УДК 004.056.55

АЛГЕБРАИЧЕСКИЙ ИММУНИТЕТ НЕЛИНЕЙНЫХ УЗЛОВ СИММЕТРИЧНЫХ ШИФРОВ

А. Кузнецов[1], Ю. Горбенко[2], И. Белозерцев[3], А. Андрушкевич[4], А. Нарежний[5]

[1,3,4,5] Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина
kuznetsov@karazin.ua, ivanbelozersevv.jw@gmail.com, hitori26@mail.ru, o.nariezhnii@karazin.ua

[2] АО «Институт информационных технологий», ул. Бакулина, 12, г. Харьков, 61166, Украина
gorbenkou@iit.kharkov.ua

Рецензент: Антон Алексейчук, д.т.н., доцент, Институт специальной связи и защиты информации национального технического университета Украины «КПИ», пр. Победы, 37, г. Киев, 03056, Украина.
alex-dtn@ukr.net

Поступила в декабре 2016

Аннотация. *Исследуются методы вычисления алгебраической иммунности криптографических булевых функций и нелинейных узлов замен (подстановок) симметричных шифров. Приводятся результаты сравнительного анализа алгебраической иммунности нелинейных узлов симметричных шифров.*

Ключевые слова*: симметричные шифры, алгебраический иммунитет, нелинейные узлы замены.*

1 Введение

Криптографическое преобразование играет важную роль в обеспечении безопасности современных информационных систем и технологий [1, 2]. Симметричные шифры, в силу свой простоты, эффективности и многофункциональности, применяются практически во всех современных криптопротоколах, а также как составная часть других криптографических примитивов: в хешировании, формировании псевдослучайных последовательностей, генерации паролей и пр. Следовательно, анализ и исследование методов синтеза симметричных криптопримитивов, разработка и теоретическое обоснование критериев и показателей эффективности, в том числе отдельных узлов современных шифров, является важной и актуальной научно-технической задачей.

Ключевым компонентом современных симметричных шифров являются нелинейные узлы (нелинейные подстановки, таблицы замен, S-блоки), которые выполняют функции скрытия статистических связей открытого текста и шифртекста, перемешивания и рассеивания данных, внесения нелинейности в процедуру зашифрования для противостояния различным криптоаналитическим и статистическим атакам. Таким образом, от показателей эффективности нелинейных узлов (сбалансированности, нелинейности, автокорреляции, корреляционной иммунности и пр.) непосредственно зависят эффективность симметричного шифра, его устойчивость к большинству известных криптографических атак и уровень обеспечиваемой им безопасности информационных технологий.

Отдельные показатели эффективности нелинейных узлов симметричных шифров рассмотрены в [3-9]. Понятие алгебраического иммунитета впервые введено в работах [10, 11] для оценки стойкости булевых функций к т.н. алгебраическому криптоанализу, предложенному в работе [12]. В работе [13] эти положения были обобщены для булевых отображений (S-блоков), для вычисления алгебраического иммунитета используется математический аппарат базисов Грёбнера.

В данной работе рассматриваются различные методы расчета алгебраического иммунитета, изучается их взаимосвязь и приводятся результаты сравнительных исследований алгебраической иммунности нелинейных узлов наиболее известных современных симметричных шифров.

2 Алгебраический иммунитет булевых функций

Понятие алгебраического иммунитета было впервые введено в работах [10,11] и подробно рассмотрено в диссертационной работе [14]. Для дальнейшего изложения материала введём необходимые определения и обозначения, придерживаясь ранее принятых в [14] формулировок.

Пусть $GF(2)$ – двоичное поле и $GF(2)^n$ – n-мерное векторное пространство над $GF(2)$.

Булева функция $f(x)$ от n переменных – это отображение $f(x): GF(2)^n \to GF(2)$, где $x = (x_1, ..., x_n)$.

Таблица истинности булевой функции $f(x)$ от n переменных – это двоичный выходной вектор значений функции, который содержит 2^n элементов, каждый элемент принадлежит множеству {0, 1}.

Алгебраическая нормальная форма (*полином Жегалкина*) булевой функции $f(x)$ от n переменных записывается в виде:

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus ... \oplus a_{(n-1)n} x_{n-1} x_n \oplus ... \oplus a_{123...n} x_1 x_2 x_3 ... x_n,$$

где коэффициенты $a_i \in \{0,1\}$ и каждая булева функция реализуется полиномом Жегалкина единственным образом, т.е. каждое представление $f(x)$ соответствует уникальной таблице истинности.

Алгебраическая степень $Deg(f)$ булевой функции $f(x)$ – число переменных в самом длинном слагаемом алгебраической нормальной формы функции, имеющем ненулевой коэффициент a_i. При этом считаем $Deg(0) = 0$.

Обозначим через V_n множество всех отображений $GF(2)^n \to GF(2)$, т.е. это множество всех возможных булевых функций $f(x)$ от n переменных.

Множество V_n в будем рассматривать и как кольцо булевых функций и как векторное (линейное) пространство над двоичным полем, т.е. $V_n = GF(2)^{2^n}$.

Булева функция $g \in V_n$ называется *аннигилятором* функции $f \in V_n$, если

$$f \cdot g = 0$$

или

$$(f + 1) \cdot g = 0.$$

Множество различных аннигиляторов булевой функции $g(x)$ образует линейное пространство, которое обозначим как

$$Ann(f) = \{g \in V_n \mid f \cdot g = 0\}.$$

Линейное пространство аннигиляторов степени $\le d$ обозначим

$$A_d^n(f) = \{g \in V_n \mid f \cdot g = 0, Deg(g) \le d\} \subset Ann(f).$$

Понятие аннигиляторов булевых функций тесно связано с оценкой эффективности алгебраического криптоанализа поточных шифров [10]. В частности, при использовании фильтрующего генератора (см. Рис. 1) псевдослучайных последовательностей (ПСП) поиск начального состояния регистра сдвига с линейной обратной связью (РСЛОС) сопряжен с понижением степени совместной системы полиномиальных булевых уравнений.

Алгоритм алгебраического криптоанализа, предложенный в [10], позволяет, при определенных условиях, по части перехваченной выходной последовательности (ПСП) находить начальное состояние РСЛОС с временной сложностью $O\left((S_n^d)^3\right)$, где

$$S_n^d = \sum_{i=0}^{d} \frac{n!}{i!(n-i)!}$$

и d - наименьшая степень ненулевого аннигилятора фильтрующей булевой функции $f(x)$ или ее инверсии $f(x)+1$.

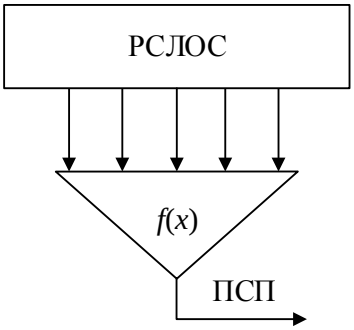

Рис. 1 – Структурная схема фильтр-генератора ПСП

Таким образом, задачей алгебраического криптоанализа является поиск ненулевых аннигиляторов или, по крайней мере, оценка их минимальной степени. С этой целью в работе [11] введено определение *алгебраической иммунности* $AI(f)$ булевой функции $f \in V_n$:

$$AI(f) = \min\{Deg(g) \mid g \in Ann(f) \text{ или } g \in Ann(f+1)\}.$$

Величина $AI(f)$ численно равна минимальной степени такой булевой функции $g \in V_n$, что $f \cdot g = 0$ или $(f+1) \cdot g = 0$.

Используя введенное выше понятие линейного пространства аннигиляторов степени $\le d$ запишем:

$$AI(f) = \min\{d \mid A_d^n(f) \neq 0 \text{ или } A_d^n(f+1) \neq 0\}, \quad (1)$$

т.е. для оценки алгебраической иммунности булевой функции $f \in V_n$ достаточно найти ненулевой базис пространства аннигиляторов наименьшей степени d.

Величина d позволяет количественно оценить сложность алгебраического криптоанализа и, при достаточно большом d, гарантировать устойчивость поточного криптоалгоритма к алгебраической атаке.

Алгоритм вычисления алгебраической иммунности булевых функций. Один из возможных алгоритмов расчета алгебраической иммунности булевых функций представлен в диссертационной работе [14]. Он основан на построении базиса линейного пространства аннигиляторов $A_d^n(f)$ заданной степени d. Итеративно увеличивая d и повторяя построение базиса пространства $A_d^n(f)$, оценку $AI(f)$ получим используя формулу (1), т.е. через ненулевой базис аннигиляторов наименьшей степени.

Для изложения сути алгоритма необходимо ввести следующие дополнительные обозначения.

Моном (одночлен) относительно переменных $x_1,...,x_n$ запишем в виде

$$x^u = \prod_{i=1}^{n} x_i^{u_i} = \begin{cases} x_i, u_i = 1, \\ 1, u_i = 0, \end{cases}$$

где вектора $x, u \in V_2^n$, $x = (x_1,...,x_n)$, $u = (u_1,...,u_n)$.

Степень одночлена x^u определяется весом Хемминга (числом ненулевых координат) $w_h(u)$ вектора $u = (u_1,...,u_n)$, т.е.

$$Deg(x^u) = w_h(u).$$

С учетом этих обозначений булеву функцию $f(x)$ в алгебраической нормальной форме (в форме полинома Жегалкина) запишем в виде

$$f(x)=\sum_{u\in GF(2)^n} a_u x^u,\ a_u\in GF(2). \quad (2)$$

Функцию (*аннигилятор*) $g\in A_d^n(f)$ также представим в виде полинома Жегалкина

$$g(x)=\sum_{v\in GF(2)^n:w_h(v)\le d} b_v x^v, \quad (3)$$

где $b_v\in GF(2)$ – неизвестные коэффициенты аннигилятора, $w_h(v)$ – вес Хемминга вектора $v=(v_1,...,v_n)$.

Функция g принадлежит пространству $A_d^n(f)$ только в том случае, если для любого $x\in GF(2)^n$ выполняется равенство $f(x)\cdot g(x)=0$.

Подставив (2) и (3) получим:

$$f(x)\cdot g(x)=\left(\sum_{u\in GF(2)^n} a_u x^u\right)\left(\sum_{v\in GF(2)^n:w_h(v)\le d} b_v x^v\right)=\sum_{u\in GF(2)^n}\left(\sum_{v\in GF(2)^n:w_h(v)\le d} a_u b_v x^{u\vee v}\right)=0,$$

где $u\vee v=(u_1\vee v_1,...,u_n\vee v_n)$, $\vee$ – дизъюнкция (логическая операция ИЛИ).

После группировки слагаемых по общему множителю, получим равенство:

$$\sum_{w\in GF(2)^n}\left(\sum_{a_u,b_v:a_u\vee b_v=w} a_u b_v\right)x^w=0, \quad (4)$$

которое выполняется для любого $w\in GF(2)^n$. Следовательно, имеем систему линейных однородных уравнений

$$\begin{cases}\sum\limits_{a_u,b_v:a_u\vee b_v=w} a_u b_v=0,\ \forall w\in GF(2)^n\end{cases} \quad (5)$$

относительно неизвестных коэффициентов b_v аннигилятора $g(x)$.

Решение данной системы уравнений (например, методом Гаусса) задает базис пространства $A_d^n(f)$.

Пример. Для $n=2$ и $d=1$ имеем:

$$f(x)=a_{00}+a_{10}x_1+a_{01}x_2+a_{11}x_1x_2,$$
$$g(x)=b_{00}+b_{10}x_1+b_{01}x_2.$$

После подстановки в $f(x)\cdot g(x)=0$ получим

$$f(x)\cdot g(x)=a_{00}b_{00}+(a_{00}b_{10}+a_{10}b_{10}+a_{10}b_{00})x_1+(a_{00}b_{01}+a_{01}b_{01}+a_{01}b_{00})x_2+$$
$$+(a_{10}b_{01}+a_{01}b_{10}+a_{11}b_{00}+a_{11}b_{10}+a_{11}b_{01})x_1x_2=0,$$

откуда имеем систему линейных однородных уравнений:

$$\begin{cases}a_{00}b_{00}=0,\\ a_{00}b_{10}+a_{10}b_{10}+a_{10}b_{00}=0,\\ a_{00}b_{01}+a_{01}b_{01}+a_{01}b_{00}=0,\\ a_{10}b_{01}+a_{01}b_{10}+a_{11}b_{00}+a_{11}b_{10}+a_{11}b_{01}=0\end{cases}$$

относительно неизвестных b_{00},b_{10},b_{01} – коэффициентов функции $g(x)$.

Тогда, например, для функции $f(x)=x_1+x_2$ (т.е. при $a_{00}=a_{11}=0$ и $a_{10}=a_{01}=1$) получим систему:

$$\begin{cases} b_{10} + b_{00} = 0, \\ b_{01} + b_{00} = 0, \\ b_{01} + b_{10} = 0, \end{cases}$$

которой удовлетворяет только два решения:

$$b_{00} = b_{10} = b_{01} = 0, \text{ т.е. } g(x) = 0,$$
$$b_{00} = b_{10} = b_{01} = 1, \text{ т.е. } g(x) = 1 + x_1 + x_2.$$

Непосредственная проверка показывает, что $g(x) = 1 + x_1 + x_2$ действительно является аннигилятором функции $f(x) = x_1 + x_2$:

$$f(x) \cdot g(x) = (x_1 + x_2)(1 + x_1 + x_2) = x_1 + x_2 + x_1 + x_1x_2 + x_1x_2 + x_2 = 0.$$

Обобщая вышеизложенное, определим основные шаги **алгоритма поиска базиса пространства аннигиляторов** [14].

Вход: $n \in \mathrm{N}, d \in \{1, ..., n\}$, функция $f(x)$ (заданная списком одночленов x^u с ненулевыми коэффициентами a_u в (2)).

Выход: Линейное пространство $A_d^n(f)$, заданное в виде параметрического семейства многочленов Жегалкина от n булевых переменных степени $\le d$.

Шаг 1. Представляем функции $f(x)$ и $g(x)$ в виде сумм (2) и (3), соответственно.

Шаг 2. Раскрываем скобки в произведении $f(x) \cdot g(x)$ и, группируя слагаемые $a_u b_v x^w$ путем сортировки по $a_u \vee b_v = w$, получаем уравнение (4).

Шаг 3. Составляем систему линейных однородных уравнений (5).

Шаг 4. Находим общее решение системы (5) в параметрическом виде и подаем на выход алгоритма.

В работе [14] приводится оценка $O\left(m \cdot \left(S_n^d\right)^3\right)$ битовой сложности рассмотренного алгоритма, где m – количество ненулевых коэффициентов a_u в (2).

Используя приведенный алгоритм поиска базиса пространства аннигиляторов можно вычислить алгебраическую иммунность булевой функции $f(x)$ последовательно перебирая все значения $d > 0$ до тех пор, пока не получим ненулевое пространство аннигиляторов $A_d^n(f)$ или $A_d^n(f+1)$.

Минимальное значение $d > 0$, для которого $A_d^n(f) \neq 0$ и/или $A_d^n(f+1) \neq 0$ соответствует значению алгебраической иммунности булевой функции $f(x)$.

Алгоритм вычисления алгебраической иммунности $AI(f)$.

Вход: $n \in \mathrm{N}$, функция $f(x)$ (заданная списком одночленов x^u с ненулевыми коэффициентами a_u в (2)).

Выход: Значение алгебраической иммунности $AI(f)$.

Шаг 1. Присваиваем $d = 1$.

Шаг 2. Вычисляем пространство аннигиляторов $A_d^n(f)$ и $A_d^n(f+1)$.

Шаг 3. Если $A_d^n(f) = 0$ и $A_d^n(f+1) = 0$, то присваиваем $d = d + 1$ и переходим к Шагу 2.

Шаг 4. Если $A_d^n(f) \neq 0$ и/или $A_d^n(f+1) \neq 0$, то присваиваем $AI(f) = d$ и подаем на выход алгоритма.

3 Алгебраический иммунитет булевых отображений (S-блоков)

Понятие алгебраической иммунности булевых функций в [13] обобщено на случай булевых отображений $F: GF(2)^n \to GF(2)^n$ (*векторных булевых функций*), которые реализуются узлами замен (*таблицами подстановок, S-блоками*) блочных симметричных шифров.

Для определения алгебраической иммунности $AI(F)$ воспользуемся терминами и определениями из работы [15].

Зафиксируем натуральные числа n, m и некоторое поле K. Рассмотрим конечную систему S из m алгебраических уравнений

$$\begin{cases} P_1(x_1, x_2, ..., x_n) = 0, \\ P_2(x_1, x_2, ..., x_n) = 0, \\ ... \\ P_m(x_1, x_2, ..., x_n) = 0 \end{cases} \quad (6)$$

от переменных $x_1, x_2, ..., x_n$ с коэффициентами над полем K.

Пусть $K[x_1, x_2, ..., x_n]$ – множество всех многочленов от переменных $x_1, x_2, ..., x_n$ с коэффициентами над полем K. На этом множестве определены операции сложения и умножения, а само множество называют *кольцом многочленов*. Это кольцо коммутативно (т.е. для любых элементов $a, b \in K[x_1, x_2, ..., x_n]$ выполняется равенство $a \cdot b = b \cdot a$), с единицей (для всех $a \in K[x_1, x_2, ..., x_n]$ выполняется равенство $a \cdot e = a$, где $e = 1$).

Непустое подмножество I коммутативного кольца с единицей R называется <u>*идеалом*</u> в R (обозначается как $I \lhd R$), если выполняются следующие два условия:

– для любых элементов $a, b \in I$ элемент $a - b \in I$;

– для любых $a \in I$ и $c \in R$ элемент $a \cdot c \in R$.

Элементы $a_1, a_2, ..., a_k$ составляют <u>*базис идеала*</u>

$$I = (a_1, a_2, ..., a_k) = \{a_1 \cdot r_1 + a_2 \cdot r_2 + ... + a_k \cdot r_k; r_1, r_2, ..., r_k \in R\} \subseteq R.$$

Принято считать, что идеал $I \lhd R$ <u>*допускает конечный базис*</u>, если в нем найдутся такие элементы $a_1, a_2, ..., a_k$, что $I = (a_1, a_2, ..., a_k)$.

Фундаментальная ***теорема Гилберта о базисе*** утверждает, что каждый идеал $I \lhd K[x_1, x_2, ..., x_n]$ допускает конечный базис, т.е. найдутся такие $f_1(x_1, x_2, ..., x_n)$, $f_2(x_1, x_2, ..., x_n)$, …, $f_k(x_1, x_2, ..., x_n) \in I$, что

$$I = (f_1, f_2, ..., f_k) = \{f_1 \cdot r_1 + f_2 \cdot r_2 + ... + f_k \cdot r_k; r_1, r_2, ..., r_k \in K[x_1, x_2, ..., x_n]\}.$$

С системой S (6) свяжем идеал I, порожденный многочленами $P_1(x_1, x_2, ..., x_n)$, $P_2(x_1, x_2, ..., x_n)$, …, $P_m(x_1, x_2, ..., x_n)$, отвечающим уравнениям системы:

$$I(S) = (P_1, P_2, ..., P_m) = \{P_1 \cdot r_1 + P_2 \cdot r_2 + ... + P_m \cdot r_m; r_1, r_2, ..., r_m \in K[x_1, x_2, ..., x_n]\}.$$

Если $F \in I(S)$, то тогда для каждого решения $(X_1, X_2, ..., X_n)$ системы (6) будет выполняться равенство

$$\begin{aligned} &F(X_1, X_2, ..., X_n) = \\ &= P_1(X_1, X_2, ..., X_n) \cdot r_1(X_1, X_2, ..., X_n) + P_2(X_1, X_2, ..., X_n) \cdot r_2(X_1, X_2, ..., X_n) + ... + \\ &+ P_m(X_1, X_2, ..., X_n) \cdot r_m(X_1, X_2, ..., X_n) = \\ &= 0 \cdot r_1(X_1, X_2, ..., X_n) + 0 \cdot r_2(X_1, X_2, ..., X_n) + ... + 0 \cdot r_m(X_1, X_2, ..., X_n) = 0. \end{aligned}$$

Если $\{P_1, P_2, ..., P_m\}$ и $\{\overline{P}_1, \overline{P}_2, ..., \overline{P}_k\}$ – два базиса одного идеала I, тогда системы алгебраических уравнений

$$\begin{cases} P_1(x_1, x_2, ..., x_n) = 0, \\ P_2(x_1, x_2, ..., x_n) = 0, \\ ... \\ P_m(x_1, x_2, ..., x_n) = 0, \end{cases} \qquad \begin{cases} \overline{P}_1(x_1, x_2, ..., x_n) = 0, \\ \overline{P}_2(x_1, x_2, ..., x_n) = 0, \\ ... \\ \overline{P}_k(x_1, x_2, ..., x_n) = 0 \end{cases}$$

эквивалентны, т.е. множества их решений совпадают.

Следовательно, множество решений системы алгебраических уравнений однозначно определяется идеалом системы, а различные базисы одного идеала отвечают эквивалентным системам [15].

Предположим, что имеется некоторый многочлен $h(x_1, x_2, ..., x_n) \in K[x_1, x_2, ..., x_n]$ и требуется за конечное число шагов выяснить, принадлежит ли он идеалу $I \lhd K[x_1, x_2, ..., x_n]$, заданному своим базисом $I = (f_1, f_2, ..., f_m)$. Другими словами, нужно решить т.н. *задачу вхождения*: – выяснить, существуют ли такие многочлены $r_1(x_1, x_2, ..., x_n)$, $r_2(x_1, x_2, ..., x_n)$, …, $r_m(x_1, x_2, ..., x_n)$, что $h = f_1 \cdot r_1 + f_2 \cdot r_2 + ... + f_m \cdot r_m$ и $h \in I = (f_1, f_2, ..., f_m)$.

Задачу вхождения решают посредством упрощения выражения для $h(x_1, x_2, ..., x_n)$ используя т.н. *редукцию многочлена*.

Запишем многочлен $h(x_1, x_2, ..., x_n)$ в виде суммы: $h = h_C + h_M$, где h_C – старший одночлен (моном), а h_M - сумма оставшихся одночленов в h. Предположим также, что h_C делится на старший член f_{iC} одного из многочленов f_i, т.е. $h_C = f_{iC} \cdot Q$ и $h = f_{iC} \cdot Q + h_M$ для некоторого одночлена Q. Тогда *операция редукции* задается выражением

$$h_1 = h - f_i \cdot Q = f_{iC} \cdot Q + h_M - f_{iC} \cdot Q - f_{iM} \cdot Q = h_M + (-f_{iM}) \cdot Q, \qquad (7)$$

где f_{iM} - сумма оставшихся одночленов в $f_i = f_{iC} + f_{iM}$. При этом старший член многочлена h_1 меньше старшего члена многочлена h. Если многочлен h принадлежит идеалу $I = (f_1, f_2, ..., f_m)$, тогда и редуцированный многочлен h_1 также будет принадлежать этому идеалу. Действительно, если $h \in (f_1, f_2, ..., f_m)$, тогда $h - h_1 = f_i Q \in (f_1, f_2, ..., f_m)$. Следовательно, задачу вхождения теперь можно решать уже не для многочлена h, а для редуцированного многочлена h_1. Если за конечное число редукций (7) многочлен h сведется (редуцируется) к нулю (ноль принадлежит любому идеалу), тогда $h \in (f_1, f_2, ..., f_m)$.

Базис $f_1, f_2, ..., f_m$ идеала $I = (f_1, f_2, ..., f_m)$ называется ***базисом Грёбнера*** этого идеала, если всякий многочлен $h \in I$ редуцируется к нулю при помощи $f_1, f_2, ..., f_m$. Иначе: набор многочленов $f_1, f_2, ..., f_m$ является базисом Грёбнера в идеале $I = (f_1, f_2, ..., f_m)$, если для любого $h \in I$ одночлен h_C делится на один из одночленов $f_{1C}, f_{2C}, ..., f_{mC}$ [15].

Для операции редукции многочленов используется понятие старшего одночлена (монома). Другими словами, предполагается, что на множестве всех одночленов кольца $K[x_1, x_2, ..., x_n]$ задан *линейный порядок* (мономиальное упорядочение $\prec$), удовлетворяющий следующим свойствам [16]:

- из $x^u \prec x^v$ следует, что $x^w \cdot x^u \prec x^w \cdot x^v$ для любых одночленов x^u, x^v, x^w (одночлены определены как в (2), т.е. $x, u, v, w \in V_2^n, x = (x_1, ..., x_n), u = (u_1, ..., u_n), v = (v_1, ..., v_n), w = (w_1, ..., w_n)$);

- $1 \preceq x^v$ для любого одночлена x^u.

В качестве примеров мономиального упорядочения приведем:

- *словарный (лексикографический) порядок (lex)*: $x^u \prec_{\text{lex}} x^v$, если существует такое i, что $u_i < v_i$ и $u_j = v_j$ для $j < i$ (сперва упорядочиваем переменные в одночленах в требуемом алфавитном порядке, а потом смотрим до первого различия в одночленах);

- *степенно-словарный порядок (deglex)*: $x^u \prec_{\text{deglex}} x^v$, если $w_h(u) < w_h(v)$ или $w_h(u) = w_h(v)$, но при этом $x^u \prec x^v$ в словарном порядке (упорядочиваем по сумме степеней, в случае равенства сумм сравниваем по словарному порядку);

- *степенной обратный словарный порядок (degrevlex)*: $x^u \prec_{\text{degrevlex}} x^v$, если $w_h(u) < w_h(v)$ или $w_h(u) = w_h(v)$, но при этом $x^u \succ_{\text{lex}} x^v$ в словарном порядке (упорядочиваем по сумме степеней, в случае равенства сумм сравниваем по обратному словарному порядку).

Решение задачи вхождения, *т.е. определение принадлежности многочлена* h *идеалу* $I = (f_1, f_2, ..., f_m)$, заключается в построении всех возможных редукций h с помощью элементов базиса Грёбнера идеала I. Многочлен h принадлежит идеалу $I = (f_1, f_2, ..., f_m)$ тогда и только тогда, когда в результате редукции получен нуль [15].

Для каждого идеала $I \lhd K[x_1, x_2, ..., x_n]$ существует базис Грёбнера, а само построение базиса Грёбнера основано на разрешении *зацеплений* [15].

Многочлены f_i и f_j имеют зацепление, если их старшие члены делятся одновременно на некоторый одночлен ω, отличный от константы. Пусть $f_{iC} = \omega \cdot q_1$, $f_{jC} = \omega \cdot q_2$, где ω – наибольший общий делитель старших одночленов f_{iC} и f_{jC}. Рассмотрим многочлен $F_{i,j} = f_i \cdot q_2 - f_j \cdot q_1 \in I$ и редуцируем его с помощью базиса $f_1, f_2, ..., f_m$ до тех пор, пока это возможно. Если полученный в результате многочлен $F'_{i,j} \equiv 0$, тогда говорят, что зацепление разрешимо. Иначе, добавим к базису $f_1, f_2, ..., f_m$ идеала I полученный многочлен $f_{m+1} = F'_{i,j}$, после чего процедуру поиска и редуцирования зацеплений продолжим. После редуцирования конечного числа зацеплений получим набор $f_1, f_2, ..., f_m, f_{m+1}, ..., f_M$, в котором каждое зацепление разрешимо.

В соответствии с ***бриллиантовой леммой*** базис $f_1, f_2, ..., f_m$ идеала $I \lhd K[x_1, x_2, ..., x_n]$ является базисом Грёбнера только тогда, когда в нем нет неразрешимых зацеплений [15].

Разрешение зацеплений позволяет определить эффективный алгоритм построения базиса Грёбнера идеала $I = (f_1, f_2, ..., f_m)$ (***алгоритм Бухбергера***).

Шаг 1. Проверяем наличие зацеплений в наборе $f_1, f_2, ..., f_m$. Если зацеплений нет, тогда набор $f_1, f_2, ..., f_m$ является базисом Грёбнера идеала $I = (f_1, f_2, ..., f_m)$. Если зацепление есть, то осуществляется переход к Шагу 2.

Шаг 2. По найденному зацеплению многочленов f_i и f_j составляем многочлен $F_{i,j} = f_i \cdot q_2 - f_j \cdot q_1$ и редуцируем его с помощью набора $f_1, f_2, ..., f_m$ пока это возможно. Если многочлен $F_{i,j}$ редуцировался к ненулевому многочлену f_{m+1}, то переходим к Шагу 3, иначе – к Шагу 4.

Шаг 3. Добавляем многочлен f_{m+1} к набору $f_1, f_2, ..., f_m$ и переходим к Шагу 4.

Шаг 4. Ищем ранее не рассмотренное зацепление и переходим к Шагу 2. Если все зацепления рассмотрены, то выводим полученный набор $f_1, f_2, ..., f_m, f_{m+1}, ..., f_M$, в котором все зацепления разрешимы. Это и есть базис Грёбнера идеала $I = (f_1, f_2, ..., f_m)$.

В настоящее время (2016 год) известны и другие алгоритмы построения базиса Грёбнера, например, алгоритмы F4, F5 [17,18].

Базис Грёбнера можно *упростить* следующими способами [15].

1. *Минимизация базиса Грёбнера*. Если f_i и f_j два элемента базиса Грёбнера, причем их старшие члены f_{iC} и f_{jC} делятся друг на друга, например, $f_{jC} \mid f_{iC}$, тогда многочлен f_i можно удалить из набора $f_1, f_2, ..., f_m$. Базис Грёбнера называют *минимальным*, если f_{iC} не делится на f_{jC} для всех $i \neq j$.
2. *Редуцирование базиса Грёбнера*. Если некоторый член q многочлена f_i делится на старший член многочлена f_j, тогда редуцируем q с помощью f_j и результат редукции запишем вместо члена q в многочлен f_i. При этом базис Грёбнера останется базисом Грёбнера, число элементов базиса не изменится, однако степени многочленов $f_1, f_2, ..., f_m$ понижаются. Базис Грёбнера называют *редуцированным*, если ни один член многочлена f_i не делится на старший член многочлена f_j для всех $i \neq j$.

Минимальный редуцированный базис Грёбнера идеала $I \lhd K[x_1, x_2, ..., x_n]$ определен однозначно (с единичными коэффициентами при старших степенях элементов базиса), т.е. не зависит от выбора исходного базиса идеала $I = (f_1, f_2, ..., f_m)$ и от последовательности проводимых операций (но зависит от упорядочения переменных $x_1, x_2, ..., x_n$) [15].

Понятие *минимального редуцированного базиса Грёбнера* было использовано в работе Жан-Шарля Фожера (Jean-Charles Faugère) [13] с целью определения алгебраической иммунности S-блоков *(нелинейных узлов усложнения)* блочных симметричных шифров.

Рассмотрим нелинейный узел (S-блок) блочного симметричного шифра (см. Рис. 2), который реализует булево отображение $S : GF(2)^n \to GF(2)^m$ [1-9].

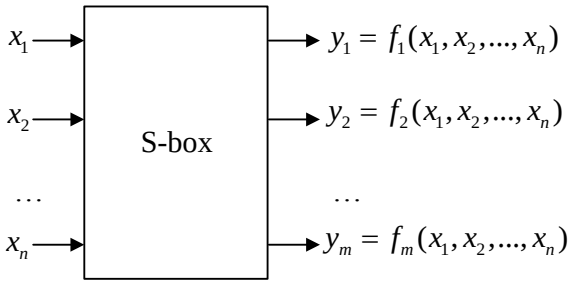

Рис. 2 – Структурная схема нелинейного узла блочного симметричного шифра

S-блок задается системой алгебраических уравнений над двоичным полем:

$$\begin{cases} f_1(x_1, x_2, ..., x_n) = y_1, \\ f_2(x_1, x_2, ..., x_n) = y_2, \\ ... \\ f_m(x_1, x_2, ..., x_n) = y_m, \end{cases} \quad (7)$$

т.е. совокупностью булевых многочленов

$$\begin{aligned} & y_1 - f_1(x_1, x_2, ..., x_n), \\ & y_2 - f_2(x_1, x_2, ..., x_n), \\ & \quad ..., \\ & y_m - f_m(x_1, x_2, ..., x_n) \end{aligned} \quad (8)$$

в кольце $K[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$ от переменных $x_1, x_2, ..., x_n, y_1, y_2, ..., y_m$ с коэффициентами над полем $K = GF(2)$.

С системой уравнений (7), алгебраически задающих структуру S-блока, свяжем идеал I, порожденный многочленами (8):

$$I(S) = (y_1 - f_1(x_1, x_2, ..., x_n), y_2 - f_1(x_1, x_2, ..., x_n), ..., y_m - f_m(x_1, x_2, ..., x_n)) =$$
$$= \{(y_1 - f_1) \cdot r_1 + (y_2 - f_1) \cdot r_2 + ... + (y_m - f_m) \cdot r_m; r_1, r_2, ..., r_m \in GF(2)[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]\}.$$

Алгебраическая иммунность нелинейного узла блочного симметричного шифра определяется как минимальная степень многочлена P из идеала $I(S)$ [13]:

$$AI(S) = \min\{\deg(P), P \in I(S) \lhd GF(2)[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]\}, \quad (9)$$

причем минимальный редуцированный базис Грёбнера идеала $I(S)$ при степенном обратном словарном упорядочении (degrevlex) содержит линейный базис полиномов P из $I(S)$, таких, что $AI(S) = \deg(P)$. Другими словами, для вычисления алгебраической иммунности $AI(S)$ достаточно построить минимальный редуцированный базис Грёбнера идеала $I(S)$, заданного уравнениями (8) и найти многочлен минимальной степени среди элементов этого базиса. Значение минимальной степени и является значением алгебраической иммунности $AI(S)$ узла замен блочного симметричного шифра.

Связь алгебраической иммунности S-блока (9) и булевой функции (1) показана на стр. 337 в работе [19].

Рассмотрим булеву функцию $f_S(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m) : GF(2)^{2n} \to GF(2)$, значения которой определим следующим образом:

$$f_S(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m) = \begin{cases} 1, \forall i, j : f_i(x_1, x_2, ..., x_n) = y_j, \\ 0, \exists i, j : f_i(x_1, x_2, ..., x_n) \neq y_j. \end{cases}$$

Множество решений уравнения

$$f_S(x_1, x_2, ..., x_n, y_1, y_2, ..., y_m) - 1 = 0$$

совпадает с множеством решений системы (7). Следовательно, имеем различные базисы $(f_S - 1)$ и $(y_1 - f_1, y_2 - f_1, ..., y_m - f_m)$ одного идеала эквивалентных систем, т.е.

$$I(f_S - 1) = I(y_1 - f_1, y_2 - f_1, ..., y_m - f_m).$$

Идеал пространства аннигиляторов $Ann(f_S)$ в кольце $GF(2)[x_1, x_2, ..., x_n, y_1, y_2, ..., y_m]$ совпадает с идеалом $I(f_S - 1)$, следовательно, алгебраическая иммунность (9) булевого отображения $S : GF(2)^n \to GF(2)^m$ совпадает с минимальной степенью ненулевых полиномов, принадлежащих аннигилятору функции f_S:

$$AI(S) = \min\{D\deg(g) \mid g \in Ann(f_S)\}.$$

Таким образом, любой S-блок можно однозначно описать булевой функцией [19], а алгебраическую иммунность этой функции можно вычислить, например, при помощи алгоритма, рассмотренного выше, в пункте 2.

4 Значения алгебраической иммунности нелинейных узлов современных шифров

В данной работе проведены сравнительные исследования алгебраической иммунности нелинейных узлов современных симметричных шифров. В качестве объектов исследования выбраны широко известные и стандартизированные на национальном и/или международном уровне блочные симметричные криптопреобразования:

- криптоалгоритм AES (стандартизирован в США, как федеральный стандарт обработки данных FIPS-197 [20], а также на международном уровне в качестве блочного шифра в ISO/IEC 18033-3 [21]);

- криптоалгоритм Camellia (стандартизирован на международном уровне в качестве блочного шифра в ISO/IEC 18033-3 [21]);
- криптоалгоритм CAST (стандартизирован на международном уровне в качестве блочного шифра в ISO/IEC 18033-3 [21]);
- криптоалгоритм SEED (стандартизирован на международном уровне в качестве блочного шифра в ISO/IEC 18033-3 [21]);
- криптоалгоритм «Калина» (национальный стандарт Украины ДСТУ 7624:2014 [22]);
- криптоалгоритм «Кузнечик» (стандартизирован в России как ГОСТ 34.12-2015 [23]);
- алгоритм «BelT» симметричного шифрования и контроля целостности Республики Беларусь (стандартизирован в СТБ 34.101.31-2011 [24]);
- криптографическая хеш-функция Whirlpool, основанная на использовании блочных симметричных криптопреобразований (стандартизирована на международном уровне в ISO/IEC 10118-3:2004 [25]).

Для вычисления алгебраического иммунитета использовалось выражение (9).

Для непосредственных вычислений использован пакет прикладного программного обеспечения Magma [26], который реализует широкий спектр функций, связанных с алгеброй, теорией групп, колец и полей, теорией чисел и многими другими разделами математики.

Исследуемые узлы замен, кроме S-блока хеш-функции Whirlpool, были подробно рассмотрены в работе [9]. В таблице 1 приведены некоторые результаты этих исследований.

Таблица 1 – Криптографические свойства нелинейных узлов блочных шифров

	B	**N**	**A**	**AD**	**PC**	**CI**	**AI**
AES	+	112	32	7	0	0	2
SEED	–	110	40	7	0	0	2
CAST-128	–	120	0	4	8	0	2
Camellia	+	112	32	7	0	0	2
«Калина»	+	104	72	7	0	0	3
«Кузнечик»	+	102	72	7	0	0	3
«BelT»	+	104	72	7	0	0	3
Whirlpool	+	95	80	7	0	0	3
Принятые обозначения:		*B – сбалансированность;*			*AD – алгебраическая степень;*		
		N – нелинейность;			*PC – критерий распространения;*		
		A – автокорреляция;			*CI – корреляционный иммунитет.*		

В последней колонке «AI» Табл. 1 приведены значения алгебраической иммунности нелинейных узлов замены современных шифров. Эти данные получены по формуле (9) посредством построения базисов Грёбнера идеалов $I(S)$, заданных совокупностями многочленов (8) из уравнений (7) соответствующих S-блоков.

Полученные результаты позволяют судить о недостаточной алгебраической иммунности нелинейных узлов блочных шифров, которые были разработаны в конце 90-х – начале 2000-х годов. Рассмотренные алгоритмы (AES, SEED, CAST-128, Camellia), представленные в современном международном стандарте ISO/IEC 18033-3, обладают сравнительно низкой алгебраической иммунностью и потенциально могут рассматриваться в качестве реальных кандидатов на построение эффективных алгебраических атак.

Напротив, блочные симметричные криптоалгоритмы «Калина», «Кузнечик», «BelT», а также криптографическая функция хеширования Whirlpool, разработаны с учетом возможного применения алгебраических атак. Нелинейные узлы замен этих алгоритмов обладают высокой алгебраической иммунностью и, по всей видимости, останутся устойчивыми к новым методам алгебраического криптоанализа.

5 Выводы

1. Методы алгебраического криптоанализа, уже с момента появления первых публикаций [27,28], превратились из абстрактных и малоприменимых математических идей в развитый и широко обсуждаемый в научном сообществе раздел современной криптологии. На сегодняшний день в этой области знаний проводится огромное число исследовательских проектов и, очевидно, что уже в ближайшие годы следует ожидать появления эффективных вычислительных алгоритмов алгебраического криптоанализа современных симметричных шифров.

2. В данной работе были рассмотрены лишь отдельные аспекты алгебраического криптоанализа, в частности, исследованы методы вычисления алгебраической иммунности нелинейных узлов симметричных шифров. Это понятие, впервые введенное для поточных криптоалгоритмов в работах [10, 11], было обобщено в [13] на случай булевых отображений, т.е. для нелинейных узлов с произвольной размерностью входов-выходов. Алгебраическая иммунность, в некотором смысле, характеризует сложность решения системы уравнений, описывающих нелинейный узел и, таким образом, позволяет получить представление об устойчивости симметричного шифра к алгебраическому криптоанализу. В частности, в работе [10] предложен алгоритм алгебраического криптоанализа поточных шифров, построенных по схеме фильтр-генератора. Сложность реализации этого алгоритма является функцией от значения алгебраической иммунности криптографической булевой функции.

3. Вычисление алгебраической иммунности нелинейного узла в общем случае сопряжено с построением базиса Грёбнера идеала кольца многочленов, заданного многочленами из уравнений блока подстановок. Эта задача решается вычислительно эффективными алгоритмами Бухбергера, F4, F5 и пр. [15-18]. Кроме того, рассмотренные математические методы могут также использоваться и для поиска эффективных алгебраических атак [19], что подтверждает перспективность и актуальность проводимых работ в данной области.

4. В данной работе приведены значения алгебраического иммунитета для узлов замен некоторых образцов современных шифров. Установлено, что криптоалгоритмы, разработанные на рубеже 90-х – начала 2000-х годов, не обладают предельными значениями алгебраической иммунности и потенциально могут рассматриваться, как кандидаты для реализации эффективных алгебраических атак. В тоже время блочные шифры последнего поколения («Калина», «Кузнечик», «BelT») учитывают возможность потенциального применения алгебраического криптоанализа и обладают предельными значениями алгебраического иммунитета.

5. Перспективным направлением являются исследования методов алгебраического криптоанализа, в частности, применение технологий квантовых вычислений для решения систем алгебраических уравнений, описывающих симметричный шифр. По мнению авторов данной работы, именно в этом направлении исследований следует ожидать наиболее значимые и интересные научные результаты.

Ссылки

[1] Menezes A. J. Handbook of Applied Cryptography / Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. – CRC Press, 1997. – 794 p.

[2] Gorbenko I.D. Prykladna kryptologija. Teorija. Praktyka. Zastosuvannja: pidruchnyk dlja vyshhyh navch. zakladiv / I.D. Gorbenko, Ju.I. Gorbenko. – Kharkiv: Vyd-vo «Fort», 2013. – 880 s.

[3] Preneel B. Analysis and Design of Cryptographic Hash Functions [Electronic resource]. – Way of access: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf.

[4] Carlet C. Vectorial boolean functions for cryptography. – Cambridge: Cambridge Univ. Press. – 95 p. [Electronic resource]. – Way of access: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf.

[5] Carlet C. Boolean functions for cryptography and error correcting codes. – Cambridge : Cambridge Univ. Press, 2007. – 148 p. [Electronic resource]. – Access mode: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf.

[6] Zepeng Z. On correlation properties of Boolean functions / Zhuo Zepeng, Zhang Weiguo // Chinese Journal of Electronics. – 2011. – Vol.20. – №1. – P.143-146.

[7] O'Connor L. An analysis of a class of algorithms for S-box construction / L. O'Connor // J. Cryptology. – 1994. – P. 133-151.

[8] Clark J.A., Jacob J.L., Stepney S. The Design of S-Boxes by Simulated Annealing / J.A. Clark, J.L. Jacob, S. Stepney // New Generation Computing. – 2005. – Issue 23(3). – P.219–231.

[9] Kuznetsov A.A. Analiz i sravnitel'nye issledovaniya nelineinykh uzlov zameny sovremennykh blochnykh simmetrichnykh shifrov / A.A. Kuznetsov, I.N. Belozertsev, A.V. Andrushkevich // Prikladnaya radioelektronika. – 2015. – T.14. – №4. – S. 343 – 350.
[10] Courtois N. Algebraic Attacks on Stream Ciphers with Linear Feedback / N. Courtois, W. Meier // Eurocrypt 2003: LNCS. – 2003. – Vol.2656. – P. 345-359.
[11] Meier W. Algebraic Attacks and Decomposition of Boolean Functions / W. Meier, E. Pasalic, C. Carlet // Eurocrypt 2004: LNCS. – 2004. – Vol.3027. – P. 474-491.
[12] Courtois N. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations / Nicolas Courtois, Josef Pieprzyk // LNCS. – 2002. – Vol.2501. – P.267–287.
[13] Ars G. Algebraic Immunities of functions over finite fields / Gw´enol´e Ars, Jean-Charles Faug`ere // RR-5532: [Research Report]. – INRIA, 2005. – P.17.
[14] Baev V. V. Effektivnye algoritmy polucheniya otsenok algebraicheskoi immunnosti bulevykh funktsii: dissertatsiya na soiskanie uchenoi stepeni kandidata fiziko-matematicheskikh nauk : 01.01.09 / Baev Vladimir Valer'evich; [Mesto zashchity: Mosk. gos. un-t im. M.V. Lomonosova. Fak. vychislit. matematiki i kibernetiki]. – Moskva, 2008. – 101 s.
[15] Arzhantsev I.V. Bazisy Grebnera i sistemy algebraicheskikh uravnenii / I.V. Arzhantsev. // Sovremennaya matematika: Letnyaya shkola (Dubna, iyul' 2002). – Moskva: MTsNMO, 2003. – 68 s.
[16] Zlobin A.I. Komp'yuternaya algebra v sisteme Sage: uchebnoe posobie / A.I. Zlobin, O.V. Sokolova. – Moskva: MGTU im. Baumana, 2011. – 55 s.
[17] Faugère J.-C. A new efficient algorithm for computing Gröbner bases / J.-C. Faugère // Journal of Pure and Applied Algebra: [F4]. –1999. – Issue 139 (1). – P.61–88.
[18] Faugère J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero / J.-C. Faugère // Proceedings of the International Symposium on Symbolic and algebraic computation (ISSAC, 2002, July): [F5] . – 2002 . – P.75–83.
[19] Gröbner Bases, Coding, and Cryptography / Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, Carlo Traverso. – Berlin: Springer-Verlag Heidelberg. – 426 p.
[20] FIPS 197. National Institute of Standards and Technology: Advanced Encryption Standard. – 2001 [Electronic resource]. – Way of access: http://www.nist.gov/aes. – Title from the screen.
[21] ISO/IEC 18033-3. Information technology – Security techniques – Encryption algorithms, Part 3: Block ciphers. – 80 p.
[22] DSTU 7624:2014. Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja. – Kyi'v: Minekonomrozvytku Ukrai'ny, 2015. – 238 s.
[23] GOST R 34.12-2015. Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Blochnye shifry. – Moskva: Standartinform, 2015. – 25 s.
[24] STB 34.101.31-2011. Informatsionnye tekhnologii i bezopasnost'. Kriptograficheskie algoritmy shifrovaniya i kon-trolya tselostnosti. – Minsk: Gosstandart, 2011. – 32 s.
[25] ISO/IEC 10118-3:2004. Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions. – 94 p.
[26] Magma Computational Algebra System [Electronic resource]. – Way of access: http://magma.maths.usyd.edu.au/magma. – Title from the screen.
[27] Courtois N. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations / Nicolas Courtois, Alexander Klimov, Jacques Patarin, Adi Shamir // Proceedings of the 19th international conference on Theory and application of cryptographic techniques EUROCRYPT'00. – 2000. – P. 392 – 407.
[28] Courtois N. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations / Nicolas Courtois, Josef Pieprzyk // Advances in cryptology (ASIACRYPT, 2002). – 2002. – P.267-287.
[29] Pyshkin A. Algebraic Cryptanalysis of Block Ciphers Using Grobner Bases: Dissertation zur Erlangung des Grades Doktor rerum naturalium / Andrey Pyshkin; [Technischen Universitat Darmstadt]. – Darmstadt, 2008. – 118 p.

Reviewer: Anton Alekseychuk, Doctor of Sciences (Engineering), Associate Prof., Institute of Special Communication and Information Security, National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine.
E-mail: alex-dtn@ukr.net

Received: December 2016.

Authors:
Alexandr Kuznetsov, Doctor of Sciences (Engineering), Full Prof., V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsov@karazin.ua
Yuriy Gorbenko, Ph.D., Senior Researcher, Institute of Information Technology (IIT), Kharkiv, Ukraine.
E-mail: YuGorbenko@iit.kharkov.ua
Ivan Belozertsev, student, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: ivanbelozersevv.jw@gmail.com
Alina Andrushkevich, Junior Researcher, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: hitori26@mail.ru
Aleksey Naregniy, Ph.D., Senior Researcher, V.N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: o.nariezhnii@karazin.ua

The algebraic immunity of nonlinear nodes symmetric ciphers.

Abstract. Researched methods for computing algebraic immunity cryptographic Boolean functions and nonlinear knots of replacements (substitutions) of symmetric ciphers. The presented results of a comparative analysis algebraic immunity of non-linear nodes of symmetric ciphers.

Keywords: symmetric ciphers, algebraic immunity, nonlinear replacement nodes.

Рецензент: Anton Alekseychuk, Doctor of Sciences (Engineering), Associate Prof., National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine.
E-mail: alex-dtn@ukr.net

Надійшло: Грудень 2016.

Автори:
Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: kuznetsov@karazin.ua
Юрій Горбенко, к.т.н., с.н.с., АТ «Інститут інформаційних технологій» (ІІТ), Харків, Україна.
E-mail: YuGorbenko@iit.kharkov.ua
Іван Білозерцев, студент, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: ivanbelozersevv.jw@gmail.com
Аліна Андрушкевіч, м.н.с, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: hitori26@mail.ru
Олексій Нарежній, к.т.н., с.н.с., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: o.nariezhnii@karazin.ua

Алгебраїчний імунітет нелінійних вузлів симетричних шифрів.

Анотація. Досліджуються методи обчислення алгебраїчної імунності криптографічних булевих функцій і нелінійних вузлів замін (підстановок) симетричних шифрів. Наводяться результати порівняльного аналізу алгебраїчної імунності нелінійних вузлів симетричних шифрів.

Ключові слова: симетричні шифри, алгебраїчний імунітет, нелінійні вузли заміни.