому описанию криптографических узлов замен симметричных шифров, исследованию и построению вычислительно эффективных алгоритмов генерации.

В первой части данной работы рассмотрен традиционный способ описания S-блоков, через совокупность компонентных булевых функций. Далее будут использованы недвоичные функции, с помощью которых удастся компактно представить S-блоки и формализовать способ их генерации. Авторским коллективом приведены некоторые результаты, касающиеся вычислительного поиска S-блоков с использованием предлагаемого подхода. Результаты данной работы являются логическим продолжением ранее опубликованных исследований [3]. Полученные данные дают основание утверждать, что формируемые S-блоки, по показателям нелинейности и автокорреляции, обладают улучшенными свойствами.

2 Представление S-блоков через компонентные булевы функции

Основные понятия и определения математического аппарата булевой алгебры, используемые при описании нелинейных узлов замен через компонентные булевы функции и оценке

их криптографических свойств, представлены в многочисленных работах [2-6 и др.]. Приведем здесь лишь краткие сведения, основные понятия и определения, которые понадобятся для дальнейшего изложения материала.

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

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

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

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

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

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

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

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

Рассмотрим криптографические свойства функций, реализующих отображения из $GF^n(2)$ в $GF^m(2)$, где $1 \leq m \leq n$. 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 $F : GF^n(2) \rightarrow GF^m(2)$ запишем через множество

$$F = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)), \text{ где } f_i(x_1, \dots, x_n) \in B_n.$$

Алгебраическая степень функции 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 $f(x_1, \dots, x_n) \in B_n$ есть вещественная функция $\bar{F}(w)$ [5]:

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

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

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 $\bar{F}(0) = 0$.

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

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

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

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

где A_n - множество всех аффинных функций от n переменных,

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

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

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

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

Адамара H_{2^n} порядка 2^n :

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

(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 следующим выражением:

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

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

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

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

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

Тогда, очевидно, выполняется равенство

$$\begin{aligned} \left((-1)^{f(x)} \Big|_{x \in GF(2)^n} \right) \cdot H_{2^n} &= \left((-1)^{f(x)} \Big|_{x \in GF^n(2)} \right) \cdot \begin{pmatrix} \left((-1)^{g_1(x)} \Big|_{x \in GF^n(2)} \right) \\ \left((-1)^{g_2(x)} \Big|_{x \in GF^n(2)} \right) \\ \dots \\ \left((-1)^{g_{2^n}(x)} \Big|_{x \in GF^n(2)} \right) \end{pmatrix}^T = \\ &= \left(\sum_{x \in GF^n(2)} (-1)^{f(x)+g_i(x)} \Big|_{x \in GF^n(2), g_i(x) \in A'_n} \right) = \left(\bar{F}(w) \Big|_{w \in GF^n(2)} \right). \end{aligned}$$

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

$$\begin{aligned} \left((-1)^{g_1(x)=0} \Big|_{x \in GF^2(2)} \right) &= (1, 1, 1, 1); \quad \left((-1)^{g_2(x)=x_1} \Big|_{x \in GF^2(2)} \right) = (1, -1, 1, -1); \\ \left((-1)^{g_3(x)=x_2} \Big|_{x \in GF^2(2)} \right) &= (1, 1, -1, -1); \quad \left((-1)^{g_4(x)=x_1+x_2} \Big|_{x \in GF^2(2)} \right) = (1, 1, -1, -1) \end{aligned}$$

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

Выражение для расчета значений коэффициентов преобразования Уолша-Адамара запишем, соответственно, в виде

$$\bar{F}(w) = \sum_{x \in GF^n(2)} (-1)^{f(x)+g_w(x)} \Big|_{x \in GF^n(2)}$$

Максимальное значение коэффициентов преобразования Уолша-Адамара $\max_{w \in GF^n(2)} \bar{F}(w)$

булевой функции $f(x)$ соответствует максимальному коэффициенту корреляции (*похожести*) последовательности этой функции и последовательностей всех аффинных функций из множества A'_n :

$$\begin{aligned} \max_{w \in GF^n(2)} \bar{F}(w) &= \max_{w \in GF^n(2)} \left(\sum_{x \in GF^n(2)} (-1)^{f(x)+g_w(x)} \Big|_{x \in GF^n(2)} \right) = \\ &= \max_{w \in GF^n(2)} \left(\begin{matrix} \text{card} \{x \mid f(x) = g_w(x), x \in GF^n(2)\} - \\ - \text{card} \{x \mid f(x) \neq g_w(x), x \in GF^n(2)\} \end{matrix} \right). \end{aligned}$$

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 $\max_{w \in GF^n(2)} |\overline{F}(w)|$ 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:

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

Поскольку

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

то справедливо следующее равенство

$$\begin{aligned} \max_{w \in GF^n(2)} |\overline{F}(w)| &= \max_{w \in GF^n(2)} \left| \sum_{x \in GF^n(2)} (-1)^{f(x)+g_w(x)} \right| = \\ &= \max_{w \in GF^n(2)} \left| \text{card} \left\{ x \mid f(x) = g_w(x), x \in GF^n(2) \right\} - \right. \\ &\quad \left. - \text{card} \left\{ x \mid f(x) \neq g_w(x), x \in GF^n(2) \right\} \right| = \max_{w \in GF^n(2)} \left| 2^n - 2 \text{card} \left\{ x \mid f(x) \neq g_w(x), x \in GF^n(2) \right\} \right| = \\ &= 2^n - 2 \min_{g \in A_n} \text{card} \left\{ x \mid f(x) \neq g(x), x \in GF^n(2) \right\} = 2^n - 2 \min_{g \in A_n} d_H(f, g) = 2^n - 2NL(f), \end{aligned}$$

откуда получаем:

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

Автокорреляционная функция, обозначаемая как $r_{\hat{f}}(\alpha)$, 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 АС функции f является максимальным абсолютным значением автокорреляционной функции [6]:

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

Таким образом, математический аппарат булевых функций является удобным инструментом для описания регулярных нелинейных узлов замен. При этом 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 генерации 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 $F : GF(2^n) \rightarrow GF(2^m)$.

3 Представление S-блоков через недвоичные булевы функции

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

Недвоичной (над полем $GF(2^{n_1})$) функцией $F(X_1, \dots, X_{n_2})$ от n_2 переменных является функция, осуществляющая отображение из поля $GF((2^{n_1})^{n_2})$ всех векторов $X = (X_1, \dots, X_{n_2})$ 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 $F(X_1, \dots, X_{n_2})$ может быть представлена в АНФ, т.е. как сумма произведений составляющих координат:

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

где $\Lambda_0, \Lambda_1, \dots, \Lambda_{12}, \dots, \Lambda_{12\dots n_2}$ - 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 $A_i = (A_1^i, A_2^i, \dots, A_{n_2}^i)$, $A_j^i \in GF(2^{n_1})$:

$$A_0 = (0, \dots, 0, 0), A_1 = (0, \dots, 0, 1), \dots, A_{2^{n_1}-1} = (0, \dots, 0, 2^{n_1}-1), A_{2^{n_1}} = (0, \dots, 1, 0), \\ A_{2^{n_1}+1} = (0, \dots, 1, 1), \dots, A_{(2^{n_1})^{n_2}-1} = (2^{n_1}-1, \dots, 2^{n_1}-1, 2^{n_1}-1), \alpha_i \in V_n,$$

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 $A_i = (A_1^i, A_2^i, \dots, A_{n_2}^i) \in V_{n_2}$ с элементами из $GF(2^{n_1})$ и двоичных векторов $\alpha_i = (\alpha_1^i, \alpha_2^i, \dots, \alpha_n^i) \in V_n$.

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

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

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:

$$\left((-1)^{w \cdot F(X)} \mid w \in GF(2^{n_1}), w \neq 0, X \in GF^{n_2}(2^{n_1}) \right) = \\ = \left(\begin{array}{l} \left((-1)^{w_1 \cdot F(A_0)}, (-1)^{w_2 \cdot F(A_0)}, \dots, (-1)^{w_{2^{n_1}-1} \cdot F(A_0)} \right), \\ \left((-1)^{w_1 \cdot F(A_1)}, (-1)^{w_2 \cdot F(A_1)}, \dots, (-1)^{w_{2^{n_1}-1} \cdot F(A_1)} \right), \dots, \\ \left((-1)^{w_1 \cdot F(A_{2^{n_1 n_2}})}, (-1)^{w_2 \cdot F(A_{2^{n_1 n_2}})}, \dots, \right. \\ \left. (-1)^{w_{2^{n_1}-1} \cdot F(A_{2^{n_1 n_2}})} \right) \end{array} \right),$$

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 $GF(2^2)$:

$$\left(F(X) \mid X \in GF^1(2^2) \right) = (F(A_0), F(A_1), F(A_2), F(A_3)) = (3, 0, 0, 3).$$

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 с длиной каждого $2^{n_1} - 1 = 3$:

$$\begin{aligned} & \left(\begin{array}{c} \left((-1)^{w_1 \cdot F(X)}, (-1)^{w_2 \cdot F(X)}, (-1)^{w_3 \cdot F(X)} \right) \\ \left[w \in GF(2^{n_1}), w \neq 0, X \in GF^1(2^2) \right] \end{array} \right) = \left(\begin{array}{c} \left((-1)^{w_1 \cdot F(A_0)}, (-1)^{w_2 \cdot F(A_0)}, (-1)^{w_3 \cdot F(A_0)} \right), \\ \left((-1)^{w_1 \cdot F(A_1)}, (-1)^{w_2 \cdot F(A_1)}, (-1)^{w_3 \cdot F(A_1)} \right), \\ \left((-1)^{w_1 \cdot F(A_2)}, (-1)^{w_2 \cdot F(A_2)}, (-1)^{w_3 \cdot F(A_2)} \right), \\ \left((-1)^{w_1 \cdot F(A_3)}, (-1)^{w_2 \cdot F(A_3)}, (-1)^{w_3 \cdot F(A_3)} \right) \end{array} \right) = \\ & = \left(\begin{array}{c} \left((-1)^{(1,0) \cdot (1,1)}, (-1)^{(0,1) \cdot (1,1)}, (-1)^{(1,1) \cdot (1,1)} \right), \\ \left((-1)^{(1,0) \cdot (0,0)}, (-1)^{(0,1) \cdot (0,0)}, (-1)^{(1,1) \cdot (0,0)} \right), \\ \left((-1)^{(1,0) \cdot (0,0)}, (-1)^{(0,1) \cdot (0,0)}, (-1)^{(1,1) \cdot (0,0)} \right), \\ \left((-1)^{(1,0) \cdot (1,1)}, (-1)^{(0,1) \cdot (1,1)}, (-1)^{(1,1) \cdot (1,1)} \right) \end{array} \right) = \left(\begin{array}{c} \left((-1)^1, (-1)^1, (-1)^0 \right), \left((-1)^0, (-1)^0, (-1)^0 \right), \\ \left((-1)^0, (-1)^0, (-1)^0 \right), \left((-1)^1, (-1)^1, (-1)^0 \right) \end{array} \right) = \\ & = ((-1, -1, 1), (1, 1, 1), (1, 1, 1), (-1, -1, 1)). \end{aligned}$$

Рассмотрим криптографические свойства функций F' , реализующих отображения из $GF^{n_2}(2^{n_1})$ в $GF^m(2^{n_1})$, где $1 \leq m \leq n_2$.

Пусть $M_{n_2}^m$ есть множество таких функций F' , а B_{n_2} - это множество недвоичных функций $F(X_1, \dots, X_{n_2})$ от n_2 переменных, т.е. 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 $F(X_1, \dots, X_{n_2})$ 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 $F': GF^{n_2}(2^{n_1}) \rightarrow GF^m(2^{n_1})$, реализующую нелинейный узел замен, запишем через множество $F' = (F_1(X_1, \dots, X_{n_2}), \dots, F_m(X_1, \dots, X_{n_2}))$, где $F_i(X_1, \dots, X_{n_2}) \in B_{n_2}$.

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

Введенная ранее формализация 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 $F: GF^n(2) \rightarrow GF^m(2)$, где $n = n_1 n_2$, $m = n_1$, можно представить в виде кортежа $F = \{f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)\}$ из $m = n_1$ булевых функций от $n = n_1 n_2$ булевых переменных каждая.

Для недвоичной функции, из предыдущего примера, имеем следующее соответствие:

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

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 функцию F , чья алгебраическая степень $\deg(F) \leq 1$. Соответственно, недвоичные функции, имеющие алгебраическую степень $\deg(F) > 1$, назовем нелинейными недвоичными функциями.

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

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

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

$$A_n = \left\{ a_0 + \sum_{i=1}^{n_2} a_i X_i / a_i \in GF(2^{n_1}), 0 \leq i \leq n \right\}. \quad (9)$$

Также 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 $G_W(x)$.

4 Вычислительный метод генерации регулярных нелинейных узлов замен

На сегодняшний день известно большое число различных вычислительных техник генерации регулярных нелинейных узлов замен. Среди наиболее известных из них следует выделить [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.

Одним из наиболее эффективных является метод имитации отжига SA. Так, например, в [10, 13] показано, что использование метода имитации отжига позволяет формировать криптографические функции с очень высокими показателями стойкости. Приведем краткое изложение этого метода из [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*, $\delta = \text{cost}(Y) - \text{cost}(S)$. Если значение *cost*(S) улучшается (*m.e.* $\delta < 0$ для задачи минимизации), тогда выполняется шаг относительно этого состояния ($S = Y$); в противном случае – он выполняется с некоторой вероятностью. Т.о. 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 (*m.e. 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 данной 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:

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

Алгоритм имитации отжига SA

```

S = S0;
T = T0;
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 генерации S-блоков через спектральные характеристики булевых функций, введем соответствующие функции стоимости для генерации S-блоков через спектры не двоичных криптографических функций.

Пусть функция $F(x): GF^n(2) \rightarrow GF^m(2)$ задает S-блок размерности $n \times m$. Пусть для $\beta \in GF^m(2)$, $F_\beta(x) = \beta_1 f_1(x) \oplus \dots \oplus \beta_m f_m(x)$ - 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 генерации S-блоков 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 следующий вид [10]:

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

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

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

Далее были разработаны *улучшенные функции*, которые основывались на следующем положении. Известно, что равенство Парсеваля $\sum_w (\hat{F}(w))^2 = 2^{2n}$ ограничивает $WHT_{\max}(f) = \max_w |\hat{F}(w)|$ значением равным как минимум $2^{n/2}$.

Данная граница достигается тогда, когда выполняется равенство $|\hat{F}(w)| = 2^{n/2}$ для каждого ω . Когда значение некоторого коэффициента $|\hat{F}(w)|$ меньше этой идеальной границы,

теорема Парсеваля утверждает, что другие значения коэффициентов $|\hat{F}(w)|$ 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 границы. Такие функции называются бент-функциями.

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

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

является возможным подходом к оптимизации нелинейности и автокорреляции. В виду 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:

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

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:

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

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]:

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

и аналогично для cost функций, основанных на автокорреляционном спектре:

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

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

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

В первой части исследований, проводимых в рамках данной работы, использовались функции стоимости вида (12), (13), с заменой *спектральных коэффициентов Уолша-Адамара* и *коэффициентов автокорреляционных спектров булевых функций* на предложенные выше *коэффициенты соответствующих спектров не двоичных функций*.

Вторая часть исследований состояла в совершенствовании функций стоимости (*критерия поиска криптографических функций*), базирующемся на изложенном ниже 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 характеристикам бент-функций, что и было использовано в предыдущих работах [10,13] при разработке функций вида (10)-(15). В тоже время, очевидным недостатком такого подхода, является использование одного (*фиксированного*) значения 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 ограничения на сбалансированность, количество возможных значений спектральных коэффициентов еще более возрастает.

При разработке новых функций стоимости, в выражениях (11) - (15) предлагается заменить весовой коэффициент X на т.н. **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:

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

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

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

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

Таким образом, в основу предлагаемого вычислительного метода генерации регулярных нелинейных узлов замен, положено применение недвоичных криптографических функций и 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 улучшенными показателями нелинейности и автокорреляции.

5 Результаты экспериментальных исследований

В данной работе представлены результаты экспериментальных исследований эффективности предлагаемого вычислительного метода (генерации регулярных нелинейных узлов замен). В этой связи важно подчеркнуть, что 1-я часть исследований была проведена с использованием **спектров недвоичных функций с весовыми коэффициентами в функциях стоимости (13) – (15) метода имитации отжига**, а 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 следующим образом:

- $\alpha = 0.95$ – 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 8×2 , 4×4 и 6×4 . Узлы замен выходной размерности 4 представлялись через одну недвоичную функцию над $GF(2^4)$.

Полученные экспериментальные результаты для S-блоков 8×2 приведены ниже, в табл. 1. Лучший полученный результат выделен **жирным шрифтом** на красном фоне.

Таблица 1 – Результаты для S-блоков 8×2

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 следует из данных Табл. 1, использование функций стоимости с динамическими весовыми коэффициентами, позволило улучшить показатели стойкости нелинейности и автокорреляции формируемых узлов замен.

В табл. 2 проведено сравнение полученных результатов уже с известными результатами, использующими традиционный подход описания S-блока, в виде совокупности компонентных булевых функций [8-12]. Как видно из табл. 2, использование динамических весовых коэффициентов позволило получить лучшие результаты для S-блоков 8×2 .

Таблица 2 – Результаты сравнения

Используемый метод генерации	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 размером 4×4 и 6×4 .

Таблица 3 – Лучшие из полученных результатов (для 4×4 и 6×4)

Размерность S-блока	Метод имитации отжига	NL	AC
4×4	Булевы функции	4	8
4×4	Функции над $GF(2^4)$	4	8
6×4	Булевы функции	22	24
6×4	Функции над $GF(2^4)$	24	24

Как следует из приведенной таблицы, применение предлагаемого подхода позволяет повысить нелинейность формируемых S-блоков размерностью 6×4 . Подобные S-блоки (размерности 6×4) применяются, например, в DES-подобных шифрах.

6 Выводы

1. Методы генерации нелинейных узлов симметричных криптоалгоритмов постоянно развиваются и совершенствуются. Одним из перспективных направлений в этом смысле является использование недвоичных криптографических функций.

2. Авторским коллективом рассмотрен один из способов подобной формализации и показано, что использование недвоичных функций позволяет, кроме прочего, интерпретировать известные методы генерации S-блоков. В частности, был реализован метод имитации отжига при недвоичном представлении функций. По результатам экспериментов показано, что в совокупности с улучшенными ценовыми функциями (*настраиваемый элемент метода имитации отжига*) удастся сформировать S-блоки с улучшенными показателями стойкости.

3. Предложенный вычислительный метод генерации S-блоков реализован программно.

4. Полученные результаты хорошо согласуются с результатами вычислительных методов традиционного подхода (*через описание S-блока булевыми функциями*).

5. Использование динамических весовых коэффициентов в функциях стоимости, позволили получить лучшие результаты для S-блоков 8×2 . Для S-блоков с размерностью 6×4 удалось поднять верхнюю границу показателя нелинейности.

6. Разработанный вычислительный метод предлагается использовать для целей генерации DES-подобных S-блоков.

7. Перспективным направлением дальнейших исследований связано с возможностями адаптации предлагаемого подхода для узлов замен больших размерностей и обобщение динамических весовых коэффициентов в функциях стоимости.

Ссылки

- [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. – X.: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 нелинейных узлов замен / Сорока Л.С., Кузнецов А.А., Исаев С.А. // Системи обробки інформації. – 2011. - № 8 (98). – С. 113 – 122.
- [4] Булева функция [Электронный ресурс] // Режим доступа: 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.

Рецензент: Сергій Толупа, д.т.н., проф., Київський національний університет імені Т. Шевченка, м. Київ, Україна
E-mail: tolupa@i.ua

Надійшло: Січень 2020.

Автори:

Микита Гончаров, студент факультету комп'ютерних наук, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: worldxdark@gmail.com

Тетяна Кузнецова, науковий співробітник, ХНУ імені В.Н. Каразіна, Харків, Україна.
E-mail: kuznetsova.tatiana17@gmail.com

Олександр Кузнецов, д.т.н., проф., ХНУ імені В.Н. Каразіна, Харків, Україна.

E-mail: kuznetsov@karazin.ua

Недвійкові криптографічні функції для генерації блоків підстановок симетричних шифрів.

Анотація. Важливим елементом сучасних симетричних криптоалгоритмів є нелінійні вузли заміни (блоки підстановок, S-блоки). Властивості цих блоків безпосередньо впливають на показники криптографічної стійкості алгоритмів шифрування. Наприклад, стійкість симетричних шифрів до диференціального і лінійного криптоаналізу безпосередньо залежить від показників нелінійності S-блоків та їх кореляційних властивостей. У даній статті досліджуються способи математичного опису регулярних нелінійних вузлів заміни, обчислювальні техніки їх генерації і оцінки криптографічних показників. Розглядається традиційний підхід, в якому для опису внутрішньої структури S-блоків використовується сукупність компонентних булевих функцій. Досліджуються недвійкові функції, за допомогою яких формуються регулярні нелінійні вузли заміни. Наводяться результати обчислювального пошуку S-блоків з використанням запропонованого підходу. Для генерації регулярних S-блоків використовувалися методи імітації віджигу, стосовно недвійкових функцій з поліпшеними цінковими функціями (елемент методу імітації віджигу, що настроюється). Показано, що за нелінійності і автокореляції, сформовані вузли заміни мають поліпшені властивості.

Ключові слова: симетричний криптоалгоритм; нелінійний вузол заміни; не лінійність; автокореляція; спектральне перетворення; криптографічна функція; імітація віджигу; цінкова функція.

Reviewer: Serhii Toliupa, Doctor of Sciences (Eng.), Full Prof., Taras Shevchenko National University of Kiev, 81 Lomonosova St., Kyiv, 03189, Ukraine. E-mail: tolupa@i.ua

Received on January 2020.

Authors:

Nikita Goncharov, Computer Science Student, V.N. Karazin Kharkiv National University, Ukraine.

E-mail: worldxdark@gmail.com

Tetiana Kuznetsova, Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.

E-mail: kuznetsova.tatiana17@gmail.com

Alexandr Kuznetsov, Doctor of Sciences (Eng.), Prof., V. N. Karazin Kharkiv National University, Department of information systems and technologies security, Kharkiv, Ukraine.

E-mail: kuznetsov@karazin.ua

Non-binary cryptographic functions for design of blocks of substitutions of symmetric cipher.

Annotation. In the paper considers the traditional way of describing S-blocks through a set of component Boolean functions. non-binary functions were used to represent s-blocks compactly and formalize the method of generating them. Some results of computational search for S-blocks were presented using the proposed approach, where the generated S-blocks have improved properties based on non-linearity and autocorrelation indicators.

Key words: Symmetric cryptoalgorithm; Nonlinearity replacement nodes; Nonlinearity; Autocorrelation; Spectrum transformation; Cryptographic function; Simulated annealing; Cost function.