МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Приложение

№ 8 **Сентябрь 2015**

Свидетельство о регистрации: ПИ №ФС 77-50702
от 17 июля 2012 г.

ТРУДЫ
Всероссийской конференции
«XIV Сибирская научная школа-семинар с международным участием
“Компьютерная безопасность и криптография” — SIBECRYPT’15»
(Новосибирск, 7–12 сентября 2015 г.)

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Адрес редакции: 634050, г. Томск, пр. Ленина, 36
E-mail: vestnik_pdm@mail.tsu.ru

Всероссийская конференция «XIV Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" — SIBECRYPT'15» проведена Национальным исследовательским Томским государственным университетом, Новосибирским государственным университетом экономики и управления и Институтом математики СО РАН им. С. Л. Соболева в сотрудничестве с Институтом криптографии, связи и информатики с 7 по 12 сентября 2015 г. в Новосибирске при финансовой поддержке РФФИ (грант № 15-07-20625-г).

Теоретические основы прикладной дискретной математики
Дискретные функции
Математические методы криптографии
Математические основы компьютерной безопасности
Математические основы надёжности вычислительных и управляющих систем
Прикладная теория кодирования, автоматов и графов
Математические основы информатики и программирования
Вычислительные методы в дискретной математике

Редактор *Н. И. Шидловская*
Верстка *И. А. Панкратовой*

Подписано к печати 02.07.2015.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 17,75. Уч.-изд. л. 19,9. Тираж 300 экз. Заказ № 1146.

Отпечатано на оборудовании
Издательского Дома Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел.: 8(3822)53-15-28, 52-98-49

СОДЕРЖАНИЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

Секция 6

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ, АВТОМАТОВ И ГРАФОВ

Секция 7

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Секция 8

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.1 DOI 10.17223/2226308X/8/1

СВОЙСТВА СТАТИСТИК МАК-МАГОНА НА МНОЖЕСТВАХ СЛОВ[1]

Л. Н. Бондаренко, М. Л. Шарапова

Рассматриваются свойства статистик Мак-Магона maj и inv на трёх множествах слов над алфавитом $\{1,\dots,n\}$: 1) перестановки степени n; 2) все слова длины n; 3) вогнутые перестановки степени n. На множествах п. 1 и 3 получены новые рекурсивные описания производящих многочленов пар $(\mathrm{des},\mathrm{maj})$ и $(\mathrm{des},\mathrm{inv})$; на множестве слов п. 2 найдены только соответствующие рекурсивные описания для пары $(\mathrm{des},\mathrm{maj})$ и статистики inv. Эти рекурсивные описания использованы на множествах п. 1 и 2 для другого доказательства известной теоремы Мак-Магона о совпадении распределений maj и inv. На множестве слов п. 2 определены статистики fas и cas как особые средние значения символа в слове, причем fas и des одинаково распределены, и доказана теорема о совпадении распределений пар $(\mathrm{fas},\mathrm{maj})$ и $(\mathrm{fas},\mathrm{inv})$, а также пар $(\mathrm{cas},\mathrm{maj})$ и $(\mathrm{cas},\mathrm{inv})$.

Ключевые слова: *статистики Мак-Магона, производящий многочлен, рекурсивное описание, статистики Эйлера.*

Для слов $\sigma = \sigma_1 \dots \sigma_l$ длины $l = r_1 + \dots + r_n$ над алфавитом $\{1,\dots,n\}$, являющихся перестановками мультимножества $M = \{1^{r_1},\dots,n^{r_n}\}$ (иначе, $\sigma \in S(M)$), функции $\mathrm{maj}(\sigma) = \sum\limits_{i=1,\sigma_i>\sigma_{i+1}}^{l-1} i$ и $\mathrm{inv}(\sigma) = \#\{(i,j) : 1 \leqslant i < j \leqslant l, \sigma_i > \sigma_j\}$ называются статистиками Мак-Магона [1]. Справедлива известная теорема Мак-Магона: $\sum\limits_{\sigma\in S(M)} q^{\mathrm{maj}(\sigma)} = \sum\limits_{\sigma\in S(M)} q^{\mathrm{inv}(\sigma)} = G_\lambda(q)$, т. е. гауссовский полиномиальный коэффициент $G_\lambda(q) = \begin{bmatrix} l \\ r_1,\dots,r_l \end{bmatrix}_q = \dfrac{(q;q)_l}{(q;q)_{r_1}\dots(q;q)_{r_l}}$, где $\lambda = (1^{r_1}\dots l^{r_l})$ — разбиение числа l, а $(t;q)_l = (1-t)(1-tq)\dots(1-tq^{l-1})$, служит производящим многочленом статистик Мак-Магона на $S(M)$ [2], иначе эти статистики одинаково распределены на $S(M)$.

При длине $l = n$ и $r_1 = \dots = r_n = 1$, т. е. $\sigma \in S_n$, в [1] приводится рекурсивное описание полиномов $A_n(t,q)$, задающих, как показал Л. Карлитц, распределение пары $(\mathrm{des},\mathrm{maj})$, где $\mathrm{des}(\sigma) = \#\{i : 1 \leqslant i \leqslant n, \sigma_i > \sigma_{i+1}, \sigma_{n+1} = 0\}$, а также описание полиномов $A^*_n(t,q)$, задающих распределение пары $(\mathrm{des},\mathrm{inv})$, с помощью соответствующей производящей функции, найденное Р. Стенли. Отметим, что в [1] вместо des употребляется статистика rize, причём $\mathrm{des}(\sigma) = \mathrm{rize}(\mathbf{c}\sigma)$, где инволюция $\mathbf{c} : S_n \to S_n$ определяется соотношением $\mathbf{c}\sigma_i = n + 1 - \sigma_i$, $i = 1,\dots,n$.

Рассмотрим получение рекурсивных описаний производящих многочленов пар $(\mathrm{des},\mathrm{maj})$ и $(\mathrm{des},\mathrm{inv})$ на трёх множествах слов σ длины n над алфавитом $\{1,\dots,n\}$: 1) перестановки $\sigma \in S_n$; 2) все слова $\sigma \in \widehat{S}_n$; 3) вогнутые перестановки $\sigma \in \widetilde{S}_n$, у

[1]Работа поддержана грантом РФФИ, проект № 14-01-00273.

которых префикс задает убывающую, а оставшийся после его удаления суффикс — возрастающую последовательность символов [3]. Отметим, что $|S_n| = n!$, $|\widehat{S}_n| = n^n$, $|\widetilde{S}_n| = 2^{n-1}$ и $\widetilde{S}_n \subset S_n \subset \widehat{S}_n$ при $n \geqslant 3$.

Теорема 1. На множестве перестановок S_n производящие многочлены $A_n(t,q)$ пары $(\mathrm{des}, \mathrm{maj})$ и $A^*_n(t,q)$ пары $(\mathrm{des}, \mathrm{inv})$ имеют следующие рекурсивные описания при $A_{1,1}(t,q)) = A^*_{1,1}(t,q) = t$ и $m = 2, \ldots, n$, $k = 1, \ldots, m$:

$$A_{m,k}(t,q) = tq^{n-m+1} \sum_{i=1}^{k-1} A_{m-1,i}(t,q) + \sum_{i=k}^{m-1} A_{m-1,i}(t,q),\ A_n(t,q) = \sum_{k=1}^{n} A_{n,k}(t,q),$$

$$A^*_{m,k}(t,q) = q^{k-1} \left(t \sum_{i=1}^{k-1} A^*_{m-1,i}(t,q) + \sum_{i=k}^{m-1} A^*_{m-1,i}(t,q) \right),\ A^*_m(t,q) = \sum_{k=1}^{m} A^*_{m,k}(t,q).$$

Рекурсивное описание $A_n(t,q)$ теоремы 1 значительно отличается от их рекурсивного описания в [1], а соответствующее описание $A^*_n(t,q)$ в [1] отсутствует (в [4] приведены два рекуррентных соотношения для многочленов $A^*_n(t,q)$).

Теорема 2. На множестве слов $\widehat{S}_n$ производящие многочлены $\widehat{A}_n(t,q)$ пары $(\mathrm{des}, \mathrm{maj})$ и $\widehat{B}^*_n(q)$ статистики inv при $k = 1, \ldots, n$, $\widehat{A}_{1,k}(t,q)) = 1$, $\widehat{B}^*_{1,k}(t,q) = 1$ и $m = 2, \ldots, n$ имеют следующие рекурсивные описания:

$$\widehat{A}_{m,k}(t,q) = tq^{n-m+1} \sum_{i=1}^{k-1} \widehat{A}_{m-1,i}(t,q) + \sum_{i=k}^{n} \widehat{A}_{m-1,i}(t,q),\ \widehat{A}_n(t,q) = \sum_{k=1}^{n} \widehat{A}_{n,k}(t,q),$$

$$\widehat{B}^*_{m,k}(q) = q^{m-1} \sum_{i=1}^{k-1} \widehat{B}^*_{m-1,i}(q) + \sum_{i=k}^{n} \widehat{B}^*_{m-1,i}(q),\ \widehat{B}^*_n(q) = \sum_{k=1}^{n} \widehat{B}^*_{n,k}(q).$$

Применение теоремы Мак-Магона к множеству слов $\widehat{S}_n$ приводит к следующему соотношению: $\widehat{B}_n(q) = \widehat{B}^*_n(q) = \sum\limits_{|\lambda|=n} \binom{n}{\#\lambda} c_\lambda G_\lambda(q)$, где $\widehat{B}_n(q) = \widehat{A}_n(1,q)$; λ — разбиение числа n; $|\lambda|$ — вес, а $\#\lambda$ — число частей разбиения λ; c_λ — число композиций, соответствующих разбиению λ с записанными $n - \#\lambda$ нулями; $G_\lambda(q)$ — гауссовский полиномиальный коэффициент.

Теорема 3. На множестве вогнутых перестановок $\widetilde{S}_n$ производящие многочлены $\widetilde{A}_n(t,q)$ пары $(\mathrm{des}, \mathrm{maj})$ и $\widetilde{A}^*_n(t,q)$ пары $(\mathrm{des}, \mathrm{inv})$ имеют тривиальные рекурсивные описания, которые приводят к соотношениям

$$\widetilde{A}_n(t,q) = \sum_{k=1}^{n} \binom{n-1}{k-1} q^{k(k-1)/2}\, t^k,\ \widetilde{A}^*_n(t,q) = \sum_{k=1}^{n} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q q^{k(k-1)/2}\, t^k = \frac{t(-t;q)_{n+1}}{1+t}$$

с биномиальными и соответственно q-биномиальными коэффициентами (аналогичное выражение для $\widetilde{A}^*_n(t,q)$ имеется в [3]).

Доказательство теорем 1–3 основано на лексикографическом упорядочении S_n, $\widehat{S}_n$, $\widetilde{S}_n$ и рассмотрении их начальных частей, имеющих соответственно мощности $m!$, n^m, 2^{m-1}, $m = 1, \ldots, n$. Эти подмножества дополнительно разбиваются соответственно на m, n и m частей, а затем применяется определение статистик и индукция.

Иное упорядочение множеств S_n и $\widehat{S}_n$ позволяет упростить рекурсивные описания многочленов пары $(\mathrm{des}, \mathrm{maj})$ теорем 1 и 2, в которых множитель q^{n-m+1} заменяется на q^{m-1} и $A_m(t,q) = \sum\limits_{k=1}^{m} A_{m,k}(t,q)$, а сравнение полученных рекурсивных описаний приводит к другому доказательству равенств $A_n(1,q) = A^*_n(1,q)$ и $\widehat{A}_n(1,q) = \widehat{B}^*_n(q)$.

Определение 1. Статистики $\mathrm{fas}(\sigma) = \left\lfloor n^{-1} \sum_{i=1}^{n} \sigma_i \right\rfloor$ и $\mathrm{cas}(\sigma) = \left\lceil n^{-1} \sum_{i=1}^{n} \sigma_i \right\rceil$ задают соответственно «пол» и «потолок» средней величины символа в слове $\sigma \in \widehat{S}_n$.

Статистика fas (под именем mes) введена в [5], где с помощью рекурсивного описания установлено, что fas и des на $\widehat{S}_n$ имеют производящий многочлен $\widehat{A}_n(t, 1)$, иначе, fas и des — эйлеровы статистики на $\widehat{S}_n$. Легко показать, что $\mathrm{fas}(\sigma) + \mathrm{cas}(\mathbf{c}\sigma) = n + 1$, т. е. многочлен $t^{n+1}\widehat{A}_n(t^{-1})$ является производящим для статистики cas.

Теорема 4. Пары $(\mathrm{fas}, \mathrm{maj})$ и $(\mathrm{fas}, \mathrm{inv})$, а также пары $(\mathrm{cas}, \mathrm{maj})$ и $(\mathrm{cas}, \mathrm{inv})$ одинаково распределены на $\widehat{S}_n$.

Доказательство. Разобьём $\widehat{S}_n$ на минимальное число подмножеств, состоящих из перестановок подходящих мультимножеств символов из алфавита $\{1, \ldots, n\}$. По теореме Мак-Магона и определению 1 пары $(\mathrm{fas}, \mathrm{maj})$ и $(\mathrm{fas}, \mathrm{inv})$, а также пары $(\mathrm{cas}, \mathrm{maj})$ и $(\mathrm{cas}, \mathrm{inv})$ одинаково распределены на этих подмножествах, что и приводит к требуемому утверждению. ■

Отметим, что для пары $(\mathrm{des}, \mathrm{maj})$ на S_n неизвестна одинаково распределённая с ней пара $(\mathrm{e}, \mathrm{inv})$, где e — эйлерова статистика [1].

ЛИТЕРАТУРА

1. *Фоата А.* Распределения типа Эйлера и Мак-Магона на группе перестановок // Проблемы комбинаторного анализа. М.: Мир, 1980. С. 120–141.
2. *Эндрюс Г.* Теория разбиений. М.: Наука, 1982. 256 с.
3. *Гульден Я., Джексон Д.* Перечислительная комбинаторика. М.: Наука, 1990. 504 с.
4. *Chow C.* A recurrence relation for the "inv" analogue of q-Eulerian polynomials // Electronic J. Combinatorics. 2010. V. 17. #N22.
5. *Бондаренко Л. Н., Шарапова М. Л.* Статистики спусков и средних на множествах слов // Проблемы теоретической кибернетики. Материалы XVII Междунар. конф. (Казань, 18–20 июня 2014 г.). Казань: Отечество, 2014. С. 63–65.

УДК 519.6 DOI 10.17223/2226308X/8/2

О ПРИМИТИВНОСТИ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ ПРЕОБРАЗОВАНИЙ РЕГИСТРОВ СДВИГА С ДВУМЯ ОБРАТНЫМИ СВЯЗЯМИ

А. М. Дорохова

Среди преобразований двоичных регистров сдвига с двумя обратными связями выделен класс подстановок, для которого получен критерий примитивности перемешивающих графов. Получены оценки экспонентов некоторых примитивных графов из данного класса.

Ключевые слова: *перемешивающий граф преобразования, регистр сдвига, экспонент графа.*

Введение. Актуальность исследования перемешивающих свойств криптографических функций достаточно обоснована в ряде работ (см., например, [1 – 5]). Точное определение существенных переменных итеративных функций весьма трудоёмко, поэтому применяется оценочный матрично-графовый подход. Перемешивающие свойства преобразования векторного пространства V_n над полем $\mathrm{GF}(2)$ кодируются перемешиваю-

щей $0,1$-матрицей порядка n или, что равносильно, перемешивающим n-вершинным орграфом Γ, у которого матрица смежности вершин совпадает с M. Для итеративных преобразований оценка перемешивающих свойств состоит в распознавании примитивности матрицы M (графа Γ) и определении экспонента.

Примитивность и экспонент изучены для различных классов матриц и графов [2]. Перемешивающие графы подстановочных регистров сдвига с одной обратной связью изучались в [3–5]. В развитие данной тематики в работе оцениваются перемешивающие свойства одного класса подстановок регистров сдвига с двумя обратными связями.

1. Биективные регистры сдвига с двумя обратными связями. Преобразование $\varphi(x_1,\ldots,x_{n+m})$ множества V_{n+m} автономного регистра левого сдвига длины $n+m$ с двумя обратными связями задаётся координатными булевыми функциями:

$$\varphi(x_1,\ldots,x_{n+m})=(x_2,\ldots,x_n,\varphi_n(x_1,\ldots,x_{n+m}),x_{n+2},\ldots,x_{n+m},\varphi_{n+m}(x_1,\ldots,x_{n+m})). \quad (1)$$

Рассмотрим класс указанных преобразований регистров сдвига (обозначим его $R(g,h)$), где

$$\varphi_n(x_1,\ldots,x_{n+m}) = x_{n+1}\oplus h(x_{n+2},\ldots,x_{n+m}); \quad (2)$$

$$\varphi_{n+m}(x_1,\ldots,x_{n+m}) = x_1\oplus g(x_1,\ldots,x_n). \quad (3)$$

Регистр из класса $R(g,h)$ изображён на рис. 1.

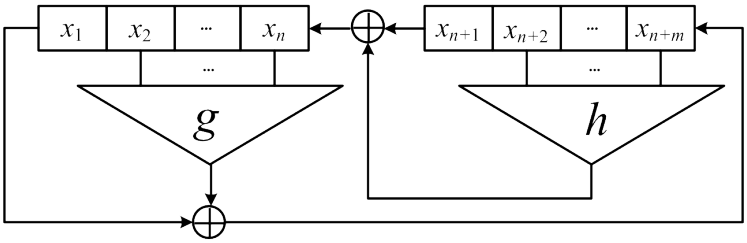

Рис. 1. Регистр сдвига с двумя обратными связями

Система функций $\Phi=\{f_1(x_1,\ldots,x_{n+m}),f_2(x_1,\ldots,x_{n+m})\}$ называется биективной по множеству переменных $\{x_i,x_j\}$, если она реализует биективное преобразование множества $\{0,1\}^2$ при любой фиксации переменных $\{x_1,\ldots,x_{n+m}\}\setminus\{x_i,x_j\}$ [6]. В силу соотношений (2), (3) система функций $\{\varphi_n,\varphi_{n+m}\}$ биективна по множеству переменных $\{x_{n+1},x_1\}$ и класс $R(g,h)$ состоит из подстановок в соответствии с теоремой 1 из [6].

2. Свойства перемешивающего графа. Обозначим через φ регистровую подстановку с двумя обратными связями, координатные функции которой заданы формулами (2) и (3) соответственно; через Δ и D — множества номеров существенных переменных соответственно функций φ_{n+m} и φ_n: $\Delta=\{\delta_1,\ldots,\delta_k\}$, $D=\{d_1,\ldots,d_q\}$, где $1=\delta_1<\ldots<\delta_k\leqslant n$, $n+1=d_1<\ldots<d_q\leqslant n+m$.

Исследуем примитивность $(n+m)$-вершинного перемешивающего орграфа $\Gamma(\varphi)$ подстановки φ. Необходимым условием примитивности орграфа $\Gamma(\varphi)$ является сильная связность.

Обозначим через Γ_0 граф $\Gamma(\varphi)$ при $h(x_{n+2},\ldots,x_{n+m})=g(x_2,\ldots,x_n)\equiv 0$. Из равенств (1)–(3) следует, что орграф Γ_0 представляет собой гамильтонов контур длины $n+m$. Так как Γ_0 — часть орграфа $\Gamma(\varphi)$ при любых функциях $h(x_{n+2},\ldots,x_{n+m})$ и $g(x_2,\ldots,x_n)$, то орграф $\Gamma(\varphi)$ сильносвязный.

Опишем контуры орграфа $\Gamma(\varphi)$. Для последовательности $w_0, w_1, \ldots, w_l$ путей в орграфе $\Gamma(\varphi)$ определим операцию конкатенации (обозначается символом $\cdot$). Если конечная вершина предыдущего пути совпадает с начальной вершиной следующего, то результатом операции является путь $w = w_0 \cdot w_1 \cdot \ldots \cdot w_l$. Обозначим $[i, j]$ путь w из вершины i в вершину j в орграфе $\Gamma(\varphi)$, $L(w)$ — длина пути w в орграфе $\Gamma(\varphi)$.

Числа множеств D и Δ определяют в $\Gamma(\varphi)$ простые контуры

$$C_{i,j} = [n, \delta_i] \cdot \mu \cdot [n + m, d_j] \cdot \nu,$$

где $\mu = (\delta_i, n + m)$ и $\nu = (d_j, n)$ — дуги орграфа $\Gamma(\varphi)$, длина контура $C_{i,j}$ определена равенством $L(C_{i,j}) = 2n + m + 2 - \delta_i - d_j$, $1 \leqslant i \leqslant q$, $1 \leqslant j \leqslant k$. Орграф $\Gamma(\varphi)$ изображён на рис. 2.

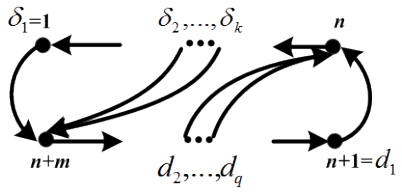

Рис. 2. Перемешивающий орграф $\Gamma(\varphi)$

Множество $\{a_1, \ldots, a_p\}$ натуральных чисел называется примитивным, если $(a_1, \ldots, a_p) = 1$. Обозначим $S = \{2n + m + 2 - \delta_i - d_j : i = 1, \ldots, q,\ j = 1, \ldots, k\}$. Справедлив следующий критерий примитивности.

Теорема 1. Перемешивающий орграф $\Gamma(\varphi)$ примитивный, если и только если множество S примитивное.

3. Оценки экспонента. Верны оценки экспонента для некоторых примитивных орграфов $\Gamma(\varphi)$.

Утверждение 1. Если $(n + 1, m - 1) = 1$ и $n + m \in D$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) \leqslant n^2 + nm + 2m - 2$.

Оценка экспонента следует из теоремы 1 [7] при $l = n + m$, $\lambda = h = n + 1$.

Утверждение 2. Если $(m + 1, n - 1) = 1$ и $n \in \Delta$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) \leqslant m^2 + mn + 2n - 2$.

Оценка экспонента следует из теоремы 1 [7] при $l = n + m$, $\lambda = h = m + 1$.

Утверждение 3. Если в D (или в Δ) имеются числа a, b, такие, что $a - b = 1$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) = \lambda^2 + 2b - 1$, где $\lambda = n + m - b$.

Оценка экспонента следует из теоремы 1 [7] при $l = \lambda + 1$, $h = \lambda$.

Обозначим через $\mu(n, m)$ чётное число из пары чисел n и m разной чётности.

Утверждение 4. Если числа n и m разной чётности, $n \in \Delta$, $n + m \in D$, то орграф $\Gamma(\varphi)$ примитивный и $\exp \Gamma(\varphi) \leqslant \mu(n, m) + 2(n + m) - 3$.

Оценка экспонента следует из теоремы 1 [7] при $l = \mu(n, m) + 1$, $\lambda = h = 2$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
3. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3(17). С. 34–40.
4. *Дорохова А. М., Фомичев В. М.* Уточненные оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов // Прикладная дискретная математика. 2014. № 1(23). С. 77–83.
5. *Дорохова А. М.* Оценки экспонентов перемешивающих графов некоторых модификаций аддитивных генераторов // Прикладная дискретная математика. Приложение. 2014. № 7. С. 60–64.
6. *Коренева А. М.* О блочных шифрах, построенных на основе регистров сдвига с двумя обратными связями // Прикладная дискретная математика. Приложение. 2013. № 6. С. 39–41.
7. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.

УДК 519.6 DOI 10.17223/2226308X/8/3

О ЛОКАЛЬНЫХ ЭКСПОНЕНТАХ ПЕРЕМЕШИВАЮЩИХ ГРАФОВ ФУНКЦИЙ, РЕАЛИЗУЕМЫХ АЛГОРИТМАМИ ТИПА A5/1

С. Н. Кяжин, В. М. Фомичев

Для реализуемых алгоритмами типа A5/1 преобразований, построенных на основе линейных регистров сдвига длин n, m и p с характеристическими многочленами веса ν, μ и π соответственно, показана примитивность перемешивающих графов. Получены верхняя и нижняя оценки экспонента и локального экспонента перемешивающего графа Γ, зависящие от указанных параметров: $1+\max\{\lceil n/\nu\rceil, \lceil m/\mu\rceil, \lceil p/\pi\rceil\} \leqslant \exp\Gamma \leqslant \max\{n, m, p\}$. Для перемешивающего графа Γ преобразования генератора A5/1 получено значение экспонента $\exp\Gamma$ и локального экспонента $*J\text{-}\exp\Gamma$ при $J = \{1, 20, 42\}$, равное 21, что согласуется с длиной холостого хода генератора.

Ключевые слова: *генератор A5/1, примитивный граф, экспонент, локальный экспонент.*

Алгоритм A5/1 [1, с. 389] — поточный шифр гаммирования, построенный на основе трёх линейных регистров сдвига (ЛРС) над GF(2) длин 19, 22 и 23. Сумма битов, снимаемых с крайних ячеек ЛРС, образует гамму. Нелинейность преобразования состояний генератора достигается за счёт самоуправляемой схемы неравномерного движения регистров (каждый такт 2 или 3 регистра сдвигаются на 1 шаг).

Опишем перемешивающий граф Γ для обобщения генератора A5/1. Обозначим $(x_1, \ldots, x_{n+m+p})$ начальное состояние генератора, $S(f)$ — множество номеров существенных переменных функции f. Пусть генератор состоит из трёх регистров длин n, m и p с функциями обратной связи f_1, f_2 и f_3, чьи множества точек съёма суть $S(f_1) = \{b_1, \ldots, b_\nu\}$, $S(f_2) = \{c_1, \ldots, c_\mu\}$ и $S(f_3) = \{d_1, \ldots, d_\pi\}$ соответственно. Движение ЛРС на 0–1 шагов определено булевой функцией $u(x_t, x_\tau, x_\theta)$ от трёх существенных переменных, где $S(u) = \{t, \tau, \theta\}$; $1 \leqslant t \leqslant n$; $t \notin S(f_1)$; $n+1 \leqslant \tau \leqslant n+m$; $\tau \notin S(f_2)$; $n+m+1 \leqslant \theta \leqslant n+m+p$; $\theta \notin S(f_3)$. Тогда преобразование g состояний генератора за-

дано системой булевых функций $g = \{g_1(x_1, \ldots, x_{n+m+p}), \ldots, g_{n+m+p}(x_1, \ldots, x_{n+m+p})\}$, где

$$\begin{gathered} S(g_n) = S(f_1) \cup \{n\} \cup S(u), S(g_i) = \{i, i+1\} \cup S(u),\ i = 1, \ldots, n-1, \\ S(g_{n+m}) = S(f_2) \cup \{n+m\} \cup S(u), \\ S(g_i) = \{i, i+1\} \cup S(u), i = n+1, \ldots, n+m-1, \\ S(g_{n+m+p}) = S(f_3) \cup \{n+m+p\} \cup S(u), \\ S(g_i) = \{i, i+1\} \cup S(u),\ i = n+m+1, \ldots, n+m+p-1. \end{gathered} \tag{1}$$

Из равенств (1) следует, что в Γ в каждой вершине имеется петля. Соответствующие ЛРС подграфы графа Γ являются сильносвязными, и имеются дуги (t, s), (τ, s) и (θ, s) при любом $s = 1, \ldots, n+m+p$. Следовательно, орграф Γ сильносвязный, примитивный.

Определим $\exp\Gamma$ и локальный экспонент $*J\text{-}\exp\Gamma$ [2] при $J = \{1, n+1, n+m+1\}$. Так как Γ содержит $n+m+p$ петель и дуги (t, s), (τ, s) и (θ, s), $s = 1, \ldots, n+m+p$, то в соответствии с теоремой 2 [3]

$$\exp\Gamma = 1 + \max\{\max_{i=1,\ldots,n} \rho(i, t), \max_{i=n+1,\ldots,n+m} \rho(i, \tau), \max_{i=n+m+1,\ldots,n+m+p} \rho(i, \theta)\}, \tag{2}$$

где $\rho(i, a)$ — длина кратчайшего пути в Γ от i до a, при этом $\rho(i, i) = 0$.

Пусть $A \subseteq \{1, \ldots, n+m+p\}$, обозначим $\rho(i, A) = \min\limits_{a \in A} \rho(i, a)$, где $\rho(i, A) = 0$, если $i \in A$. Тогда

$$\rho(i, t) = \rho(i, S(f_1)) + 1 + n - t \text{ при } i < t, \rho(i, t) = i - t \text{ при } i > t; \tag{3}$$

$$\rho(i, \tau) = \rho(i, S(f_2)) + 1 + n + m - \tau \text{ при } i < \tau, \rho(i, \tau) = i - \tau \text{ при } i > \tau; \tag{4}$$

$$\rho(i, \theta) = \rho(i, S(f_3)) + 1 + n + m + p - \theta \text{ при } i < \theta, \rho(i, \theta) = i - \theta \text{ при } i > \theta. \tag{5}$$

Из равенств (2)–(5) следует

$$\begin{gathered} \exp\Gamma = 2 + \max\{n - t + \max_{i=1,\ldots,t-1} \rho(i, S(f_1)), \\ n + m - \tau + \max_{i=n+1,\ldots,\tau-1} \rho(i, S(f_2)), n + m + p - \theta + \max_{i=n+m+1,\ldots,\theta-1} \rho(i, S(f_3))\}. \end{gathered} \tag{6}$$

Из (6) в данных условиях получаем:

1) $\exp\Gamma$ принимает наименьшее значение, равное $1 + \max\{\lceil n/\nu \rceil, \lceil m/\mu \rceil, \lceil p/\pi \rceil\}$, если $t = n$, $\tau = n+m$, $\theta = n+m+p$ и множества $S(f_1)$, $S(f_2)$ и $S(f_3)$ разделяют приблизительно на равные отрезки соответственно числовые множества $\{1, \ldots, n\}$, $\{n+1, \ldots, n+m\}$ и $\{n+m+1, \ldots, n+m+p\}$;
2) $\exp\Gamma$ принимает наибольшее значение, равное $\max\{n, m, p\}$, если $t = 1$, $\tau = n+1$, $\theta = n+m+1$.

В силу наличия в Γ дуг (t, s), (τ, s) и (θ, s) при любом $s = 1, \ldots, n+m+p$ оценка локального экспонента $*J\text{-}\exp\Gamma$ не зависит от J и совпадает с оценкой экспонента Γ.

В схеме генератора A5/1 $n = 19$, $m = 22$, $p = 23$, $\nu = 4$, $\mu = 2$, $\pi = 4$. Расчёты показали, что $*J\text{-}\exp\Gamma = 21$, где $J = \{1, 20, 42\}$.

Длина холостого хода генератора A5/1 (количество начальных тактов, при которых знаки гаммы игнорируются) равна 100, то есть более чем в 4 раза превышает значение экспонента. Это, по-видимому, надёжно обеспечивает зависимость каждого знака гаммы от всех знаков начального состояния генератора и делает конструктивно обоснованным выбор длины холостого хода.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
3. *Фомичев В. М.* Свойства путей в графах и мультиграфах // Прикладная дискретная математика. 2010. № 1(7). С. 118–124.

УДК 519.7 DOI 10.17223/2226308X/8/4

О НЕКОТОРЫХ МЕТРИЧЕСКИХ СВОЙСТВАХ ЛИНЕЙНЫХ ПОДПРОСТРАНСТВ БУЛЕВА КУБА[1]

А. К. Облаухов

Исследуются метрические дополнения подмножеств булева куба. Дана общая характеризация метрических дополнений линейных подпространств. Доказано, что полностью регулярные коды являются метрически регулярными.

Ключевые слова: *подпространство, метрически регулярное множество, метрическое дополнение, полностью регулярный код.*

Через $\mathbb{F}_2^n$ в работе обозначается множество всех двоичных векторов длины n. *Расстоянием Хэмминга* от вектора $y \in \mathbb{F}_2^n$ до множества $X \subseteq \mathbb{F}_2^n$ называется $\mathrm{d}(y, X) = \min\limits_{x \in X} \mathrm{wt}(y \oplus x)$, $\mathrm{wt}(\cdot)$ — двоичный вес (число единиц в векторе). *Максимальным расстоянием* от множества $X \subseteq \mathbb{F}_2^n$ называется $\mathrm{d}(X) = \max\limits_{z \in \mathbb{F}_2^n} \mathrm{d}(z, X)$. Вектор y называется *максимально удалённым* от множества X, если $\mathrm{d}(y, X) = \mathrm{d}(X)$. Через $|X|$ обозначается мощность множества X, через $\mathrm{supp}(y)$ — носитель вектора y — множество $\{i : y_i = 1\}$. *Сдвигом* множества X на вектор $a \in \mathbb{F}_2^n$ называется множество $a \oplus X = \{a \oplus x : x \in X\}$.

Множество $Y \subseteq \mathbb{F}_2^n$, состоящее из всех максимально удалённых от множества X векторов, назовём *метрическим дополнением* множества X и обозначим $Y = \widehat{X}$. Множество $X \subseteq \mathbb{F}_2^n$ называется *метрически регулярным*, если $X = \widehat{\widehat{X}}$.

В [1] была поставлена задача классификации метрически регулярных множеств. Известно [2], что множество всех аффинных функций метрически регулярно.

Исследуются свойства метрических дополнений линейных подпространств. Множество $L \subseteq \mathbb{F}_2^n$ называется *линейным подпространством*, если для любых векторов $x, y \in L$ их сумма $x \oplus y$ лежит в L. Следующие два утверждения характеризуют метрические дополнения линейных подпространств.

Утверждение 1. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда множество $\widehat{L}$ — это объединение сдвигов подпространства L. Пусть $a \in \mathbb{F}_2^n$ — произвольный вектор. Тогда расстояние от L до любого вектора из сдвига $a \oplus L$ совпадает с расстоянием от L до вектора a.

Теорема 1. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k. Тогда

$$\mathrm{d}(L) \leqslant n - k.$$

У каждого линейного подпространства L существует единственный базис специального вида, который назовём *каноническим базисом*. Матрица из векторов этого базиса имеет вид

[1]Исследование выполнено при финансовой поддержке РФФИ (проект № 15-31-20635).

$$M = \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccccccc} & & & s_1 & & s_2 & & s_3 & & & & s_k & \\ \end{array} \\ \begin{pmatrix} 0 & \dots & 0 & 1 & * & 0 & * & 0 & * & \dots & * & 0 & * \\ 0 & \dots & \dots & \dots & 0 & 1 & * & 0 & * & \dots & * & 0 & * \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 & 1 & * & \dots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & * & 0 & * \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 0 & 1 & * \end{pmatrix} \end{array}.$$

Каноническим представителем назовём вектор, у которого в координатах s_i, $i = 1, \dots, k$, находятся нули, а остальные координаты произвольны. Нетрудно доказать, что канонические представители определяют все сдвиги подпространства, причём два разных представителя определяют два разных сдвига.

Теорема 2. Равенство в оценке теоремы 1 достигается тогда и только тогда, когда $\mathrm{wt}(e_i) \leqslant 2$ для всех $i \in \{1, \dots, k\}$, где $\{e_i : i = 1, \dots, k\}$ — канонический базис L. Множество $\widehat{L}$ в таком случае совпадает со сдвигом $a \oplus L$, где a — канонический представитель максимального веса.

Теорема 3. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство размерности k, $\mathrm{wt}(e_i) \leqslant 3$ для всех e_i из канонического базиса L и существует вектор канонического базиса веса 3. Тогда $\mathrm{d}(L) = n - k - 1$ тогда и только тогда, когда $\mathrm{supp}(e_i) \cap \mathrm{supp}(e_j) \neq \varnothing$ для всех i, j, таких, что $\mathrm{wt}(e_i) = \mathrm{wt}(e_j) = 3$. При этом сдвиг на канонический представитель максимального веса лежит в $\widehat{L}$.

При наложении дополнительных условий на базис добавляются дополнительные максимально удалённые сдвиги. Все приведённые выше результаты тривиально обобщаются на случай аффинных подпространств.

Известно, что подпространство аффинных функций является метрически регулярным. Однако не любое линейное подпространство обладает этим свойством.

Теорема 4. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $x \in \widehat{\widehat{L}}$ тогда и только тогда, когда $\widehat{L}$ инвариантно относительно сдвига на x, т. е. $\widehat{L} = x \oplus \widehat{L}$.

Следствие 1. Пусть $L \subseteq \mathbb{F}_2^n$ — линейное подпространство, а $\widehat{L}$ — аффинное подпространство, то есть $\widehat{L} = a \oplus L_1$, где $L_1 \subseteq \mathbb{F}_2^n$ — линейное подпространство. Тогда $\widehat{\widehat{L}} = L_1$.

Используя следствие 1, можно сразу выделить класс метрически регулярных подпространств, таких, что $|L| = |\widehat{L}|$.

Интерес также вызывают метрические свойства различных кодов. Следуя определению из [3], код $\mathcal{C} \subseteq \mathbb{F}_2^n$ называется *полностью регулярным*, если весовой спектр любого его сдвига $x \oplus \mathcal{C}$ зависит только от $\mathrm{d}(x, \mathcal{C})$. Полностью регулярные коды введены в [4], там же доказано, что всякий совершенный код и всякий равномерно упакованный код являются полностью регулярными.

Теорема 5. Пусть $\mathcal{C} \subseteq \mathbb{F}_2^n$ — полностью регулярный код. Тогда $\mathcal{C}$ метрически регулярно.

Обратное, вообще говоря, неверно. Например, линейный код $\mathcal{C} = \{(000), (011)\}$ является метрически регулярным множеством с $\mathrm{d}(\mathcal{C}) = 2$, $\widehat{\mathcal{C}} = \{(101), (110)\}$, но не является полностью регулярным.

ЛИТЕРАТУРА

1. *Tokareva N. N.* Bent functions: results and applications to cryptography. Acad. Press. Elsevier, 2015. 230 p.
2. *Tokareva N. N.* Duality between bent functions and affine functions // Discr. Math. 2012. V. 312. Iss. 3. P. 666–670.
3. *Solé P.* Completely regular codes and completely transitive codes // Discr. Math. 1990. V. 81. Iss. 2. P. 193–201.
4. *Delsarte P.* An Algebraic Approach to the Association Schemes of Coding Theory. Thesis. Universite Catholique de Louvain, 1973.

УДК 519.7 DOI 10.17223/2226308X/8/5

СВОЙСТВА ГРУППЫ, ПОРОЖДЁННОЙ ГРУППАМИ СДВИГОВ ВЕКТОРНОГО ПРОСТРАНСТВА И КОЛЬЦА ВЫЧЕТОВ

Б. А. Погорелов, М. А. Пудовкина

Аддитивные группы кольца вычетов $\mathbb{Z}_{2^n}$ и векторного пространства V_n над полем GF(2), а также порождённая ими группа G_n имеют общие системы импримитивности и являются подгруппами силовской 2-подгруппы симметрической группы $S(\mathbb{Z}_{2^n})$. Данные группы возникают в криптографии при использовании в качестве способа наложения ключа относительно операций сложения из V_n и $\mathbb{Z}_{2^n}$. В работе приведено подстановочное строение подгрупп группы G_n. Показано, что подгруппами G_n являются группа нижнетреугольных $(n\times n)$-матриц над полем GF(2) и полная аффинная группа над кольцом вычетов $\mathbb{Z}_{2^n}$. Рассмотрена характеризация импримитивных подгрупп группы G_n.

Ключевые слова: *сплетение групп подстановок, импримитивная группа, силовская 2-подгруппа, аддитивная группа кольца вычетов, аддитивная группа векторного пространства, ARX-шифрсистема.*

Аддитивная группа $\mathbb{Z}_{2^n}^+$ кольца вычетов $\mathbb{Z}_{2^n}$ и аддитивная группа V_n^+ n-мерного векторного пространства V_n над полем GF(2), а также порождённая ими группа $G_n = \left\langle V_n^+, \mathbb{Z}_{2^n}^+ \right\rangle$ являются подгруппами силовской 2-подгруппы $P_n \in \mathrm{Syl}_2\left(S_{2^n}\right)$, описываемой операцией сплетения $P_n = P_2 \wr P_{n-1}$. Все эти группы имеют общие системы импримитивности $W^{(i,n)} = \left\{W_0^{(i,n)}, \ldots, W_{2^i-1}^{(i,n)}\right\}$, где

$$W_t^{(i,n)} = \left\{j \in \{0, \ldots, 2^n - 1\} : j \equiv t \,(\mathrm{mod}\ 2^i)\right\},\ i = 1, \ldots, n-1,\ t = 0, \ldots, 2^i - 1.$$

Заметим, что в криптографии группа G_n возникает в блочных шифрсистемах, использующих в качестве наложения ключа сложения в кольце вычетов и в векторном пространстве, например IDEA, ARX. В связи с наличием общих систем импримитивности у групп $\mathbb{Z}_{2^n}^+$, V_n^+ операции сложения $+$, $\oplus$ в кольце вычетов $\mathbb{Z}_{2^n}$ и в векторном пространстве V_n соответственно оказались достаточно близки.

Приведём подстановочное строение подгрупп группы G_n, из описания которого, в частности, следует известный порядок группы G_n, полученный ранее в [1].

Теорема 1. Пусть $n \geqslant 2$. Тогда:

1) если $\varphi_{n-1}^{(G_n)}$ — естественный гомоморфизм импримитивной группы G_n в группу, действующую на множестве блоков импримитивности $\{\{0, 2^{n-1}\}, \ldots, \{2^{n-1} - 1, 2^n - 1\}\}$, то $\mathrm{Im}\varphi_{n-1}^{(G_n)} \cong G_{n-1}$ и

$$\mathrm{Ker}\varphi_{n-1}^{(G_n)} = \Big\langle \Big\{ \big(r, 2^{n-1}+r\big) \cdot \big(2^{n-2}+r, 2^{n-1}+2^{n-2}+r\big) : r = 0, \ldots, 2^{n-2}-1 \Big\}, \prod_{t=0}^{2^{n-2}-1} \big(2^{n-2}+t, 2^{n-1}+2^{n-2}+t\big) \Big\rangle;$$

2) справедливы равенства $\left|\mathrm{Ker}\varphi_{n-1}^{(G_n)}\right| = 2^{2^{n-2}+1}$, $|G_n| = 2^{2^{n-1}+n-1}$.

Пусть $u_{r,n} = (r, 2^{n-1}+r) \cdot (2^{n-2}+r, 2^{n-1}+2^{n-2}+r)$ — произведение транспозиций для $r \in \big\{0, \ldots, 2^{n-2}-1\big\}$.

Опишем нормальные подгруппы группы G_n. Для $n \geqslant 2$ положим

$$R_n^{(j)} = \left\langle \prod_{t=0}^{2^{n-2-j}} u_{r+2^j t(\bmod 2^{n-2}),n} : r \in \big\{0, \ldots, 2^j-1\big\} \right\rangle, j = 0, \ldots, n-2.$$

Заметим, что

$$R_n^{(0)} = Z(G_n),\ \langle e_n \rangle < R_n^{(0)} < R_n^{(1)} < \ldots < R_n^{(n-2)} < \mathrm{Ker}\varphi_{n-1}^{(G_n)},$$
$$\left|R_n^{(j)}\right| = 2^{2^j},\ j = 0, \ldots, n-2,$$

где $Z(G_n)$ — центр группы G_n; e_n — единичный элемент группы G_n.

Утверждение 1. Пусть $n \geqslant 2$. Тогда:

1) $R_n^{(m)} \lhd G_n$ для произвольного $m \in \{0, \ldots, n-2\}$;
2) группа $R_n^{(1)}$ является единственной нормальной подгруппой группы G_n, удовлетворяющей одновременно условиям $|R_n^{(1)}| = 4$, $Z(G_n) < R_n^{(1)} < \mathrm{Ker}\varphi_{n-1}^{(G_n)}$;
3) группа $R_n^{(n-2)}$ является максимальной нормальной подгруппой группы G_n в $\mathrm{Ker}\varphi_{n-1}^{(G_n)}$.

Как следствие теоремы 1 описаны некоторые модулярные представления группы G_n над полем $\mathrm{GF}(2)$.

Доказано, что примитивная группа, подгруппой которой является G_n, совпадает с группой $S(\mathbb{Z}_{2^n})$. Поэтому представляют интерес только импримитивные группы, содержащие G_n и её подгруппы. В частности, для характеризации импримитивных подгрупп группы G_n рассмотрены полная аффинная группа $AGL_1(\mathbb{Z}_{2^n})$ над $\mathbb{Z}_{2^n}$ и группа LT_n нижнетреугольных $(n \times n)$-матриц над полем $\mathrm{GF}(2)$. Доказаны включения $LT_n < G_n$, $GL_1(\mathbb{Z}_{2^n}) < G_n$ для $n \geqslant 2$. Рассмотрено также обратное преобразование s_n над кольцом $\mathbb{Z}_{2^n}$, являющееся аналогом преобразования $x \mapsto x^{-1}$ над полем $\mathrm{GF}(2^n)$, и доказана справедливость включения $s_n \in P_n$ для $n \geqslant 2$.

ЛИТЕРАТУРА

1. *Grossman E.* Group Theoretic Remarks on Cryptographic Systems Based on Two Types of Additions. IBM Report RC-4742, Yorktown Heights, N.Y., Feb. 1974.

УДК 519.7 DOI 10.17223/2226308X/8/6

$\otimes_{\mathbf{W},\mathrm{ch}}$-МАРКОВСКИЕ ПРЕОБРАЗОВАНИЯ

Б. А. Погорелов, М. А. Пудовкина

Разностный криптоанализ итеративных алгоритмов блочного шифрования с алфавитом текстов X, как правило, проводится в рамках марковской модели. При этом фиксируется регулярная абелева группа $(X, \otimes)$ и используется тот факт, что для $\otimes$-марковских алгоритмов блочного шифрования последовательность разностей (относительно операции $\otimes$) пар промежуточных шифртекстов i-го раунда, $i = 1, 2, \ldots$, образует цепь Маркова. В работе рассматриваются $\otimes$-марковские алгоритмы блочного шифрования, у которых существует укрупнение состояний цепи Маркова до блоков разбиения $\mathbf{W}$, также являющееся цепью Маркова. Такие алгоритмы блочного шифрования, а также подстановки на X вместе с операцией $\otimes$ наложения ключа, задающие раундовую функцию алгоритма шифрования, названы $\otimes_{\mathbf{W},\mathrm{ch}}$-марковскими. Получены условия на блоки разбиения $\mathbf{W}$ и элементы матрицы разностей переходов раундовой функции, при которых алгоритм блочного шифрования является $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским. Приведены преобразования, основанные на операциях экспоненцирования и логарифмирования в кольце вычетов $\mathbb{Z}_n$ и поле $\mathrm{GF}(n+1)$, а также указаны разбиения $\mathbf{W}$, при которых данные преобразования являются $+_{\mathbf{W},\mathrm{ch}}$-марковскими относительно соответствующей операции сложения $+$ в кольце или поле.

Ключевые слова: *марковский алгоритм блочного шифрования, цепи Маркова, метод усечённых разностей, экспоненциальные преобразования.*

Пусть $(X, \otimes)$ — произвольная регулярная абелева группа на конечном множестве X с бинарной операцией $\otimes$ и единичным элементом e; α^{-1} — обратный к α элемент относительно операции $\otimes$, $\alpha \otimes \beta^{-1} = \alpha \bar{\otimes} \beta$ для любых $\alpha, \beta \in X$; $X^{\times} = X \setminus \{e\}$; $S(X)$ — симметрическая группа на X; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; $K^{(i)}$ — множество всех раундовых ключей i-го раунда, $k^{(i)} \in K^{(i)}$; $g^{(i)} : (x, k^{(i)}) \mapsto g^{(i)}(x, k^{(i)})$ и $g^{(i)}_{k^{(i)}} : \alpha \mapsto g^{(i)}(\alpha, k^{(i)})$ — раундовые функция i-го раунда, где $x \in X$, $k^{(i)} \in K^{(i)}$; $f_{\mathbf{k}_t} = g^{(1)}_{k^{(1)}} \cdot \ldots \cdot g^{(t)}_{k^{(t)}}$ для $\mathbf{k}_t = (k^{(1)}, \ldots, k^{(t)}) \in K^{(1)} \times \ldots \times K^{(t)}$;

$$p_{\theta,\varepsilon}\left(g^{(i)}\right) = \left|\left\{(\alpha, k^{(i)}) \in X \times K^{(i)} : (\theta \otimes \alpha)^{g^{(i)}_{k^{(i)}}} = \varepsilon \otimes \alpha^{g^{(i)}_{k^{(i)}}}\right\}\right| \cdot \left|K^{(i)}\right|^{-1} \cdot |X|^{-1}.$$

В [1] показано, что если $\xi^{(0)}$ — дискретная случайная величина на множестве $X^{\times}$, то в l-раундовом $\otimes$-марковском алгоритме блочного шифрования с независимыми и равномерно распределёнными раундовыми ключами раундовые разности $\xi^{(t)} = \left(\xi^{(0)} \otimes \alpha\right)^{f_{\mathbf{k}_t}} \bar{\otimes} \alpha^{f_{\mathbf{k}_t}}$, являясь случайными величинами, образуют однородную цепь Маркова.

Для $\mathbf{W}$-разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X рассмотрим последовательность таких дискретных случайных величин $\tilde{\xi}^{(0)}_{\mathbf{W}}, \ldots, \tilde{\xi}^{(l)}_{\mathbf{W}}$ на множестве $\{0, \ldots, r-1\}$, что $\tilde{\xi}^{(t)}_{\mathbf{W}} = j$ тогда и только тогда, когда $\xi^{(t)} \in W_j$, $j \in \{0, \ldots, r-1\}$, $t = 1, \ldots, l$. Для $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ и $i = 1, \ldots, l$ положим

$$p_{\theta,W_c}\left(g^{(i)}\right) = \sum_{\theta' \in W_c} p_{\theta,\theta'}\left(g^{(i)}\right), \theta \in X^{\times}.$$

Приведём условия, при которых для $\otimes$-марковского алгоритма блочного шифрования последовательность случайных величин $\tilde{\xi}^{(0)}_{\mathbf{W}}, \ldots, \tilde{\xi}^{(l)}_{\mathbf{W}}$ является цепью Маркова.

Утверждение 1. Пусть для итерационного l-раундового $\otimes$-марковского алгоритма блочного шифрования с раундовой функцией i-го раунда $g^{(i)}$ разбиение $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $r \geqslant 2$, множества X $(X^{\times})$ таково, что:

1) $\mathbf{P}\left\{\xi^{(0)} = \theta^{(0)}\right\} = \mathbf{P}\left\{\xi^{(0)} = \theta'^{(0)}\right\}$ для всех $\theta^{(0)}, \theta'^{(0)} \in W_c$, $c \in \{0, \ldots, r-1\}$;
2) для каждых $(c, j) \in \{0, \ldots, r-1\}^2$, $(\theta, i) \in W_j \times \{1, \ldots, l\}$ и некотором $a_{j,c}^{(i)}$, $0 \leqslant a_{j,c}^{(i)} \leqslant 1$, выполняется равенство $p_{\theta, W_c}\left(g^{(i)}\right) = a_{j,c}^{(i)}$.

Тогда последовательность случайных величин $\tilde{\xi}_{\mathbf{W}}^{(0)}, \ldots, \tilde{\xi}_{\mathbf{W}}^{(l)}$ над $\{0, \ldots, r-1\}$ образует цепь Маркова. Если $g^{(1)} = g^{(2)} = \ldots = g^{(l)}$, то эта цепь Маркова является однородной.

Определение 1. Назовём l-раундовый $\otimes$-марковский алгоритм блочного шифрования $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским для разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $r \geqslant 2$, если последовательность случайных величин $\tilde{\xi}_{\mathbf{W}}^{(0)}, \ldots, \tilde{\xi}_{\mathbf{W}}^{(l)}$ является цепью Маркова, т. е. раундовая функция $g^{(i)}$ удовлетворяет п. 2 утверждения 1.

Определение 2. Назовём преобразование $b \in S(X)$ $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским для разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $r \geqslant 2$, если для каждых $(c, j) \in \{0, \ldots, r-1\}^2$, $\theta \in W_j$ и некоторых $a_{j,c}$, $0 \leqslant a_{j,c} \leqslant 1$, выполняется равенство $p_{\theta, W_c}(b) = a_{j,c}$.

Отметим, что неявно допущение о $\otimes_{\mathbf{W},\mathrm{ch}}$-марковости алгоритма блочного шифрования для некоторого класса блоков разбиений $\mathbf{W}$ и наборов номеров таких блоков используется в методе усечённых разностей — в одном из наиболее распространённых обобщений разностного метода [2–6]. В этом случае неявно полагают, что для итеративных $\otimes$-марковских алгоритмов шифрования вероятность $\mathbf{P}\left\{\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)\right\}$ набора усечённых разностей $\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)$ находится как $\prod\limits_{i=0}^{l-1} p_{j^{(i)}, j^{(i+1)}}\left(g^{(i+1)}\right)$, где $A_{j^{(i)}}$ — блок некоторого разбиения множества $X^{\times}$; $p_{j^{(i)}, j^{(i+1)}}\left(g^{(i+1)}\right)$ — вероятность перехода блока $A_{j^{(i)}}$ в блок $A_{j^{(i+1)}}$ под действием раундовой функции $g^{(i+1)}$ в предположении, что раундовый ключ выбирается случайно и равновероятно из множества $K^{(i)}$, $i = 0, \ldots, l$. В ряде работ (см., например, [3, 5]) при применении метода усечённых разностей происходит проверка корректности равенства

$$\mathbf{P}\left\{\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)\right\} = \prod_{i=0}^{l-1} p_{j^{(i)}, j^{(i+1)}}\left(g^{(i+1)}\right) \tag{1}$$

посредством вычислительных экспериментов. Так, в [5] показано, что экспериментальная оценка вероятности $\mathbf{P}\left\{\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)\right\}$ может быть больше найденной по формуле (1).

В XSL-алгоритмах блочного шифрования и алгоритмах шифрования Фейстеля с XSL-функцией усложнения марковость последовательности случайных величин $W_{t_0}, \ldots, W_{t_{l-1}}$ определяется свойствами s-боксов. Поэтому в качестве примеров в данной работе приведены преобразования, основанные на операциях экспоненцирования и логарифмирования в кольце вычетов $\mathbb{Z}_n$ (с операцией сложения $+$) и поле $\mathrm{GF}(n+1)$, а также указаны разбиения $\mathbf{W}$, при которых данные преобразования являются $+_{\mathbf{W},\mathrm{ch}}$-марковскими. К этим преобразованиям относятся подстановки s-боксов алгоритма блочного шифрования SAFER [7], экспоненциальные подстановки [8] и логарифмические подстановки. Логарифмические подстановки были предложены первым автором данной работы и М. Е. Масленниковым. Они применяются в семействе функций хеширования MCSSHA, причём первая функция хеширования этого семейства MCSSHA-1

являлась кандидатом для участия в конкурсе SHA-3. Перемешивающие свойства логарифмических подстановок рассматривались, например, в [9].

Пусть $\mathbb{Z}$ — множество всех целых чисел, $\mathbb{Z}_n = \{0, \ldots, n-1\}$. Для $a \in \mathbb{Z}$ через $a_{(d)}$ обозначим такой наименьший элемент $a_{(d)} \in \{0, \ldots, d-1\}$, что $a_{(d)} \equiv a \pmod{d}$. Пусть также $n \in \mathbb{N}$, $n+1$ — простое число, θ — примитивный элемент поля Галуа $\mathrm{GF}(n+1)$ и подстановка $\mu_{\theta,\delta,c} \in S(\mathbb{Z}_n)$ задана условием

$$\mu_{\theta,\delta,c} : x \mapsto \left(\theta^{x+c} \bmod (n+1) + \delta\right)_{(n)}, \ \delta, c \in \mathbb{Z}_n.$$

Утверждение 2. Пусть $m \geqslant 1$, $n = 2^m$ и матрица $\mathbf{p}(b)$ вероятностей переходов разностей подстановки $b \in S(\mathbb{Z}_n)$ такова, что справедливо одно из условий:

1) $p_{i,j}(u) = p_{2^m-i,2^m-j}(b)$ для каждых $i, j \in \mathbb{Z}_n^\times$;
2) $p_{i,j}(b) = p_{2^m-i,j}(b)$ для каждых $i, j \in \mathbb{Z}_n^\times$.

Тогда подстановка b является $+_{\mathbf{W},\mathrm{ch}}$-марковской для разбиения $\mathbf{W} = \{W_0, W_1, \ldots, W_{2^{m-1}}\}$, где

$$W_i = \begin{cases} \{i, 2^m - i\}, & \text{если } i \in \{1, \ldots, 2^{m-1} - 1\}, \\ \{i\}, & \text{если } i \in \{0, 2^{m-1}\}. \end{cases}$$

Из утверждения 2 следует $+_{\mathbf{W},\mathrm{ch}}$-марковость подстановки $\mu_{\theta,\delta,0}$ для $\mathbf{W}$-разбиения, так как для произвольных $\varepsilon, \lambda \in \mathbb{Z}_n^\times$ справедливы равенства

$$p_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = p_{\varepsilon,2^m-\lambda}(\mu_{\theta,\delta,0}), \quad p_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = p_{2^m-\varepsilon,\lambda}(\mu_{\theta,\delta,0}).$$

Из утверждения 2 также следует $+_{\mathbf{W},\mathrm{ch}}$-марковость класса экспоненциальных подстановок $\mu'_\theta : \mathbb{Z}_{2^m} \mapsto \mathrm{GF}(2^m)$, заданных условием

$$\mu'_\theta : \alpha \mapsto \begin{cases} 0, & \text{если } \alpha = 0, \\ \theta^\alpha, & \text{если } \alpha \neq 0, \end{cases}$$

где θ — примитивный элемент поля $\mathrm{GF}(2^m)$.

ЛИТЕРАТУРА

1. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // EUROCRYPT'1991. LNCS. 1991. V. 547. P. 17–38.
2. *Knudsen L. R.* Truncated and higher order differentials // FSE'1995. LNCS. 1995. V. 1008. P. 196–211.
3. *Matsui M. and Tokita T.* Cryptanalysis of a reduced version of the block cipher E2 // FSE'1999. LNCS. 1999. V. 1636. P. 71–80.
4. *Moriai S., Sugita M., Aoki K., and Kanda M.* Security of E2 against truncated differential cryptanalysis // SAC'1999. LNCS. 2000. V. 1758. P. 106–117.
5. *Reichardt B. and Wagner D.* Markov truncated differential cryptanalysis of Skipjack // SAC'2002. LNCS. 2003. V. 2595. P. 110–128.
6. *Blondeau C.* Improbable differential from impossible differential: on the validity of the model // INDOCRYPT'2013. LNCS. 2013. V. 8250. P. 149–160.
7. *Massey J. L.* SAFER K-64: One year later // FSE'1994. LNCS. 1995. V. 1008. P. 212–232.
8. *Агиевич С. В., Афоненко А. А.* Экспоненциальные s-блоки // Материалы конф. МаБит. М.: МЦНМО, 2003. С. 127–130.
9. *Шемякина О. В.* Об оценке характеристик разбиений различных алгебраических структур // Сб. трудов конф. ИБРР-2011. СПб.: СПОИСУ, 2011. С. 137.

УДК 519.6 DOI 10.17223/2226308X/8/7

О СТЕПЕННОЙ СТРУКТУРЕ ГРАФОВ

В. М. Фомичев

Представлены свойства степенной структуры различных классов графов, описана степенная структура минимальных примитивных орграфов с числом вершин n и числом дуг $n+1$ и $n+2$. При любом $n \geqslant 5$ и при $k = 2, \ldots, n-3$ показано существование n-вершинного минимального примитивного орграфа с числом дуг $n+k$ и со степенной структурой $\{(1,1)^{n-1}, (k+1,k+1)^1\}$.

Ключевые слова: *минимальный примитивный граф, степенная структура графа.*

В [1] введено мультимножество, называемое степенной структурой графа. Укажем определяющие свойства степенной структуры графов.

1. Ориентированные графы

Для n-вершинного орграфа Γ обозначим $n_{r,s}$ число вершин с полустепенью захода r и полустепенью исхода s, где $0 \leqslant r, s, n_{r,s} \leqslant n$. Целое неотрицательное число $n_{r,s}$ называется кратностью пары (r,s) полустепеней вершин в орграфе Γ. Мультимножество всех пар (r,s) полустепеней вершин в орграфе Γ называется степенной структурой орграфа Γ, обозначается $D(\Gamma)$. Таким образом, $D(\Gamma) = \{(r,s)^{n_{r,s}}\}$, где, как правило, пары с нулевой кратностью не записаны в мультимножестве $D(\Gamma)$.

Например, степенная структура контура K длины n имеет вид $D(K) = \{(1,1)^n\}$, степенная структура полного n-вершинного орграфа Γ имеет вид $D(\Gamma) = \{(n,n)^n\}$.

Для степенной структуры n-вершинного орграфа Γ, заданной мультимножеством $D(\Gamma) = \{(r,s)^{n_{r,s}}\}$, выполнен ряд свойств.

1) Для орграфа Γ с числом вершин $n > 1$ и с числом дуг m

$$\sum_{(r,s)} n_{r,s} = n; \tag{1}$$

$$\sum_{(r,s)} (r+s) n_{r,s} = 2m. \tag{2}$$

Равенство (2) есть запись одной из первых теорем теории графов, доказанных Эйлером, в терминах степенной структуры орграфа.

2) Если орграфы Γ и Γ' изоморфны, то $D(\Gamma) = D(\Gamma')$.

3) В орграфе Γ:
   - $n_{0,0}$ есть число изолированных вершин;
   - $\sum\limits_{s} n_{0,s}$ есть число вершин с полустепенью захода 0;
   - $\sum\limits_{r} n_{r,0}$ есть число вершин с полустепенью исхода 0;
   - если орграф Γ сильносвязный, то $n_{0,s} = n_{r,0} = 0$ при любых s и r;
   - число ациклических неизолированных вершин не меньше $\sum\limits_{s>0} n_{0,s} + \sum\limits_{r>0} n_{r,0}$;
   - число циклических вершин не превышает $n - \sum\limits_{s} n_{0,s} - \sum\limits_{r} n_{r,0}$.

4) Пусть X есть n-множество, $\Gamma(g)$ — граф преобразования g множества X, тогда
   - $n_{r,s} = 0$ при любом $s \neq 1$, r любое;

— равенства (1) и (2) имеют вид

$$n_{0,1} + n_{1,1} + \ldots + n_{n,1} = n; \tag{3}$$

$$\sum_{r=0}^{n} (r+1) n_{r,1} = 2n; \tag{4}$$

— $n_{0,1}$ есть число элементов X, не имеющих прообразов относительно g;
— число ациклических вершин не меньше $n_{0,1}$;
— число циклических вершин не превышает $n - n_{0,1}$.

2. Неориентированные графы

Для n-вершинного графа Γ обозначим $q(r)$ число вершин степени r, $0 \leqslant r$, $q(r) \leqslant n$ (кратность степени r). Мультимножество допустимых натуральных чисел r назовём степенной структурой графа Γ (обозначим её $\Delta(\Gamma)$); таким образом, $\Delta(\Gamma) = \{r^{[q(r)]}\}$, при $q(r) = 0$ элемент r опускается.

Например, степенная структура цикла C длины n имеет вид $\Delta(C) = \{2^{[n]}\}$, степенная структура полного n-вершинного графа Γ имеет вид $\Delta(\Gamma) = \{n^{[n]}\}$.

Для степенной структуры n-вершинного графа Γ, заданной мультимножеством $\Delta(\Gamma) = \{r^{[q(r)]}\}$, выполнен ряд свойств.

1) Для графа Γ с числом вершин $n > 1$ и с числом рёбер m

$$q(0) + q(1) + \ldots + q(n) = n; \tag{5}$$

$$\sum_{r} r q_r = 2m. \tag{6}$$

2) Если графы Γ и Γ' изоморфны, то $\Delta(\Gamma) = \Delta(\Gamma')$.
3) $q(0)$ есть число изолированных вершин.

3. Описание степенной структуры минимальных примитивных орграфов

Примитивный орграф называется минимальным, если любая его n-вершинная часть не является примитивным графом. Обозначим $\Gamma^P_{\min}(n, m)$ множество всех минимальных примитивных n-вершинных орграфов с числом дуг $m > n$.

Теорема 1 [1]. При $n \geqslant 3$ орграф $\Gamma \in \Gamma^P_{\min}(n, n+1)$, если и только если Γ есть объединение двух простых контуров взаимно простых длин l и λ, общая часть которых есть путь длины q, где $0 \leqslant q \leqslant n-2$, $l > \lambda$, $l + \lambda - q = n + 1$; при $q = 0$ общая часть контуров есть вершина.

Следствие 1. Для $\Gamma \in \Gamma^P_{\min}(n, n+1)$, где $n \geqslant 3$, или $D(\Gamma) = \{(1,1)^{n-2}, (1,2), (2,1)\}$, или $D(\Gamma) = \{(1,1)^{n-1}, (2,2)\}$.

Теорема 2 [1]. Если $\Gamma \in \Gamma^P_{\min}(n, n+2)$, то $D(\Gamma)$ принадлежит следующим 9 классам при указанных n:

№	$n \geqslant \ldots$	$D(\Gamma)$	№	$n \geqslant \ldots$	$D(\Gamma)$
1	5	$(1,1)^{n-1}, (3,3)^1$	6	6	$(1,1)^{n-3}, (2,1)^2, (1,3)^1$
2	5	$(1,1)^{n-2}, (2,1)^1, (2,3)^1$	7	6	$(1,1)^{n-3}, (1,2)^2, (3,1)^1$
3	5	$(1,1)^{n-2}, (1,2)^1, (3,2)^1$	8	6	$(1,1)^{n-3}, (1,2)^1, (2,1)^1, (2,2)^1$
4	5	$(1,1)^{n-2}, (2,2)^2$	9	6	$(1,1)^{n-4}, (1,2)^2, (2,1)^2$
5	4	$(1,1)^{n-2}, (1,3)^1, (3,1)^1$			

Лемма 1. Пусть a, b — взаимно простые натуральные числа, тогда любое натуральное $n > ab$ представимо линейной комбинацией $n = la + \lambda b$, где $l, \lambda > 0$.

Теорема 3. Для любого $n \geqslant 5$ и $k = 2, \ldots, n-3$ имеется орграф $\Gamma \in \Gamma^P_{\min}(n, n+k)$ со степенной структурой $D(\Gamma) = \{(1,1)^{n-1}, (k+1, k+1)^1\}$.

В силу леммы любое число, не меньшее 7, представимо линейной комбинацией $2l + 3\lambda$, где $l, \lambda > 0$. Значит, при $n \geqslant 5$ и $k = 2, \ldots, n-3$ множество дуг орграфа (порядка $n + k$) можно разделить на l контуров длины 2 и λ контуров длины 3 с единственной общей вершиной, что обеспечивает примитивность и минимальность орграфа. Для данного орграфа $n + k = 2l + 3\lambda$, $n = l + 2\lambda + 1$, отсюда $k = l + \lambda - 1$. Значит, степенная структура имеет требуемый вид.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Свойства минимальных примитивных орграфов // Прикладная дискретная математика. 2015. № 2(28). С. 86–96.

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/8/8

О ЧИСЛЕ СИММЕТРИЧЕСКИХ КООРДИНАТНЫХ ФУНКЦИЙ APN-ФУНКЦИИ[1]

В. А. Виткуп

Исследуются симметрические свойства APN-функций. Доказана теорема о несуществовании перестановки на координатах, относительно которой APN-функция сохраняет свои значения. Получены верхние оценки количества симметрических булевых функций среди координатных функций APN-функции, а также количества функций, сохраняющих своё значение на циклических сдвигах координат. Получена нижняя оценка числа различных значений APN-функции. Доказаны утверждения о максимально возможном количестве одинаковых значений у APN-функции при малом числе переменных.

Ключевые слова: *векторная булева функция, APN-функция, симметрическая функция.*

Важной частью в конструкции блочных шифров являются векторные булевы функции (S-блоки), которые должны обладать определёнными криптографическими свойствами. Доказанной стойкостью к дифференциальному криптоанализу обладает класс APN-функций — почти совершенно нелинейных функций [1]. В основе данной криптоатаки лежит анализ пар открытых текстов (P, P') и соответствующих им пар шифртекстов (C, C'), между которыми существуют разности $\Delta P = P \oplus P'$ и $\Delta C = C \oplus C'$.

Функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *APN-функцией*, если для любого $a \in (\mathbb{F}_2^n)^*$ и любого $b \in \mathbb{F}_2^n$ уравнение $F(x) + F(x + a) = b$ имеет не более двух решений. В разное время [2] были получены некоторые алгебраические конструкции APN-функций: R. Gold (1968), T. Kasami (1971), H. Dobbertin (1999, 2000), T. Beth и C. Ding (1993), L. Budaghyan, C. Carlet, G. Leander (2008, 2009, 2013) [3], C. Bracken, E. Byrne, N. Markin, G. McGuire (2008, 2011). Исследованию свойств APN-функций посвящено много работ (М. М. Глухов, В. А. Зиновьев, K. Nyberg, C. Carlet, P. Charpin, H. Dobbertin, L. Budaghyan и др.). Тем не менее класс APN-функций до сих пор не описан и мало изучен, поэтому в данной области существует много интересных открытых вопросов, таких, как классификация и оценки количества функций этого класса, поиск конструкций и построение новых APN-функций, в частности взаимно однозначных. В силу сложности описания этого класса естественно рассматривать свойства его наиболее простых представителей, таких, например, как функций с низкой алгебраической степенью, симметрических функции и т. д.

Булева функция f от n переменных — *симметрическая*, если для любой перестановки $\pi \in S_n$ для любых $x_1, \ldots, x_n$ выполнено $f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$. Можно заметить, что значение симметрической булевой функции $f(x)$ зависит только от веса вектора x, следовательно, вектор значений и АНФ такой функции могут быть

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

представлены в более компактном виде, что может быть полезно при аппаратной и программной реализации шифра.

Теорема 1. Пусть F — APN-функция от n переменных. Тогда не существует перестановки $\pi \in S_n$, отличной от тождественной, такой, что $F(x) = F(\pi(x))$ для любого $x \in \mathbb{F}_2^n$.

Пусть функция F принимает t различных значений $y_1, \ldots, y_t$. Определим множество $M_i = \{x : F(x) = y_i\}$. Заметим, что если F — APN-функция от n переменных и принимает t различных значений $y_1, \ldots, y_t$, то множества M_i, $i = 1, \ldots, t$, не могут все одновременно являться слоями булева куба E^n.

Теорема 2. Пусть F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, f_i — координатные булевы функции. Тогда среди $f_1, \ldots, f_n$ не более $\sigma(n)$ симметрических, где

$$\sigma(n) = \left\lfloor n - \log_2 C_n^{\lfloor (n-1)/2 \rfloor} \right\rfloor.$$

Помимо симметрических булевых функций, интерес в криптографии представляют также функции, которые сохраняют значения на всех циклических сдвигах координат вектора x, т. е. $f(x_1, x_2, \ldots, x_n) = f(x_2, \ldots, x_n, x_1) = \ldots = f(x_n, x_1, \ldots, x_{n-1})$ для любого вектора x из $\mathbb{F}_2^n$ — так называемые *rotation symmetric Boolean functions* (RotS). Следующее утверждение даёт верхнюю оценку количества координатных RotS-функций у APN-функции.

Теорема 3. Пусть F — APN-функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, f_i — координатные булевы функции. Тогда среди $f_1, \ldots, f_n$ не более $\rho(n)$ RotS-функций, где

$$\rho(n) = \lfloor n - \log_2 n \rfloor.$$

Утверждение 1. Пусть F — APN-функция от n переменных. Тогда:
а) F принимает не менее $\mu(n)$ различных значений, где

$$\mu(n) = \frac{1 + \sqrt{2^{n+2} - 7}}{2};$$

б) мощность $|M_{\max}| \leqslant 2^n - \mu(n) + 1$, где $M_{\max}$ — максимальное по мощности множество M_i.

Верхняя оценка из утверждения 1, к сожалению, не даёт приближенного значения величины $|M_{\max}|$ для наиболее распространённых размерностей, однако следующие свойства множеств M_i дают близкие к точным (в некоторых случаях — точные) оценки для малых n.

Утверждение 2. Пусть F — APN-функция. Тогда для любого i, для любых попарно различных векторов v_r, v_j, v_l, v_s из M_i верно $v_r + v_j + v_l + v_s \neq 0$. В частности, никакое аффинное подпространство $\mathcal{L}$, $\dim(\mathcal{L}) \geqslant 2$, не может быть подмножеством M_i.

Из утверждения 2 и свойств линейных пространств следуют оценки размера множества $M_{\max}$.

Утверждение 3. Пусть F — APN-функция от n переменных, $n \leqslant 9$. Тогда мощность $|M_{\max}|$ не превышает числа $\xi(n)$, где $\xi(n)$ имеет следующие значения:

n	2	3	4	5	6	7	8	9
$\xi(n)$	3	4	6	7	9	11	14	15

На следующих функциях оценка $\xi(n)$ достигается:

$n = 2$, $F =$(0 0 0 1);

$n = 3$, $F =$(0 2 2 2 2 3 6 5);

$n = 5$, $F =$(0 0 0 1 0 2 4 8 0 3 6 12 7 16 25 23 0 7 3 22 28 19 9 0 19 8 15 28 21 9 29 2).

Для следующих функций достижима оценка $\xi(n) - 1$:

$n = 4, F =$(0 0 0 1 0 2 4 7 0 4 6 3 8 14 10 13);

$n = 6$, $F =$(0 0 0 1 0 2 4 7 0 4 6 3 8 14 10 13 0 8 16 25 5 15 17 26 32 44 54 59 45 35 63 48 0 16 26 36 34 48 60 0 45 57 49 11 7 17 31 39 43 28 14 23 12 57 45 54 38 21 5 24 9 56 46 49).

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // Eurocrypt'1993. LNCS. 1994. V. 765. P. 55–64.
2. *Туэжилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Habilitation Thesis, University of Paris, Sept. 2013.

УДК 519.7 DOI 10.17223/2226308X/8/9

О ПЕРЕСЕЧЕНИИ МНОЖЕСТВ ЗНАЧЕНИЙ ПРОИЗВОДНЫХ APN-ФУНКЦИЙ[1]

А. А. Городилова

Исследуются пересечения множеств значений производных двух APN-функций. Формулируются два вопроса: какова минимальная мощность таких пересечений и как связаны любые две APN-функции, множества значений производных которых попарно совпадают по каждому направлению. Получены частичные результаты по каждому из вопросов.

Ключевые слова: *векторная булева функция, производная по направлению, APN-функция.*

В работе рассматривается специальный класс векторных булевых функций — почти совершенные нелинейные функции (APN-функции). Векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *APN-функцией*, если для любых векторов $a, b \in \mathbb{F}_2^n$, где a — ненулевой вектор, уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более двух решений. Данные функции представляют интерес для использования в качестве узлов замены в блочных шифрах в силу их оптимальной стойкости к разностному криптоанализу. Однако класс APN-функций достаточно слабо изучен (см., например, обзор [2]), остаётся большое число открытых вопросов [3].

Настоящая работа посвящена исследованию пересечений множеств значений производных APN-функций. Производной функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ по направлению $a \in \mathbb{F}_2^n$ называется функция $D_aF(x) = F(x) \oplus F(x \oplus a)$. По определению F — APN-функция, если её производные по каждому направлению принимают в точности 2^{n-1} различных значений, т. е. $|B_a(F)| = |\{D_aF(x) : x \in \mathbb{F}_2^n\}| = 2^{n-1}$. Для автора представляется интересным найти ответы на следующие вопросы.

Открытый вопрос 1. Каково минимальное пересечение множеств значений производных двух APN-функций?

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

Открытый вопрос 2. Как связаны APN-функции F и G от n переменных, если их производные по каждому направлению имеют одинаковые множества значений соответственно, т. е. для любого $a \neq 0$ верно $B_a(F) = B_a(G)$?

Первый вопрос связан, в частности, с поиском итеративной конструкции. Из теоремы 1 [1] следует, что если взять две APN-функции F, G от n переменных и две булевы функции f, g от n переменных, для которых выполнено условие допустимости (для всех $x, y, a \in \mathbb{F}_2^n$, $a \neq 0$, хотя бы одно из равенств $D_aF(x) = D_aG(y)$ и $D_af(x) = D_ag(y)$ нарушается), то по ним можно определить APN-функцию от $n+1$ переменной. Фактически, вся сложность описанного подхода к итеративному построению APN-функций заключается в поиске исходных *допустимых* векторных функций F и G (т. е. тех, для которых существуют булевы функции f, g, такие, что для F, G, f, g выполнено условие допустимости). Получен следующий эквивалентный критерий проверки допустимости пары APN-функций F и G, который не включает в рассмотрение соответствующие булевы функци f и g.

Утверждение 1. Пара APN-функций F и G от n переменных допустима тогда и только тогда, когда для любого нечётного k, $k \geqslant 3$, не существует набора векторов x^i, y^i, a^i, $i = 1, \ldots, k$, где $a^i \neq 0$, таких, что $F(x^i) \oplus F(x^i \oplus a^i) = G(y^i) \oplus G(y^i \oplus a^i)$, $i = 1 \ldots, k$, и каждый из векторов x и y среди x^i, $x^i \oplus a^i$ и y^i, $y^i \oplus a^i$ соответственно $(i = 1, \ldots, k)$ встречается чётное число раз.

Как можно видеть из утверждения 1, необходимо отслеживать, какие пересечения имеют множества значений производных функций F и G по всем направлениям. Логично предположить, что чем меньше мощности пересечений значений производных функций F и G, тем больше вероятность, что будут выполнены условия утверждения 1.

Утверждение 2. Для любых двух APN-функций F и G от n переменных, $n \geqslant 3$, существует ненулевой вектор $a \in \mathbb{F}_2^n$, такой, что множества значений производных D_aF и D_aG пересекаются.

Далее рассмотрим отдельно случай двух квадратичных APN-функций, которые в сумме дают линейную функцию. Пусть F — квадратичная APN-функция, а L — линейная от n переменных (для любых $x, y \in \mathbb{F}_2^n$ выполнено $L(x \oplus y) = L(x) \oplus L(y)$). Тогда производные F по всем направлениям аффинны и, следовательно, множества $B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{F}_2^n\}$ являются аффинными подпространствами $\mathbb{F}_2^n$ размерности $n-1$. Далее, поскольку $B_a(F \oplus L) = B_a(F) \oplus L(a)$, то $B_a(F)$ и $B_a(F \oplus L)$ либо совпадают, либо не пересекаются. Из этого следует также, что $F \oplus L$ является APN-функцией.

Утверждение 3. Пусть F — квадратичная APN-функция, а L — произвольная линейная функция от n переменных. Пусть существуют в точности k различных ненулевых $a^i \in \mathbb{F}_2^n$, при которых $B_{a^i}(F) = B_{a^i}(F \oplus L)$. Тогда если $k > 2^{n-1}$, то пара F, $F \oplus L$ не является допустимой.

Гипотеза 1. Для любой квадратичной APN-функции F от n переменных существует линейная функция L от n переменных, такая, что пара F и $F \oplus L$ является допустимой.

Гипотеза 1 выполняется для $n = 3$; найдены также примеры, подтверждающие её при $n = 4, 5$ (эти размерности вычислительно не позволяют провести полный перебор).

Второй вопрос связан с описанием классов APN-функций, у которых множества значений производных попарно совпадают по каждому направлению. Ранее авто-

ром неверно предполагалось, что для каждой APN-функции F такой класс состоит только из функций $F(x \oplus c) \oplus d$, где c, d пробегают $\mathbb{F}_2^n$. Однако найдены примеры квадратичных функций F от 4 переменных, для которых существуют линейные функции L, прибавление которых к исходной функции F сохраняет множества значений производных по всем направлениям, но при этом $F \oplus L$ не лежит в классе $\{F(x \oplus c) \oplus d : c, d \in \mathbb{F}_2^n\}$. Например, в качестве F можно выбрать APN-функцию $F(x_1, x_2, x_3, x_4) = (x_1x_2,\ x_1x_3 \oplus x_2x_4,\ x_2x_3 \oplus x_1x_4 \oplus x_2x_4,\ x_3x_4)$, а в качестве линейной следующую: $L(x_1, x_2, x_3, x_4) = (x_1 \oplus x_2,\ x_2 \oplus x_3,\ x_2,\ x_3 \oplus x_4)$. Тогда для любого ненулевого $a \in \mathbb{F}_2^4$ верно $B_a(F) = B_a(F \oplus L)$.

ЛИТЕРАТУРА

1. *Городилова А. А.* Характеризация APN-функций через подфункции // Прикладная дискретная математика. Приложение. 2014. № 7. С. 15–16.
2. *Туэкилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
3. *Carlet C.* Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.

УДК 512.552.18 DOI 10.17223/2226308X/8/10

ИССЛЕДОВАНИЕ ГРУППЫ БИЕКТИВНЫХ ДИФФЕРЕНЦИРУЕМЫХ ПО МОДУЛЮ p^n ФУНКЦИЙ

А. С. Ивачев

Описана с точностью до изоморфизма группа биективных дифференцируемых по модулю p^n функций, предложен способ поиска сопрягающего элемента в этой группе с помощью решения системы линейных уравнений над $\mathbb{Z}_p$, а также предложен способ генерации транзитивных функций с помощью биективных дифференцируемых по модулю p^n функций путём сопряжения функции $f(x) = x + 1$ биективными функциями.

Ключевые слова: *дифференцируемая по модулю p^n функция, биективная функция, транзитивная функция, сопряжение.*

Генерация последовательностей больших периодов, состоящих из элементов конечного кольца, является важной задачей в криптографии. Для генерации последовательности может использоваться следующая рекуррентная формула:

$$x_{i+1} = f(x_i), i = 1, 2, \ldots,$$

где f — некоторая функция над кольцом $\mathbb{Z}_{p^n}$.

Возникает проблема выбора f, такой, чтобы она легко вычислялась и генерировала последовательность $x_1x_2\ldots$ максимального периода p^n.

Как вариант выбора таких f в [1] предложены и исследованы дифференцируемые по модулю p^n функции, в том числе те из них, которые являются биективными и транзитивными. В частности, построены критерии биективности и транзитивности и получена формула для вычисления обратных биективных дифференцируемых по модулю p^n функций.

В данной работе проведено более глубокое изучение биективных дифференцируемых функций, а также основных задач, в которых данные функции могут быть применимы.

Напомним основные определения и утверждения, связанные с дифференцируемыми по модулю функциями.

Определение 1. Любая функция $f : \mathbb{Z}_p \to \mathbb{Z}_p$ является дифференцируемой функцией по модулю p. Функция $f : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$ называется дифференцируемой по модулю p^n $(n > 1)$, если:

1) $f \bmod p^i$ — дифференцируемая по модулю p^i функция, $i = 1, \ldots, n-1$;
2) $f(x + ap^{n-1}) = f(x) + ap^{n-1}f'(x) \pmod{p^n}$, где f' — некоторая функция из $\mathbb{Z}_{p^n}$ в $\mathbb{Z}_{p^n}$. Функция f' называется производной функции f по модулю p^n.

Класс дифференцируемых функций обозначается D_n.

Пусть

$A_n = \{f : f \in D_n \wedge f_{n-1}(x) = 0\}$;
$B_n = \{f : f(x + ap^{n-1}) \equiv f(x) \pmod{p^n} \wedge f(x) \equiv 0 \pmod{p^{n-1}}\}$;
$C_n = \{f : f(x) = x_{n-1}p^{n-1}h'(x)$, где h' — производная некоторой функции из $D_n\}$.

Утверждение 1 [1]. Для любой функции f из D_n существует единственная тройка (f_A, f_B, f_C), где $f_A \in A_n$, $f_B \in B_n$, $f_C \in C_n$, такая, что $f(x) = f_A(x) + f_B(x) + f_C(x)$. Обратно, для каждой тройки (f_A, f_B, f_C), где $f_A \in A_n$, $f_B \in B_n$, $f_C \in C_n$, существует функция f из D_n, такая, что $f(x) = f_A(x) + f_B(x) + f_C(x)$.

Определение 2. Дифференцируемая по модулю p^n функция f называется обратимой (или биективной), если существует функция g, такая, что $g(f(x)) = x$. Функция g называется обратной для функции f.

Определение 3. Дифференцируемая по модулю p^n функция называется транзитивной, если она индуцирует одноцикловую подстановку на $\mathbb{Z}_{p^n}$.

Будем обозначать группу биективных дифференцируемых по модулю p^n функций с композицией в качестве операции как Bi_n. Пусть отображение $\pi_n : Bi_n \to Bi_{n-1}$ определяется как $\pi_n(f) = f \bmod p^{n-1}$. Очевидно, что это гомоморфизм с ядром

$$\operatorname{Ker}\pi_n = \{f : f(x) = x_0 + x_1p + \ldots + x_{n-2}p^{n-2} + f_B(x) + f'(x)x_{n-1}p^{n-1}, f_B \in B_n\}.$$

Ядро $\operatorname{Ker}\pi_n$ является группой относительно композиции функций в нем. В дальнейшем эта группа обозначается IB_n.

Пусть $\mathbb{L}_p = \langle \{f : \mathbb{Z}_p \to \mathbb{Z}_p : f(x) = ax + p, a \neq 0\}, \circ \rangle$.

Теорема 1.

$$Bi_n \simeq Bi_{n-1} \rtimes IB_n \simeq Bi_{n-1} \rtimes \bigoplus_{i=1}^{p^{n-1}} \mathbb{L}_p,$$

где при композиции функций в Bi_n компонента $\hat{f}$ из Bi_{n-1} переставляет функции f в IB_n по следующему закону:

$$\phi_{\hat{f}}(f)(x) = x_0 + x_1p + \ldots + x_{n-2}p^{n-2} + f_B(\hat{f_A}(x)) + f'(\hat{f_A}(x))x_{n-1}p^{n-1},$$

а именно: в сумме $\bigoplus_{i=1}^{p^{n-1}} \mathbb{L}_p$ слагаемое $ax + b$ с номером i ставится на место слагаемого $a^{\hat{f_A}}x + b^{\hat{f_A}}$ с номером $\hat{f_A}(i)$.

Здесь и далее если слагаемое $ax+b$ суммы $\bigoplus\limits_{i=1}^{p^{n-1}} \mathbb{L}_p$ имеет номер i и $f_A \in A_n$, то через $a^{f_A}x + b^{f_A}$ обозначается слагаемое этой суммы с номером $f_A(i)$.

Рассмотрим следующее равенство:

$$u = f^{-1} \circ v \circ f, \tag{1}$$

где $f, v, u \in Bi_n$. Оно фигурирует при рассмотрении следующих задач:

— поиск сопрягающего элемента;
— генерация транзитивных функций с помощью биективных.

Задача поиска сопрягающего элемента — это решение функционального уравнения, которое задаётся равенством (1) при известных u и v и неизвестном f. Искать сопрягающий элемент можно с помощью теоремы 1. Используя равенство

$$Bi_n \simeq Bi_{n-1} \rtimes \bigoplus_{i=1}^{p^{n-1}} \mathbb{L}_p,$$

можно проводить вычисления во второй части полупрямого произведения, если они уже проведены по первой. В $\mathbb{L}_p$ содержатся функции вида $ax+b$, $a \neq 0$. Соответственно, при решении уравнения (1) для каждого слагаемого суммы $\bigoplus\limits_{i=1}^{p^{n-1}} \mathbb{L}_p$ выполняется выражение

$$v_1 x + v_2 = (f_1^{u_A \circ f_A})^{-1}(u_1^{f_A}(f_1 x + f_2) + u_2^{f_A}) - (f_1^{u_A \circ f_A})^{-1} f_2^{u_A \circ f_A},$$

которое упрощается в систему

$$\begin{cases} v_1 f_1^{u_A \circ f_A} - u_1^{f_A} f_1 = 0, \\ v_2 f_1^{u_A \circ f_A} - u_2^{f_A} + f_2^{u_A \circ f_A} - u_1^{f_A} f_2 = 0. \end{cases}$$

Объединив эти системы для всех слагаемых, получим систему из $2p^{n-1}$ уравнений. Отметим, что она является линейной.

Получившуюся систему можно разбить на две части, одна — только из уравнений, в которых отсутствуют f_2, вторая — из уравнений, в которых f_2 присутствуют, и решать сначала первую, а затем вторую. Матрица получившейся системы представляет собой сумму перестановочных матриц, т. е. содержит большое число нулей, что может способствовать более быстрому её решению.

Другой задачей, в которой фигурируют биективные дифференцируемые по модулю p^n функции, является генерация транзитивных дифференцируемых по модулю p^n функций. Генерировать транзитивные функции с помощью равенства (1) можно, если положить v транзитивной функцией, и тогда u будет также транзитивной. Например, можно выбрать $v(x) = x + 1$, и тогда достаточно уметь генерировать биективные функции и вычислять значение обратной функции, чтобы вычислять u. Критерии биективности и формулу для вычисления обратной функции можно найти в [1]. Верна следующая

Теорема 2. Все транзитивные дифференцируемые по модулю p^n функции могут быть получены сопряжением функции $f(x) = x+1$ биективными дифференцируемыми по модулю p^n функциями.

Таким образом, пробегая по всем биективным функциям, можно предложенным способом получить все транзитивные функции.

Итак, для генерации последовательностей больших периодов биективные дифференцируемые по модулю p^n функции могут быть использованы как сопрягающие для транзитивных функций. Представляют интерес также статистические свойства таких последовательностей. Поэтому группа дифференцируемых по модулю p^n функций заслуживает внимания. Однако пока не описано представление, позволяющее эффективно вычислять данные функции, их реальное использование не практично. Поэтому в дальнейшем стоит задача поиска эффективного представления для функций из класса дифференцируемых по модулю p^n функций или из его подклассов. Предполагается, что данное представление можно получить для этих функций по модулю 2^n, используя элементарные операции, такие, как AND, XOR, RIGHT_SHIFT.

ЛИТЕРАТУРА

1. *Ивачев А. С.* Исследование класса дифференцируемых функций в кольцах классов вычетов по примарному модулю // Прикладная дискретная математика. Приложение. 2014. № 7. С. 19–22.

УДК 512.543.72 DOI 10.17223/2226308X/8/11

ОБРАЩЕНИЕ ДИФФЕРЕНЦИРУЕМЫХ ПЕРЕСТАНОВОК НАД ГРУППОЙ

А. В. Карпов

Вводится понятие дифференцируемой функции над группой с нормальным рядом, обобщающее понятие полиномиальной функции. Для абелевых, нильпотентных и разрешимых групп доказывается формула для нахождения обратной в смысле композиции перестановки к заданной дифференцируемой перестановке.

Ключевые слова: *перестановка, полином над группой, дифференцируемая функция.*

Пусть задана группа $\mathbb{G}$ с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$. Через Ψ обозначим множество функций, отображающих $\mathbb{G}$ в себя, которые действуют на факторах H_k/H_{k+1} ($k \in \{0, \ldots, n-1\}$) как эндоморфизмы.

Определение 1. Функция $f : \mathbb{G} \to \mathbb{G}$ называется *дифференцируемой* в точке $a \in \mathbb{G}$ относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$, если существует функция $\psi_{f,a} \in \Psi$, такая, что для любого члена нормального ряда H_k и любого элемента $h \in H_k$ выполняется равенство

$$f(a+h) \equiv f(a) + \psi_{f,a}(h) \pmod{H_{k+1}}.$$

Функция называется дифференцируемой, если она дифференцируема в каждой точке группы $\mathbb{G}$. Функция $\psi_{f,a}$ называется производной функции f в точке a.

В качестве примеров дифференцируемых функций можно привести следующие: полиномиальные функции над примарным кольцом вычетов $\mathbb{Z}_{p^n}$, где в качестве $\mathbb{G}$ выступает $(\mathbb{Z}_{p^n}, +)$, $H_k = p^k\mathbb{Z}_{p^n}$, $\psi_{f,a} = f'(a)$ и $\psi_{f,a}(h) = h * f'(a)$; полиномиальные вектор-функции, т. е. системы из m полиномов от m переменных с коэффициентами из $\mathbb{Z}_{p^n}$, где $\mathbb{G} = (\mathbb{Z}_{p^n}^m, +)$, $\psi_{f,a}$ совпадает с матрицей частных производных, вычисленных в точке a;

полиномы над разрешимой группой вида $u(x) = g_1 x^{\varepsilon_1} g_2 x^{\varepsilon_2} \dots g_k x^{\varepsilon_1}$ с $\psi_{u,a}(h) = h^{\sum\limits_{i=1}^{k} \varepsilon_i}$ в случае центрального ряда.

Следующая теорема обобщает критерий биективности из [1] на случай дифференцируемой функции.

Теорема 1. Пусть $u : \mathbb{G} \to \mathbb{G}$ — дифференцируемая относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \dots \trianglerighteq H_n = e$ функция. Тогда u биективна на $\mathbb{G}$, если и только если выполняются следующие два условия:

1) u биективна по модулю H_1;
2) для всех $x \in \mathbb{G}$ производная $\psi_{u,x}$ является автоморфизмом на всех факторах ряда.

Естественно называть дифференцируемую биективную функцию *дифференцируемой перестановкой*. Будем говорить, что v — *обратная* (*по модулю* H_k) к u дифференцируемая перестановка, если для всех $x \in \mathbb{G}$ выполняется

$$v(u(x)) = x \quad (v(u(x)) \equiv x \pmod{H_k}).$$

В работе решается задача нахождения обратной дифференцируемой перестановки к заданной. Нормальный ряд в группе $\mathbb{G}$ задаёт структуру, аналогичную последовательности модулей $p,\ p^2, \dots, p^n$ в случае примарного кольца, что даёт возможность применять схожие с [2] методы обращения перестановок. Основная идея заключается в сведении задачи обращения над всей группой к обращению над «маленькой» фактор-группой с последующим подъёмом решения. Это удаётся сделать, если группа $\mathbb{G}$ разрешима и известно промежуточное решение по модулю некоторой подгруппы из нормального ряда.

Теорема 2. Пусть u — перестановка элементов разрешимой группы $\mathbb{G}$, дифференцируемая относительно нормального ряда $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \dots \trianglerighteq H_n = e$, v_k — обратная перестановка к u по модулю H_k. Тогда обратной к u по модулю H_{k+1} является перестановка

$$v_{k+1}(x) = v_k(x) - \psi^{-1}_{u,v_k(x)}(-x + u(v_k(x))),$$

где $\psi^{-1}_{u,v_k(x)}$ — обратный к $\psi_{u,v_k(x)}$ автоморфизм в $\mathrm{Aut}(H_k/H_{k+1})$. Если дополнительно $\psi_{u,v_k(x)}$ и $\psi_{v_k,x}$ — взаимно обратные автоморфизмы фактора H_k/H_{k+1}, то

$$v_{k+1}(x) = v_k(x) - v_k(u(v_k(x))) + v_k(x).$$

Возможно также обращение дифференцируемой перестановки, если известно обращение другой дифференцируемой перестановки, отличающейся от заданной на определённую добавку.

Теорема 3. Пусть u и v — взаимно обратные по модулю H_k дифференцируемые перестановки и для всех $x \in \mathbb{G}$ дифференцируемая функция u_0 удовлетворяет следующим условиям:

1) $u_0(x) \in H_{k-1}$;
2) $\psi_{u_0,x} : H_{k-1} \to H_k$.

Тогда обратной к $u^*(x) = u(x) + u_0(x)$ по модулю H_k является перестановка $v^*(x) = v(x) - \psi_{v,x}(u_0(v(x)))$.

В качестве примера рассмотрим $\mathbb{G} = T_3(\mathbb{Z}_7)$ с разрешимым рядом $\mathbb{G} = T_3(\mathbb{Z}_7) \trianglerighteq \trianglerighteq UT_3(\mathbb{Z}_7) \trianglerighteq UT_3^2(\mathbb{Z}_7) \trianglerighteq UT_3^3(\mathbb{Z}_7) = e$, где $UT_3^i(\mathbb{Z}_7)$ — подгруппа, состоящая из унитреугольных матриц с $(i-1)$ нулевыми диагоналями над главной.

Введём функцию $u(x) = \begin{pmatrix} 2 & 4 & 3 \\ 0 & 3 & 5 \\ 0 & 0 & 6 \end{pmatrix} x \begin{pmatrix} 1 & 2 & 5 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} x^{-1} \begin{pmatrix} 1 & 6 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x$. Сначала обратим $u(x)$ в первом факторе $T_3(\mathbb{Z}_7)/UT_4(\mathbb{Z}_7) \simeq \mathbb{Z}_7^* \otimes \mathbb{Z}_7^* \otimes \mathbb{Z}_7^*$:

$$v_1(x) = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 6 \end{pmatrix} x,\ v_1\left(u\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & \mathbf{0} & \mathbf{4} \\ 0 & 2 & \mathbf{6} \\ 0 & 0 & 4 \end{pmatrix} \equiv \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix} (\bmod\ UT_3(\mathbb{Z}_7)).$$

Так как производная $\psi_{u,x}$ — тождественный автоморфизм, по теореме 2 получаем

$$v_2(x) = v_1(x)(x^{-1}u(v_1(x)))^{-1},\quad v_3 = v_2(x)(x^{-1}u(v_2(x)))^{-1},$$

$$v_2\left(u\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & \mathbf{6} \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix} \equiv \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix} (\bmod\ UT_3^2(\mathbb{Z}_7)),$$

$$v_3\left(u\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}.$$

Умножим справа $u(x)$ на добавку $u_0(x)$, удовлетворяющую условиям 1 и 2 теоремы 3:

$$u_0(x) = x^{-1}\begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} x,\quad u^*(x) = u(x)u_0(x).$$

Построенная ранее $v_3(x)$ не обращает $u^*(x)$:

$$v_3\left(u^*\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & \mathbf{5} \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}.$$

Построим обратную к $u^*(x)$ функцию:

$$v^*(x) = v_3(x)(\psi_{v_3,x}(u_0(v_3(x))))^{-1} = v_3(x)(u_0(v_3(x)))^{-1},$$

$$v^*\left(u^*\left(\begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}\right)\right) = \begin{pmatrix} 3 & 6 & 2 \\ 0 & 2 & 5 \\ 0 & 0 & 4 \end{pmatrix}.$$

Таким образом, задача обращения дифференцируемой перестановки над разрешимой группой сводится к обращению над фактор-группой с последующим подъёмом решения. Если известна обратная перестановка по модулю H_k, то можно строить другие пары взаимно обратных перестановок по модулю H_k, используя теорему 3.

ЛИТЕРАТУРА

1. *Anashin V. S.* Noncommutative algebraic dynamics: ergodic theory for profinite groups // Proc. Steklov Institute of Math. 2009. V. 265. P. 30–58.
2. *Карпов А. В.* Перестановочные многочлены над примарными кольцами // Прикладная дискретная математика. 2013. № 4(22). С. 16–21.

УДК 519.7 DOI 10.17223/2226308X/8/12

О СВЯЗНОСТИ ГРАФА МИНИМАЛЬНЫХ РАССТОЯНИЙ МНОЖЕСТВА БЕНТ-ФУНКЦИЙ[1]

Н. А. Коломеец

Рассматривается связность графа GB_{2k} минимальных расстояний множества бент-функций. Вершинами данного графа являются все бент-функции от $2k$ переменных, две вершины-функции соединены ребром, если они находятся на расстоянии 2^k друг от друга. Доказано, что подграф GB_{2k}, порождённый множеством бент-функций, аффинно эквивалентных бент-функциям из класса Мэйорана — МакФарланда, является связным. Доказана связность графов GB_2, GB_4 и GB_6.

Ключевые слова: *булевы функции, бент-функции, минимальное расстояние.*

Отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой функцией* от n переменных. *Аффинной* булевой функцией называется функция вида $\langle a, x\rangle \oplus c$, где $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$ и $\langle a, x\rangle = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$. *Расстоянием Хэмминга* $\mathrm{dist}(f, g)$ между двумя булевыми функциями f и g от n переменных называется количество $x \in \mathbb{F}_2^n$, таких, что $f(x) \neq g(x)$. *Бент-функцией* называется булева функция от чётного числа переменных, находящаяся на максимально возможном расстоянии от множества всех аффинных функций. Обозначим через $\mathcal{B}_{2k}$ множество всех бент-функций от $2k$ переменных. Бент-функции предложены О. Ротхаусом [1]. Они имеют большое число приложений в алгебре, комбинаторике, теории кодирования, криптографии [2].

Граф $GB_{2k} = (V, E)$ называется *графом минимальных расстояний множества бент-функций*, если $V = \mathcal{B}_{2k}$ и $(f, g) \in E$ тогда и только тогда, когда $\mathrm{dist}(f, g) = 2^k$. Заметим, что 2^k является минимально возможным расстоянием между двумя бент-функциями от $2k$ переменных.

Напомним, что функции следующего вида являются бент-функциями и образуют класс Мэйорана — МакФарланда M_{2k} [3]:

$$f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y),$$

где $x, y \in \mathbb{F}_2^k$; π — подстановка на множестве $\mathbb{F}_2^k$; φ — произвольная булева функция от k переменных.

Пусть множество $\widetilde{M}_{2k}$ содержит все функции вида $f(Ax \oplus b)$, где $f \in M_{2k}$; A — обратимая двоичная матрица размера $2k \times 2k$ и $b \in \mathbb{F}_2^{2k}$. Другими словами, любая функция из $\widetilde{M}_{2k}$ является бент-функцией, *аффинно эквивалентной* некоторой бент-функции из класса Мэйорана — МакФарланда. Заметим, что $f \oplus \ell$ лежит в $\widetilde{M}_{2k}$ для любой $f \in \widetilde{M}_{2k}$ и любой аффинной функции ℓ от $2k$ переменных.

Обозначим через GM_{2k} подграф графа GB_{2k}, порождённый множеством вершин $\widetilde{M}_{2k}$. Известно [4], что максимальная степень вершины в графах GB_{2k} и GM_{2k} равна $2^k(2^1 + 1)(2^2 + 1)\ldots(2^k + 1)$, причём любая вершина максимальной степени является квадратичной бент-функцией.

В данной работе рассматривается связность графов GB_{2k} и GM_{2k}.

Утверждение 1. Степень любой вершины графа GM_{2k} не меньше, чем $2^{2k+1} - 2^k$.

Теорема 1. Граф GM_{2k} является связным для любого $k \geqslant 1$.

Следствие 1. Граф GM_{2k} является рёберно 3-связным.

[1]Работа поддержана грантом РФФИ, проект № 15–31–20635.

Следствие 2. Графы GB_2, GB_4 и GB_6 являются связными.

Отметим, что в общем случае граф GB_{2k} не является связным, поскольку он может содержать изолированные вершины. В частности, это справедливо при $2k \geqslant 14$.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N. N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
3. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.
4. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. 2014. №3. С. 28–39.

УДК 519.7 DOI 10.17223/2226308X/8/13

О САМОДУАЛЬНЫХ БУЛЕВЫХ БЕНТ-ФУНКЦИЯХ[1]

А. В. Куценко

Получен критерий самодуальности (анти-самодуальности) булевой бент-функции, а именно доказано, что булева бент-функция f от чётного числа переменных является самодуальной (анти-самодуальной) тогда и только тогда, когда при каждом фиксированном $y \in \mathbb{F}_2^n$ для булевой функции $F_y(x) = f(x) \oplus f(y) \oplus x \cdot y$ справедливо $\mathrm{wt}(F_y) = 2^{n-1} - 2^{n/2-1}$ (соответственно $\mathrm{wt}(F_y) = 2^{n-1} + 2^{n/2-1}$).

Ключевые слова: *булева функция, бент-функция, самодуальная бент-функция.*

Булевой функцией f называется любое отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Скалярным произведением* $x \cdot y$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ называется $x \cdot y = \bigoplus\limits_{i=1}^{n} x_i y_i$. *Преобразованием Уолша – Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x \cdot y}$. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$. Булева функция $\tilde{f}$ называется *дуальной* к бент-функции f, если $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ для каждого $x \in \mathbb{F}_2^n$. Бент-функция f называется *самодуальной (анти-самодуальной)*, если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). *Носителем* булевой функции f от n переменных называется множество $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. *Весом* вектора $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ называется число $\mathrm{wt}(x) = \sum\limits_{i=1}^{n} x_i$. *Весом Хэмминга* булевой функции f называется вес её вектора значений $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. Сложной задачей является полная характеризация и описание класса самодуальных бент-функций. Этому вопросу посвящены несколько работ за рубежом (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou и др.). В частности, в работе [1] перечислены все самодуальные бент-функции от 2, 4 и 6 переменных и все квадратичные самодуальные бент-функции от 8 переменных; в [2] приведена классификация всех квадратичных самодуальных бент-функций.

[1]Исследование выполнено при финансовой поддержке РФФИ (проект №15-31-20635).

Теорема 1. Булева бент-функция f от чётного числа переменных n является самодуальной (анти-самодуальной) тогда и только тогда, когда при каждом фиксированном $y \in \mathbb{F}_2^n$ для булевой функции $F_y(x) = f(x) \oplus f(y) \oplus x \cdot y$ справедливо $\mathrm{wt}(F_y) = 2^{n-1} - 2^{n/2-1}$ (соответственно $2^{n-1} + 2^{n/2-1}$).

ЛИТЕРАТУРА

1. *Carlet C., Danielson L. E., Parker M. G., Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
2. *Hou X.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. Iss. 2. P. 183–198.

УДК 519.7 DOI 10.17223/2226308X/8/14

ОБ ОБРАТИМОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ

И. А. Панкратова

Рассматривается класс $\mathcal{F}_{n,m,k}$ обратимых векторных булевых функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$, координатные функции которых существенно зависят от заданного числа k переменных. Доказано: 1) таких функций не существует при любом $n = m$ и $k = 2$; 2) функции класса $\mathcal{F}_{n,n,n-1}$ могут (не могут) быть построены из аффинных координатных функций при чётном (нечётном) n; 3) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то и $\mathcal{F}_{n+1,m+1,k} \neq \varnothing$.

Ключевые слова: *векторная булева функция, обратимые функции.*

Задача построения обратимых векторных булевых функций возникает при создании многих криптосистем; в частности, такие функции используются в многораундовых симметричных блочных шифрах класса SIBCipher [1]. Для того чтобы значения функции можно было эффективно вычислять, часто вводится ограничение на количество существенных переменных у каждой координатной функции векторной функции.

Для $n, m, k \in \mathbb{Z}$ обозначим через $\mathcal{F}_{n,m,k}$ класс функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, где $F = (f_1 \dots f_m)$, таких, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, m$, существенно зависят ровно от k переменных и функция F — инъекция (т. е. обратима).

В случае $n = m$ (практически важном для построения многораундовых шифров) будем обозначать $\mathcal{F}_{n,k} = \mathcal{F}_{n,n,k}$.

Непосредственно проверяются следующие свойства:

1) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $m \geqslant n$;
2) если $F \in \mathcal{F}_{n,k}$, то F есть подстановка на $\mathbb{F}_2^n$ и все её координатные функции уравновешены;
3) если $F = (f_1 \dots f_m) \in \mathcal{F}_{n,m,k}$, то и $F' = (f_1 \dots \bar{f}_i \dots f_m) \in \mathcal{F}_{n,m,k}$, $i \in \{1, \dots, m\}$;
4) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $\mathcal{F}_{n,t,k} \neq \varnothing$ для любого $t > m$;
5) если $\mathcal{F}_{k,k} \neq \varnothing$, то $\mathcal{F}_{ks,k} \neq \varnothing$ для любого $s > 1$.

Последнее свойство используется при построении шифров SIBCiphers семейства Люцифер [1]: ks переменных разбиваются на блоки по k переменных в каждом и «большая» раундовая функция набирается из s «маленьких» функций — подстановок на $\mathbb{F}_2^k$.

Пример 1. Функция $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ с вектором значений (0 6 7 2 4 3 1 5) принадлежит множеству $\mathcal{F}_{3,3}$; её координатные функции $f_1 = x_1 \oplus x_2 \oplus x_3$, $f_2 = x_1x_2 \oplus \oplus x_2x_3 \oplus x_2 \oplus x_3$, $f_3 = x_1x_3 \oplus x_2x_3 \oplus x_2$.

Утверждение 1. $\mathcal{F}_{n,2} = \varnothing$ для любого $n \geqslant 2$.

Доказательство. Предположим, $F \in \mathcal{F}_{n,2}$. Тогда по свойству 2 все её координатные функции уравновешены, т. е. имеют вид $x_i \oplus x_j \oplus c$ для некоторых $1 \leqslant i < j \leqslant n$, $c \in \mathbb{F}_2$. Но в этом случае $F(x) = F(\bar{x})$ для любого $x \in \mathbb{F}_2^n$, что невозможно для инъективной функции. ■

Заметим, что при $m > n$ уравновешенность координатных функций уже не обязательна и класс $\mathcal{F}_{n,m,2}$ может быть не пуст.

Пример 2. Функция $F : \mathbb{F}_2^2 \to \mathbb{F}_2^3$ с вектором значений (0 5 4 2) принадлежит классу $\mathcal{F}_{2,3,2}$; её координатные функции $f_1 = x_1 \oplus x_2$, $f_2 = x_1 x_2$, $f_3 = x_1 x_2 \oplus x_2$.

Утверждение 2.

1) Если n чётное, то некоторая $F \in \mathcal{F}_{n,n-1}$ может быть построена из аффинных координатных функций.
2) Если n нечётное, то никакая $F \in \mathcal{F}_{n,n-1}$ не может быть построена из аффинных координатных функций.

Доказательство. Пусть $F(x_1, \ldots, x_n) = (f_1 \ldots f_n)$, $f_i = \bigoplus\limits_{j \neq i} x_j \oplus c_i$, $c_i \in \mathbb{F}_2$, $i = 1, \ldots, n$; $a = (a_1 \ldots a_n) \in \mathbb{F}_2^n$ — произвольное значение. Ввиду свойства 3 без ограничения общности можно полагать, что все c_i равны нулю. Составим уравнение $F(x) = a$, или в матричном виде $Ax = a$, где x и a — вектор-столбцы, A — $(n \times n)$-матрица:

$$A = \begin{pmatrix} 0 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & 1 & \ldots & 1 & 1 \\ 1 & 1 & 0 & \ldots & 1 & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & 1 & \ldots & 0 & 1 \\ 1 & 1 & 1 & \ldots & 1 & 0 \end{pmatrix}.$$

Легко убедиться, что $\det A = (n-1) \bmod 2$ над полем $\mathbb{F}_2$, поэтому уравнение $F(x) = a$ имеет решения для всех a (что равносильно условию $F \in \mathcal{F}_{n,n-1}$), если и только если n чётно.

Для завершения доказательства п. 2 утверждения осталось заметить, что перестановка координатных функций не влияет на принадлежность функции F классу $\mathcal{F}_{n,n-1}$; других способов выбора n различных аффинных функций, существенно зависящих от $(n-1)$ переменных каждая и от всех n переменных в совокупности (что, очевидно, необходимо для принадлежности функции F классу $\mathcal{F}_{n,n-1}$), нет. ■

Следствие 1. $\mathcal{F}_{n,n-1} \neq \varnothing$ для любого чётного n.

Утверждение 3. Если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $\mathcal{F}_{n+1,m+1,k} \neq \varnothing$.

Доказательство. Пусть $F(x_1, \ldots, x_n) = (f_1 \ldots f_m) \in \mathcal{F}_{n,m,k}$. Построим функцию $G : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{m+1}$ так: $G(x_1, \ldots, x_n, x_{n+1}) = (f_1 \ldots f_m\, g)$, где $g(x_1, \ldots, x_n, x_{n+1}) = x_{n+1} \oplus$ $\oplus\, h(x_1, \ldots, x_n)$, h — любая функция, существенно зависящая от $(k-1)$ переменных. Тогда $G(a_1, \ldots, a_n, 0) \neq G(a_1, \ldots, a_n, 1)$ для любого $a_1 \ldots a_n \in \mathbb{F}_2^n$ ввиду линейности функции g по переменной x_{n+1}; $G(a_1, \ldots, a_n, c) \neq G(b_1, \ldots, b_n, c)$ для любых $a_1 \ldots a_n \neq$ $\neq b_1 \ldots b_n$, $c \in \mathbb{F}_2$ ввиду обратимости функции F. ■

Из утверждения 3, свойства 4 и примеров 1 и 2 следует, что $\mathcal{F}_{n,m,3} \neq \varnothing$ для всех $m \geqslant n \geqslant 3$ и $\mathcal{F}_{n,m,2} \neq \varnothing$ для всех $m > n \geqslant 2$.

ЛИТЕРАТУРА

1. *Агибалов Г. П.* SIBCiphers — симметричные итеративные блочные шифры из булевых функций с ключевыми аргументами // Прикладная дискретная математика. Приложение. 2014. № 7. С. 43–48.

УДК 519.7 DOI 10.17223/2226308X/8/15

ОБ АЛГЕБРАИЧЕСКОЙ ИММУННОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ[1]

Д. П. Покрасенко

Исследуется компонентная алгебраическая иммунность векторных булевых функций. Доказана теорема о соответствии между максимальной компонентной алгебраической иммунностью и сбалансированностью функции. Получена связь между максимальной компонентной алгебраической иммунностью и матрицами специального вида. При малом числе переменных построены функции, имеющие максимальную компонентную алгебраическую иммунность.

Ключевые слова: *векторная булева функция, компонентная алгебраическая иммунность.*

В 2003 г. N. Courtois и W. Meier предложили алгебраический метод криптоанализа шифров [1]. В случае поточных шифров этот метод использует следующие слабости фильтрующей функции: наличие у неё аннигиляторов низкой степени и множителей, уменьшающих степень функции. В настоящее время данный вид криптоанализа является одним из наиболее перспективных и развивающихся; соответственно возникает вопрос о поиске функций, способных ему противостоять.

В 2004 г. W. Meier, E. Pasalic и C. Carlet в работе [2] ввели понятие алгебраической иммунности для булевых функций. *Алгебраической иммунностью* $\mathrm{AI}(f)$ булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется такое минимальное число d, что существует булева функций g степени d, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)g = 0$. Для любой булевой функции выполняется $\mathrm{AI}(f) \leqslant \lceil n/2 \rceil$ и существуют функции, имеющие $\mathrm{AI}(f) = \lceil n/2 \rceil$. Высокая алгебраическая иммунность позволяет противостоять алгебраическим атакам.

Понятие алгебраической иммунности различными способами было обобщено на векторный случай. Так, в работе [3] F. Armknecht и M. Krause, а также G. Ars и J.-C. Faugère в [4] рассмотрели алгебраическую иммунность S-блоков и ввели понятия базовой $\mathrm{AI}(F)$ и графической $\mathrm{AI}_{\mathrm{gr}}(F)$ алгебраической иммунности векторных булевых функций. При этом базовая алгебраическая иммунность больше 1 только при малых значениях m, поэтому данный параметр анализируется у S-блоков, которые используются в поточных шифрах. Графическая алгебраическая иммунность используется для изучения сопротивляемости алгебраическим атакам блочных шифров.

Следующее обобщение является одним из наиболее естественных с криптографической точки зрения. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ называется минимальная алгебраическая иммунность компонентных функций $b \cdot F$ ($b \in \mathbb{F}_2^m, b \neq 0$), т. е. $\mathrm{AI}_{\mathrm{comp}}(F) = \min\{\mathrm{AI}(b \cdot F) : b \in \mathbb{F}_2^m, b \neq 0\}$, где $b \cdot F = b_1 f_1 \oplus \ldots \oplus b_m f_m$. Данное определение является наиболее универсальным, наличие высокой компонентной алгебраической иммунности S-блоков

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

способствует противостоянию алгебраическому криптоанализу поточных и блочных шифров.

В [5] получена оценка $\mathrm{AI}_{\mathrm{comp}} \leqslant \min\{\lceil n/2 \rceil, d^o_{\min} F\}$, где $d^o_{\min} F$ — минимальная степень компонентных функций $b \cdot F$. При этом остаётся не изученным вопрос о существовании функций, имеющих $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$.

В работе получены следующие результаты.

Теорема 1. Для любого нечётного n векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, имеющая $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$, является сбалансированной. В случае $n = m$ функция F взаимно однозначна.

Занумеруем через $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ мономы от n переменных, где a_i соответствует появлению в мономе переменной x_i, а $a = (0, \ldots, 0)$ соответствует 1. Например, вектор $a = (1, 0, 1, 0, \ldots, 0)$ соответствует моному $x_1 x_3$. Для каждой векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ введём две матрицы M_F, M'_F, элементами которых являются булевы функции от n переменных. Построим эти матрицы следующим способом: в матрице M_F j-му столбцу соответствует умножение компонентной функции $b \cdot F$, $b \neq 0$, на мономы степени меньше $\lceil n/2 \rceil$. Нумерация столбцов идёт по вектору $b \in \mathbb{F}_2^m$, $b \neq 0$. Соответственно число столбцов $2^m - 1$. Строки занумерованы с помощью вектора $a = (a_1, \ldots, a_n)$. Матрица M'_F строится аналогично, только вместо $b \cdot F$ подставляется $b \cdot F \oplus 1$:

$$M_F = \begin{pmatrix} f_1 & f_2 & \ldots & f_1 \oplus f_2 \oplus \ldots \oplus f_m \\ f_1 x_1 & f_2 x_1 & \ldots & (f_1 \oplus f_2 \oplus \ldots \oplus f_m) x_1 \\ \ldots & \ldots & \ldots & \ldots \\ f_1 x_1 x_2 & \ldots & \ldots & (f_1 \oplus f_2 \oplus \ldots \oplus f_m) x_1 x_2 \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix},$$

$$M'_F = \begin{pmatrix} f_1 \oplus 1 & f_2 \oplus 1 & \ldots & f_1 \oplus \ldots \oplus f_m \oplus 1 \\ (f_1 \oplus 1) x_1 & (f_2 \oplus 1) x_1 & \ldots & (f_1 \oplus \ldots \oplus f_m \oplus 1) x_1 \\ \ldots & \ldots & \ldots & \ldots \\ (f_1 \oplus 1) x_1 x_2 & \ldots & \ldots & (f_1 \oplus \ldots \oplus f_m \oplus 1) x_1 x_2 \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

Функции $f_1, \ldots, f_n$ являются *линейно независимыми*, если выражение $a_1 f_1 \oplus a_2 f_2 \oplus \oplus \ldots \oplus a_n f_n$, где $a_1, a_2, \ldots, a_n \in \mathbb{F}_2$, тождественно равно нулю только при условии $a_1 = a_2 = \ldots = a_n = 0$.

Теорема 2. Векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ имеет максимальную компонентную алгебраическую иммунность $\mathrm{AI}_{\mathrm{comp}}(F) = \lceil n/2 \rceil$ тогда и только тогда, когда в матрицах M_F и M'_F элементы любого столбца образуют линейно независимое множество.

Для малого числа переменных найдены векторные булевы функции, которые имеют $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$, подсчитано число таких функций. В таблице приведено количество векторных булевых функций с максимальной компонентной алгебраической иммунностью, общее количество векторных булевых функций, действующих из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$, и доля функций с $\mathrm{AI}_{\mathrm{comp}} = \lceil n/2 \rceil$ от общего числа векторных булевых функций.

(n,m)	Функции с $\mathrm{AI}_{\mathrm{comp}}(F)=\lceil n/2\rceil$	Все функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$	Доля функций
(2,2)	168	256	0,65625
(3,2)	1344	65536	0,02051
(3,3)	10752	16777216	0,00064
(4,2)	$\approx 10^8$	4294967296	$\approx 0{,}02$

ЛИТЕРАТУРА

1. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt'2003. LNCS. 2003. V. 2656. P. 345–359.
2. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt'2004. LNCS. 2004. V. 3027. P. 474–491.
3. *Armknecht F. and Krause M.* Constructing single- and multi-output Boolean functions with maximal immunity // ICALP'2006. LNCS. 2006. V. 4052. P. 180–191.
4. *Ars G. and Faugère J.-C.* Algebraic immunities of functions over finite fields // Proc. Conf. BFCA. 2005. P. 21–38.
5. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Amsterdam: IOS Press, 2009. P. 104–116.

УДК 519.7 DOI 10.17223/2226308X/8/16

СВОЙСТВА p-ИЧНЫХ БЕНТ-ФУНКЦИЙ, НАХОДЯЩИХСЯ НА МИНИМАЛЬНОМ РАССТОЯНИИ ДРУГ ОТ ДРУГА[1]

В. Н. Потапов

Доказано, что минимальное расстояние Хэмминга между двумя p-ичными бент-функциями от $2n$ переменных равно p^n в случае, когда число p простое. Число p-ичных бент-функций на минимальном расстоянии от квадратичной бент-функции равно $p^n(p^{n-1}+1)\cdots(p+1)(p-1)$ при $p>2$.

Ключевые слова: *бент-функция, расстояние Хэмминга, квадратичная форма.*

Введение

Рассмотрим конечную абелеву группу G и векторное пространство $V(G)$, состоящее из функций $f: G \to \mathbb{C}$, со скалярным произведением

$$(f,g)=\sum_{x\in G} f(x)\overline{g(x)}.$$

Характерами называются гомоморфизмы группы G в мультипликативную группу поля $\mathbb{C}$, т. е. такие $\phi \in V(G)$, что $\phi(x+y)=\phi(x)\phi(y)$, для любых $x,y\in G$. Характеры абелевой группы G образуют ортогональный базис в $V(G)$. Если $G=\mathbb{Z}_q^n$, то для любого $z\in\mathbb{Z}_q^n$ характер группы G определяется равенством $\phi_z(x)=\xi^{\langle x,z\rangle}$, где $\xi=e^{2\pi i/q}$ и $\langle x,y\rangle = x_1y_1+\ldots+x_ny_n \bmod q$. Характерами прямой суммы двух групп являются всевозможные попарные произведения характеров первой и второй группы. Поскольку любая конечная абелева группа представляется в виде прямой суммы циклических групп, характеры произвольной конечной абелевой группы являются произведениями функций определённого выше вида.

Преобразованием Фурье функции из $V(G)$ называется вектор коэффициентов в разложении по базису характеров. Нам будет удобнее определить преобразование Фурье

[1]Работа поддержана грантом РФФИ № 13-01-00463.

изометричным образом: $\widehat{f}(z) = (f, \phi_z)/|G|^{1/2}$. Тогда равенство Парсеваля принимает вид $\|f\| = \|\widehat{f}\|$ и справедлива формула обращения $\widehat{(\widehat{f}(x))} = f(-x)$. *Носителем* функции называется множество аргументов, на которых функция принимает ненулевые значения $\mathrm{supp}(f) = \{x \in G : f(x) \neq 0\}$. Доказательство следующего утверждения имеется, например, в [1].

Утверждение 1 (принцип неопределённости). Пусть G — конечная абелева группа, тогда

$$|\mathrm{supp}(f)||\mathrm{supp}(\widehat{f})| \geqslant |G|. \tag{1}$$

Причём равенство в формуле (1) достигается только для характеристических функций подгрупп с точностью до естественных преобразований, сохраняющих мощности носителей функции и её фурье-образа.

Если p — простое число, то группу $\mathbb{Z}_p^n$ можно рассматривать как n-мерное векторное пространство над полем $\mathrm{GF}(p)$.

Следствие 1. Пусть $G = \mathbb{Z}_p^n$ и p — простое число. Равенство в формуле (1) достигается, если и только если $f = c\phi_z\chi^\Gamma$, где $z \in G$; $c \in \mathbb{C}$ — константа и χ^Γ — характеристическая функция аффинного подпространства Γ в G.

Известно (см., например, [2, с. 33, лемма 1.1.26]) следующее равенство.

Утверждение 2 (тождество Саркара). Пусть p — простое число и Γ — линейное подпространство в $\mathbb{Z}_p^n$. Тогда

$$\sum_{y\in\Gamma} \widehat{f}(y) = p^{\dim\Gamma - n/2} \sum_{x\in\Gamma^\perp} f(x).$$

Определим *свёртку* двух функций $f, g \in V(G)$ равенством $f*g(z) = \sum\limits_{x\in G} f(x)g(z-x)$. Из определения свёртки нетрудно получить известное равенство

$$\widehat{f * g} = |G|^{1/2}\widehat{f}\cdot\widehat{g}. \tag{2}$$

1. Бент-функции

Для функций $g : \mathbb{Z}_q^n \to \mathbb{Z}_q$ определим *преобразование Уолша — Адамара* следующим образом: $W_g(z) = \widehat{\xi^g}(z)$. Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ называется *бент-функцией* (q-ичной), если $|W_f(y)| = 1$ для любых $y \in Z_q^n$, или (что то же самое) $\widehat{\xi^f}\cdot\overline{\widehat{\xi^f}} = I$, I — функция, всюду равная 1 [3 – 5]. Из (2) следует, что определение бент-функции эквивалентно равенству $\xi^f * \overline{\xi^f} = |G|\chi^{\{0\}}$. Отсюда непосредственно вытекает, что матрица $A = (a_{z,y})$, где $a_{z,y} = \xi^{f(z+y)}$, является обобщённой матрицей Адамара, как и матрица $H = (h_{z,y})$, где $h_{z,y} = \xi^{\langle z,y\rangle}$. Нетрудно видеть, что невырожденные аффинные преобразования аргументов бент-функции и прибавление аффинной функции не выводят из класса бент-функций.

Бент-функция b называется *регулярной*, если найдётся функция $b' : \mathbb{Z}_q^n \to \mathbb{Z}_q$, удовлетворяющая равенству $\xi^{b'} = \widehat{\xi^b}$. Из формулы обращения следует, что b' также является бент-функцией. Известно следующее

Утверждение 3.

1) $\sum\limits_{j=0}^{q-1} \xi^{kj} = 0$ при $k \neq 0 \pmod q$;

2) если q — простое, то ξ не является корнем многочлена степени меньше $q-1$;
3) если q — степень простого числа, то алгебраическая система, полученная присоединением элемента ξ к полю рациональных чисел, является полем.

Из свойства 3 непосредственно получаем

Следствие 2. Если q — степень простого числа и n чётно, то все бент-функции регулярны.

Для доказательства следствия нужно использовать то, что число $|G|^{n/2}$ — целое и линейная комбинация элементов поля содержится в поле.

В дальнейшем полагаем p простым, а n чётным. Из свойства 2 утверждения 3 можно получить

Следствие 3. Для любых двух p-ичных бент-функций b и b' справедливо равенство $|\mathrm{supp}(\xi^b - \xi^{b'})| = |\mathrm{supp}(\widehat{\xi^b} - \widehat{\xi^{b'}})|$.

Для доказательства следствия достаточно проверить, что имеется $(p-1)/2$ различных чисел вида $|\xi^i - \xi^j|^2$, $i \neq j$, которые независимы над полем рациональных чисел.

Отсюда и из утверждения 1, а также следствия 1 имеем

Следствие 4. Расстояние Хэмминга между двумя бент-функциями, т. е. число аргументов из $\mathbb{Z}_p^n$, на которых они различаются, не меньше $p^{n/2}$. Если это расстояние равно $p^{n/2}$, то разность между ними равна $c\chi^\Gamma$, где $c \in \mathbb{Z}_p$; Γ — аффинное подпространство размерности $n/2$.

Из утверждения 2 можно получить

Следствие 5. Если бент-функция $b : \mathbb{Z}_p^n \to \mathbb{Z}_p$ аффинна на аффинном подпространстве Γ, то $\dim \Gamma \leqslant n/2$.

Следствие 6. Если бент-функция $b : \mathbb{Z}_p^n \to \mathbb{Z}_p$ аффинна на аффинном подпространстве размерности $n/2$, то найдётся ровно $p-1$ бент-функций, отличающихся от b только на этом подпространстве.

Поскольку аффинные преобразования не выводят из класса бент-функций, при доказательстве следствия 6 достаточно рассматривать содержащие нулевой вектор грани Γ размерности $n/2$ и бент-функции, постоянные на этой грани. Из утверждения 2 видно, что если ξ^b постоянна на Γ, то и $\widehat{\xi^b}$ постоянна на $\Gamma^\perp$ и принимает это же значение ξ^k, $k \in \mathbb{Z}_p$. Нетрудно видеть, что $\chi^{\Gamma^\perp} = \widehat{\chi^\Gamma}$. Тогда сумма $\xi^b + (\xi^m - \xi^k)\chi^\Gamma$, $m \in \mathbb{Z}_p$, также является бент-функцией.

Следствия 4–6 при $p = 2$ доказаны в [6] (следствия 5 и 6 имеются в [7]). В двоичном случае исследованы также возможные (не превышающие двух минимальных) расстояния между двумя бент-функциями [8].

2. Число бент-функций на минимальном расстоянии от квадратичной

Квадратичная форма $Q : (\mathrm{GF}(q))^n \to \mathrm{GF}(q)$ называется *невырожденной*, если её ядро $\{x \in (\mathrm{GF}(q))^n : \forall y \in (\mathrm{GF}(q))^n\,(Q(y+x) = Q(y))\}$ состоит из нуля. Линейное подпространство U в $(\mathrm{GF}(q))^n$ называется *тотально изотропным*, если $Q(U) = 0$. Максимальная размерность тотально изотропного подпространства называется *индексом Витта* формы Q. При $n = 2d$ максимальный индекс Витта невырожденной квадратичной формы равен d. Все квадратичные формы максимального индекса Витта эквива-

лентны (переводятся друг в друга невырожденным линейным преобразованием). Одним из представлений такой формы является $Q_0(v_1, \ldots, v_d, u_1, \ldots, u_d) = v_1u_1 + \ldots + v_du_d$.

Нетрудно показать, что Q_0 является бент-функцией (частным примером конструкции Майорана — МакФарланда [5]). Известно (см., например, [9, p. 274, Lemma 9.4.1]) следующее

Утверждение 4. Число тотально изотропных подпространств максимального индекса $d = n/2$ у квадратичной формы Q_0 равно $\prod_{i=1}^{d}(q^{d-i} + 1)$.

Нетрудно видеть, что если форма Q_0 аффинна на некотором аффинном подпространстве, то она аффинна и на любом его смежном классе. При $q > 2$ если форма Q_0 аффинна на некотором линейном подпространстве индекса d, то это подпространство тотально изотропно. Таким образом, форма Q_0 аффинна на всех смежных классах тотально изотропных подпространств индекса d и не аффинна на других аффинных подпространствах той же размерности.

Из утверждения 4 и следствия 6 имеем

Следствие 7. Пусть p — простое, $p > 2$. Тогда количество p-ичных бент-функций от $2d$ переменных, находящихся на расстоянии p^d от квадратичной формы Q_0, равно $p^d(p^{d-1} + 1) \cdots (p + 1)(p - 1)$.

В двоичном случае аналогичное утверждение доказано в [10]. В [11] доказано, что максимальное количество близких соседних бент-функций имеется только у квадратичной бент-функции. Можно предположить, что последнее свойство, характеризующее квадратичные функции, остаётся верным для всех простых $p > 2$.

ЛИТЕРАТУРА

1. *Tao T.* An uncertainty principle for cyclic groups of prime order // Math. Res. Lett. 2005. V. 12. No. 1. P. 121–127.
2. *Влэдуц С. Г., Ногин Д. Ю., Цфасман М. А.* Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003. 504 с.
3. *Kumar P. V., Scholtz R. A., and Welch L. R.* Generalized bent functions and their properties // J. Comb. Theory. Ser. A. 1985. V. 40. No. 1. P. 90–107.
4. *Токарева Н. Н.* Бент-функции и их обобщения // Прикладная дискретная математика. Приложение. 2009. № 2. С. 5–17.
5. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. опер. 2010. Т. 17. № 1. С. 34–64.
6. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
7. *Carlet C.* Two new classes of bent functions // Advances in Cryptology — EUROCRYPT'93. LNCS. 1994. No. 765. P. 77–101.
8. *Потапов В. Н.* Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информ. 2012. Т. 48. № 1. С. 54–63.
9. *Brouwer A. E., Cohen A. M., and Neumaier A.* Distance-Regular Graphs. N. Y.: Springer Verlag, 1989. 485 p.
10. *Коломеец Н. А.* Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. опер. 2012. Т. 19. № 1. С. 41–58.

11. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. 2014. №3. С. 28–39.

УДК 519.719.1 DOI 10.17223/2226308X/8/17

ПЕРЕЧИСЛЕНИЕ ДВОИЧНЫХ ФУНКЦИЙ, ИМЕЮЩИХ ЗАДАННОЕ ЧИСЛО АФФИННЫХ СОМНОЖИТЕЛЕЙ

А. В. Черемушкин

Предлагается рекурсивный способ вычисления числа двоичных функций от n переменных, имеющих заданное число аффинных сомножителей, допускающий введение ограничений на вес или степень нелинейности функций.

Ключевые слова: *двоичные функции, аффинная классификация, формула обращения Мёбиуса.*

1. Случай обычных функций

Пусть $n \geqslant 0$. Подсчитаем число двоичных функций от n переменных заданного веса, имеющих аффинные сомножители. Функция $f : V_n(2) \to \{0, 1\}$ *имеет аффинные сомножители*, если найдутся такие функция $l(x) = (x, a^*) \oplus b$, $x \in V_n(2)$, $0 \neq a^* \in \in V_n(2)^*$ ($V_n(2)^*$ — сопряжённое пространство), $b \in \{0, 1\}$ и функция h, что $f = l \cdot h$.

Пусть $k \in \{0, \ldots, n\}$. Обозначим через $\mathcal{F}_n(k)$ множество всех двоичных функций от n переменных, имеющих ровно k аффинных сомножителей. Функцию $f \equiv 0$ не включаем ни в одно из множеств $\mathcal{F}_n(k)$. Легко видеть, что выполняется равенство

$$\mathcal{F}_n = \bigcup_{k=0}^{n} \mathcal{F}_n(k) \cup \{0\}. \tag{1}$$

Справедливы следующие свойства:

1. Множества $\mathcal{F}_n(k)$ при разных k не пересекаются, $k = 0, \ldots, n$.
2. Множества $\mathcal{F}_n(k)$, $k = 0, \ldots, n$, инвариантны относительно действия полной аффинной группы $\mathbf{AGL}\,(n, 2)$ (и, следовательно, разбиваются на классы эквивалентности относительно этой группы).
3. Каждую функцию $f \in \mathcal{F}_n(k)$ можно привести с помощью некоторого аффинного преобразования к виду

$$h(x) = f(xQ \oplus b) = \overline{x}_1 \ldots \overline{x}_k g(x_{k+1}, \ldots, x_n), \tag{2}$$

   где $g \in F_{n-k}(0)$.
4. Если $k \in \{0, \ldots, n\}$ и $f \in \mathcal{F}_n(k)$, то $1 \leqslant \|f\| \leqslant 2^{n-k}$, где $\|f\|$ — вес функции f.
5. Множество векторов, входящих в область истинности $\{a \in V_n(2) : f(a) = 1\}$ функции f вида (2), порождает смежный класс по подпространству размерности $n - k$.

Теорема 1. Пусть $1 \leqslant k \leqslant n$ и функции $f, h \in \mathcal{F}_n(k)$ и $g \in \mathcal{F}_{n-k}(0)$ удовлетворяют равенству (2). Тогда порядки групп инерции функций f, h и g в группе аффинных преобразований связаны равенством

$$|\mathbf{AGL}\,(n, 2)_f| = |\mathbf{AGL}\,(n, 2)_h| = 2^{k(n-k)} |\mathbf{GL}\,(k, 2)| \cdot |\mathbf{AGL}\,(n-k, 2)_g|. \tag{3}$$

Доказательство вытекает из инвариантности подпространства, порождённого областью истинности функции.

При $n \geqslant 1$ числа

$$\left[\begin{array}{c} n \\ k \end{array} \right]_2 = \begin{cases} \prod\limits_{i=0}^{k-1} \dfrac{2^n - 2^i}{2^k - 2^i}, & \text{если } k \in \{1, \ldots, n\}, \\ 1, & \text{если } k = 0, \end{cases}$$

называются *коэффициентами Гаусса* (индекс 2 для простоты записи далее будем опускать).

Теорема 2. При $1 \leqslant k \leqslant n$ справедливо равенство

$$|\mathcal{F}_n(k)| = 2^k \left[\begin{array}{c} n \\ k \end{array} \right] \cdot |\mathcal{F}_{n-k}(0)|. \tag{4}$$

Доказательство. Для каждой функции $f \in \mathcal{F}_n(k)$ число эквивалентных ей функций совпадает с индексом группы инерции

$$|f^{\mathbf{AGL}\,(n,2)}| = (\mathbf{AGL}\,(n,2) : \mathbf{AGL}\,(n,2)_f),$$

который в силу теоремы 1 равен $2^k \left[\begin{array}{c} n \\ k \end{array} \right] \cdot |g^{\mathbf{AGL}\,(n-k,2)}|$. Применяя данное равенство для всех функций $f \in \mathcal{F}_n(k)$, получаем формулу (4). ■

Наряду с множествами $\mathcal{F}_n$ и $\mathcal{F}_n(k)$, $k = 0, \ldots, n$, рассмотрим $(2^n + 1)$-мерные вектор-столбцы $\mathcal{F}_n^{\downarrow}$ и $\mathcal{F}_n^{\downarrow}(k)$, j-я координата которых равна числу функций из соответствующего множества, имеющих вес j, $j = 0, \ldots, 2^n$. Для этих векторов справедливо аналогичное (1) соотношение

$$\mathcal{F}_n^{\downarrow} = \sum_{k=0}^{n} \mathcal{F}_n^{\downarrow}(k) + \{\varepsilon_0^{\downarrow}\},$$

где $\varepsilon_0^{\downarrow}$ — вектор, у которого первая координата равна 1, а остальные — нули. В силу свойства 4 у векторов $\mathcal{F}_n^{\downarrow}(k)$ первая координата и последние $2^n - 2^{n-k}$ координат равны нулю. Заметим, что в (2) веса функций f, h и g совпадают. Поэтому равенства, аналогичные (4), выполняются между первыми $2^{n-k} + 1$ координатами вектор-столбцов $\mathcal{F}_n^{\downarrow}$ и $\mathcal{F}_{n-k}^{\downarrow}(0)$. Дополним вектор $\mathcal{F}_{n-k}^{\downarrow}(0)$, имеющий длину $2^{n-k} + 1$, до вектора длины $2^n + 1$, полагая координаты с номерами j, $2^{n-k} + 1 \leqslant j \leqslant 2^n$, равными нулю. С учётом этого дополнения можно записать равенство (4) в векторном виде

$$\mathcal{F}_n^{\downarrow}(k) = 2^k \left[\begin{array}{c} n \\ k \end{array} \right] \mathcal{F}_{n-k}^{\downarrow}(0). \tag{5}$$

В силу равенств (4) и (5) для вычисления значений $\mathcal{F}_n^{\downarrow}(k)$, $k = 0, \ldots, n$, достаточно вычислить лишь величины $z_m = |\mathcal{F}_m(0)|$ и $z_{mj} = \mathcal{F}_m^{\downarrow}(0)_j$, $j = 0, \ldots, 2^m$, $m = 0, \ldots, n$.

Воспользуемся равенством

$$2^{2^n} = \sum_{k=0}^{n} |\mathcal{F}_n(k)| + 1,$$

которое непосредственно вытекает из равенства (1) и свойства 1.

Обозначая для краткости

$$h(n,k) = 2^k \left[\begin{array}{c} n \\ k \end{array} \right],$$

с учётом равенства (4) получаем рекуррентное соотношение

$$z_n = 2^{2^n} - 1 - \sum_{k=1}^{n} h(n,k) z_{n-k}. \tag{6}$$

Аналогично, с учётом равенства (5) имеем $z_{n0} = 0$ и для $j = 1, \ldots, 2^n$

$$z_{nj} = \binom{2^n}{j} - \sum_{k=1}^{n} h(n,k) z_{n-k,j}. \tag{7}$$

При этом при всех $n \geqslant 0$ выполнено равенство $\sum\limits_{j=0}^{2^n} z_{nj} = z_n$.

Рекуррентные соотношения (6) и (7) позволяют вычислять значения величин z_n и z_{nj}, $j = 0, \ldots, 2^n$, последовательно для $n = 0, 1, 2, \ldots$ В табл. 1 приведены соответствующие значения при $n = 3$.

Таблица 1

j	$\lvert\mathcal{F}_3\rvert$	$\{0\}$	$\lvert\mathcal{F}_3(3)\rvert$	$\lvert\mathcal{F}_3(2)\rvert$	$\lvert\mathcal{F}_3(1)\rvert$	$\lvert\mathcal{F}_3(0)\rvert$
0	1	1	0	0	0	0
1	8	0	8	0	0	0
2	28	0	0	28	0	0
3	56	0	0	0	56	0
4	70	0	0	0	14	56
5	56	0	0	0	0	56
6	28	0	0	0	0	28
7	8	0	0	0	0	8
8	1	0	0	0	0	1
Всего	256	1	8	28	70	149

Найдём теперь общий вид решений рекуррентных уравнений (6) и (7). Формула обращения Мёбиуса в данном случае принимает следующий вид.

Утверждение 1 [1, 2]. Если последовательности $\{u_n\}$ и $\{w_n\}$ связаны соотношением

$$u_n = \sum_{k=0}^{n} \left[\begin{array}{c} n \\ k \end{array} \right] w_{n-k}, \qquad n \geqslant 0,$$

то

$$w_n = \sum_{k=0}^{n} (-1)^k 2^{k(k+1)/2} \left[\begin{array}{c} n \\ k \end{array} \right] u_{n-k}, \qquad n \geqslant 0.$$

Переписав рекуррентное соотношение (6) в виде $\dfrac{2^{2^n}-1}{2^n} = \sum\limits_{k=0}^{n} \left[\begin{array}{c} n \\ k \end{array} \right] \dfrac{z^{n-k}}{2^{n-k}}$, с помощью формулы обращения получаем следующий окончательный результат.

Теорема 3. При всех $n \geqslant 0$ справедлива формула

$$z_n = |\mathcal{F}_n(0)| = \sum_{k=0}^{n} (-1)^k 2^{k(k+1)/2} \left[\begin{array}{c} n \\ k \end{array} \right] (2^{2^{n-k}} - 1) 2^k.$$

Эта формула позволяет, например, оценить вероятность p_n того, что у функции $f(x_1,\dots,x_n)$ есть аффинные сомножители:

$$p_n = 1 - \frac{z_n}{2^{2^n}}.$$

Значения вероятности p_n при $1 \leqslant n \leqslant 10$ представлены в табл. 2.

Таблица 2

n	p_n	n	p_n
1	0,75	6	$2{,}9 \cdot 10^{-8}$
2	0,6875	7	$1{,}3 \cdot 10^{-17}$
3	0,4218	8	$1{,}4 \cdot 10^{-38}$
4	0,0809	9	$8{,}8 \cdot 10^{-75}$
5	$8{,}9 \cdot 10^{-4}$	10	$1{,}5 \cdot 10^{-151}$

2. Случай сравнения функций по модулю

При $-1 \leqslant s \leqslant n-1$ обозначим $\mathcal{U}_s$ подпространство функций, степень нелинейности которых не превышает s (степень нулевой функции полагаем равной -1).

Аналогично предыдущему случаю, при $k \in \{0,\dots,n\}$ обозначим через $\mathcal{F}_n^{(s)}(k)$ множество всех двоичных функций, имеющих ровно k линейно независимых аффинных сомножителей по модулю $\mathcal{U}_s$. Функции $f \in \mathcal{U}_s$ не включаем ни в одно из множеств $\mathcal{F}_n^{(s)}(k)$, $k = 0,\dots,n$. Легко видеть, что выполняется равенство

$$\mathcal{F}_n = \bigcup_{k=0}^{n} \mathcal{F}_n^{(s)}(k) \cup \mathcal{U}_s.$$

Заметим, что в работе [4] получена точная формула для числа функций от n переменных с алгебраической иммунностью равной 1, т. е. $AI_n(f) = 1$. Этот класс функций можно записать в виде

$$B_1 = \bigcup_{k=1}^{n} \mathcal{F}_n^{(0)}(k).$$

Справедливы следующие свойства:

1. Множества $\mathcal{F}_n^{(s)}(k)$ при разных k не пересекаются, $k = 0,\dots,n$.
2. Множества $\mathcal{F}_n^{(s)}(k)$, $k = 0,\dots,n$, инвариантны относительно действия группы $\mathbf{AGL}\,(n,2)\mathcal{U}_s$ (и, следовательно, разбиваются на классы эквивалентности относительно этой группы).
3. Каждую функцию $f \in \mathcal{F}_n^{(s)}(k)$ можно привести с помощью некоторого аффинного преобразования к виду

$$h(x) = f(xQ \oplus b) \equiv \overline{x}_1 \cdots \overline{x}_k g(x_{k+1},\dots,x_n) \ (\mathrm{mod}\,\mathcal{U}_s), \tag{8}$$

где $g \in F_{n-k}^{(s-k)}(0)$.

Аналогично предыдущему случаю (подробнее см. [3]) доказываются:

Теорема 4. Пусть $s \geqslant 0$, $1 \leqslant k \leqslant n$ и функции $f, h \in \mathcal{F}_n^{(s)}(k)$ и $g \in \mathcal{F}_{n-k}^{(s-k)}(0)$ удовлетворяют равенству (8). Тогда порядки групп инерции функций f, h и g по модулю $\mathcal{U}_s$ связаны равенством

$$|\mathbf{AGL}\,(n,2)_f^{(s)}| = |\mathbf{AGL}\,(n,2)_h^{(s)}| =$$

$$= \begin{cases} 2^{k(n-k+1)}|\mathbf{GL}\,(k,2)| \cdot |\mathbf{AGL}\,(n-k,2)_g^{(s-k)}|, & \text{если } s = \deg f - 1, \\ 2^{k(n-k)}|\mathbf{GL}\,(k,2)| \cdot |\mathbf{AGL}\,(n-k,2)_g^{(s-k)}|, & \text{если } s \leqslant \deg f - 2. \end{cases}$$

Теорема 5. При всех $s \geqslant 0$, $1 \leqslant k \leqslant n$ справедливо равенство

$$|\mathcal{F}_n^{(s)}(k)| = \begin{cases} \begin{bmatrix} n \\ k \end{bmatrix} |\mathcal{F}_{n-k}^{(s-k)}(0)| \dfrac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } s = \deg f - 1, \\ 2^k \begin{bmatrix} n \\ k \end{bmatrix} |\mathcal{F}_{n-k}^{(s-k)}(0)| \dfrac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } s \leqslant \deg f - 2. \end{cases} \tag{9}$$

Равенство (9) позволяет составить соотношение рекуррентного типа, которое можно решить также с помощью формулы обращения Мёбиуса. Обозначим

$$z_{nj}^{(s)} = |\mathcal{F}_n^{(s)}(0) \cap (\mathcal{U}_j \backslash \mathcal{U}_{j-1})|, \quad j = 0, \ldots, n.$$

Аналогично введём $(n+1)$-мерные векторы $\mathcal{F}_n^{(s)}(k)^{\Downarrow}$, j-я координата которых равна числу функций из множества $\mathcal{F}_n^{(s)}(k)$ степени нелинейности j, $j = 0, \ldots, n$.

Пусть $n > j > s$. Воспользуемся соотношением

$$(2^{\binom{n}{j}} - 1)|\mathcal{U}_{j-1}^{(n)}| = \sum_{k=0}^{n} (\mathcal{F}_n^{(s)}(k)^{\Downarrow})_j,$$

которое непосредственно вытекает из свойства 1. С учётом равенства (9) и теоремы 5 при фиксированных j и s получаем соотношение

$$(2^{\binom{n}{j}} - 1)|\mathcal{U}_{j-1}^{(n)}| = \begin{cases} \displaystyle\sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} z_{n-k,j-k}^{(s-k)} \frac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } j = s+1, \\ \displaystyle\sum_{k=0}^{n} 2^k \begin{bmatrix} n \\ k \end{bmatrix} z_{n-k,j-k}^{(s-k)} \frac{|\mathcal{U}_s^{(n)}|}{|\mathcal{U}_{s-k}^{(n-k)}|}, & \text{если } j > s+1. \end{cases}$$

В табл. 3 приведены для примера соответствующие значения при $n = 3$.

Таблица 3

s	$\{\mathcal{U}_s\}$	$\lvert\mathcal{F}_3^{(s)}(3)\rvert$	$\lvert\mathcal{F}_3^{(s)}(2)\rvert$	$\lvert\mathcal{F}_3^{(s)}(1)\rvert$	$\lvert\mathcal{F}_3^{(s)}(0)\rvert$
-1	1	8	28	70	149
0	2	16	56	126	56
1	16	128	112	0	0
2	128	128	0	0	0
3	256	0	0	0	0

ЛИТЕРАТУРА

1. *Comtet M. L.* Nombres de Stirling generaux et fonctions symmetriques // C. R. Acad. Sc. Paris. 1972. V. 275. Ser. A. P. 747–750.
2. *Bender E. A. and Goldman J. R.* On the application of the Möbius inversion in combinatorial analysis // Amer. Math. Monthly. 1975. V. 82. No. 8. P. 789–803.
3. *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. Т. 4. М.: Физматлит, 2001. С. 273–314.
4. *Tu Z. and Deng Y.* Algebraic Immunity Hierarchy of Boolean Functions. Cryptology ePrint Archive, Report 2007/259, 2007. `e-print.iacr.org`. 6 p.

УДК 512.55 DOI 10.17223/2226308X/8/18

НЕКОТОРЫЕ СТРУКТУРНЫЕ СВОЙСТВА КВАДРАТИЧНЫХ БУЛЕВЫХ ПОРОГОВЫХ ФУНКЦИЙ

А. Н. Шурупов

На основе бинарного отношения частичного порядка, заданного на множестве квадратичных форм с булевыми переменными, предлагается способ описания классов квадратичных булевых пороговых функций (к.б.п.ф.), одновременно допускающих (или не допускающих) нетривиальную декомпозицию. Указаны представители классов, функциональная разделимость которых означает выполнение этого свойства и для всех функций из класса. В частных случаях исследована существенная зависимость к.б.п.ф. от своих переменных.

Ключевые слова: *квадратичная булева пороговая функция, декомпозиция, существенная переменная.*

Полиномиальные булевы пороговые функции определяются следующим образом [1]:

$$f(x_1,\dots,x_n)=0 \Leftrightarrow g(x_1,\dots,x_n)\leqslant 0, \tag{1}$$

где g — действительный полином. Если $\deg g=2$, то говорят о к.б.п.ф. В последнем случае неравенство из (1) может быть преобразовано в эквивалентное $q(x_1,\dots,x_n)\leqslant t$, где q — квадратичная форма, а t — свободный член многочлена g, взятый с противоположным знаком и называемый порогом.

Пусть $A_w=\{\{w(x):x\in\{0,1\}^n\}\}$ — мультимножество значений квадратичной формы $w(x)$. Через $\{A_w\}$ обозначается множество значений $w(x)$. Под набором $w^*=\big(w_0^*,w_1^*\dots,w_{2^n-1}^*\big)$ понимается набор упорядоченных по неубыванию элементов множества A_w. В тексте без особых оговорок используются обозначения из [2] для линейных булевых пороговых функций, которые без изменения переносятся на полиномиальный случай. В частности, факт, что к.б.п.ф. задаётся квадратичной формой q и порогом t, для краткости записывается как $f\sim(q,t)$. Имея две квадратичные формы от независимых переменных — $p(x)$ и $q(y)$, можно составить новую квадратичную форму $h(x,y)=p(x)+q(y)$ (будем обозначать $h=p|q$).

Рассмотрим бинарное отношение частичного порядка на множестве действительных квадратичных форм. Если q^* является подпоследовательностью r^* для квадратичных форм $q(x)$ и $r(y)$ (возможно, от разного числа переменных, но все переменные из x входят в y), то будем обозначать этот факт как $q\prec r$. В дальнейшем без ограничения общности будем полагать все веса целыми числами. Важность введённого бинарного отношения по отношению к изучению функциональной структуры к.б.п.ф. следует из следующего утверждения.

Утверждение 1 [2]. Пусть к.б.п.ф. $f\sim(p_1|q_1,t)$ и $g\sim(p_2|q_2,t)$ удовлетворяют свойству $p_1\prec p_2$, $q_1\prec q_2$. Тогда если g допускает простую декомпозицию, то и f допускает простую декомпозицию.

Под нетривиальной простой декомпозицией понимается следующая бесповторная суперпозиция для некоторого $m\in\{2,\dots,n-1\}$:

$$f(x_1,\dots,x_n)=\varphi\big(\psi(x_1,\dots,x_m),x_{m+1},\dots,x_n\big).$$

Утверждение 1 позволяет предложить способ построения классов функционально разделимых (или функционально неразделимых) к.б.п.ф., равно как и подход к анализу функциональной разделимости заданной к.б.п.ф. Пусть $\{u_i\}$ и $\{v_i\}$ — множества

квадратичных форм от m_i и n_i переменных ($m_i, n_i > 1$), имеющие верхние грани u и v относительно введённого бинарного отношения. Тогда если пороговая функция со структурой $(u|v,t)$ функционально разделима, то и любая пороговая функция со структурой $(u_i|v_i,t)$ также функционально разделима. Справедливо и отрицание этого утверждения.

Замечание 1. Утверждение 1 и вышеприведённые рассуждения не зависят от вида неравенства, задающего пороговую функцию, и поэтому справедливы для полиномиальных пороговых функций.

Для целочисленной матрицы W квадратичной формы определим *троичное представление* — матрицу $U^W = (u^W_{ij})_{i,j=1,\dots,N}$ некоторой квадратичной формы u^W, задаваемую следующим образом. Элементу w_{ij} матрицы W в матрице U^W соответствует клетка размера $l_i \times l_j$, причём клетки не пересекаются и расположены в том же порядке, что и сами элементы w_{ij} в матрице W. Натуральные числа l_i, $i = 1, \dots, n$, удовлетворяют условиям

$$\begin{cases} l_i l_j \geqslant |w_{ij}|, \\ N = \sum\limits_{i=1}^{n} l_i \to \min. \end{cases} \tag{2}$$

В каждой клетке произвольным образом (с сохранением свойства симметричности матрицы U^W) расставляются единицы в случае $w_{ij} > 0$ и -1 для $w_{ij} < 0$. Остальные элементы полагаются равными нулю. Троичное представление всегда существует, например, можно положить $l_i = \max\limits_{j\in\{1,\dots,n\}} w_{ij}$, хотя в этом случае условие минимальности размера N троичного представления не обязательно выполняется. Несмотря на то, что минимизация размера N полезна в практическом смысле, использование троичного представления не связано строго с этим свойством, поэтому в дальнейшем под троичным представлением также будем понимать и неоптимальные по размеру матрицы.

Дополнительный способ сокращения размера троичного представления связан с переходом к матрице $\tilde{W} = \dfrac{1}{d}W$, где $d = \text{НОД}\{w_{ij}\}$.

Задача (2) относится к задачам целочисленного квадратичного программирования с линейной целевой функцией. Путём перехода к величинам $r_i = \log l_i$ эта задача приобретает вид задачи линейного программирования в дискретной решётке $\log \mathbb{N}$. Для решения последней задачи с учётом необязательности выполнения требования оптимальности может быть применён полиномиальный алгоритм Хачияна [3] с последующим «округлением» результата в ближайший узел решётки. Отсутствие требования оптимальности делает возможным использование приближённых алгоритмов решения задачи целочисленного программирования [4, 5].

Из определения троичного представления и предшествующих рассуждений следует его неоднозначность. Другое важное свойство заключается в том, что если для булева вектора $a = (a_1, \dots, a_n)$ положить компоненты булева вектора $b = (b_1, \dots, b_N)$ в соответствии с условием $a_i = 1 \Leftrightarrow b_{l_1+\dots+l_{i-1}+1} = \dots = b_{l_1+\dots+l_i} = 1$, то

$$w(a) = aWa^T = bU^W b^T \stackrel{\text{def}}{=} u^W(b). \tag{3}$$

Справедливость (3) следует из того, что серии нулей и единиц в векторе b соответствуют клеткам матрицы U^W. Следовательно, коэффициенты w_{ij}, участвующие в вычислении (т. е. индексы i и j, такие, что $a_i = a_j = 1$), соответствуют клеткам с суммарным количеством элементов равным $\operatorname{sgn}(w_{ij})|w_{ij}|$. Таким образом, доказано

Утверждение 2. Справедливы следующие отношения:
1) $w \prec u^W$;
2) $w \prec du^{\tilde{W}}$, где $d = \text{НОД}\{w_{ij}\}$.

Представляет интерес описание функциональной структуры к.б.п.ф с матрицей квадратичной формы, имеющей вид троичного представления. Для этого, в частности, рассмотрим вопрос о существенных переменных к.б.п.ф. с матрицами квадратичных форм простого вида.

Пусть $\mathbf{1}_n$ — целочисленная квадратная матрица размера n, состоящая из одних единиц. Легко видеть, что $\{A_{\mathbf{1}_n}\} = \{k^2 : k = 0, \ldots, n\}$.

Утверждение 3. К.б.п.ф. $f \sim (\mathbf{1}_n, t)$, отличная от константы, зависит существенно от всех своих переменных.

Доказательство. Так как функция f симметричная, достаточно доказать утверждение для первой переменной. Пусть для некоторого s выполняется $t \in [s^2, (s+1)^2)$. Такое $0 \leqslant s \leqslant n-1$ существует всегда, так как по условию $0 \leqslant t < n^2$. Тогда выполняются неравенства $w(0, a) = s^2 \leqslant t$ и $w(1, a) = s^2 + 2n - 1 \geqslant (s+1)^2 > t$, где a — произвольный вектор размера $n-1$ с весом s. ■

Рассмотрим структурные свойства к.б.п.ф. $f \sim (\mathbf{1}_m | \mathbf{1}_{n-m}, t)$, где $1 \leqslant m \leqslant n-1$.

Утверждение 4. К.б.п.ф. $f \sim (\mathbf{1}_m | \mathbf{1}_{n-m}, t)$ зависит существенно от первых m $(1 \leqslant m \leqslant n-1)$ переменных, если и только если найдутся такие $r \in \{0, \ldots, m-1\}$, $s \in \{0, \ldots, n-m\}$, что выполняется система неравенств

$$\begin{cases} r^2 + s^2 \leqslant \lfloor t \rfloor_w, \\ (r+1)^2 + s^2 \geqslant \lceil t \rceil_w, \end{cases} \tag{4}$$

где квадратичная форма $w = (\mathbf{1}_m | \mathbf{1}_{n-m})$; $\lfloor t \rfloor_w$ и $\lceil t \rceil_w$ — нижние и верхнее приближения числа t в множестве $\{A_w\}$ [2].

Доказательство. Без ограничения общности будем рассматривать существенную зависимость функции f от первой переменной. Докажем утверждение, заменив (4) на равносильную систему

$$r^2 + s^2 \leqslant t < (r+1)^2 + s^2. \tag{5}$$

Действительно, по свойствам верхнего и нижнего приближений $\lfloor t \rfloor_w \leqslant t < \lceil t \rceil_w$, поэтому из (4) следует (5). Так как $r^2 + s^2$, $(r+1)^2 + s^2 \in \{A_w\}$, то справедлива и обратная импликация.

Достаточность. Если для некоторых $r \in \{0, \ldots, m-1\}$ и $s \in \{0, \ldots, n-m\}$ выполняется (4), то значения функции f на булевых векторах $(0, u, v)$ и $(1, u, v)$ различаются, где u — произвольный вектор длины $m-1$ и веса r, а v — произвольный вектор длины $n-m$ веса s. Действительно, $w(0, u, v) = r^2 + s^2 \leqslant t < (r+1)^2 + s^2 = w(1, u, v)$.

Необходимость. Пусть от противного выполняется отрицание (5), т. е. для каждой пары (r, s) верно $t < r^2 + s^2$ или $t \geqslant (r+1)^2 + s^2$, что в силу неравенств $t < r^2 + s^2 < (r+1)^2 + s^2$ и $t \geqslant (r+1)^2 + s^2 > r^2 + s^2$ равносильно совпадению значений функции на произвольных векторах $(0, u, v)$ и $(1, u, v)$, т. е. несущественной зависимости функции f от первой переменной. ■

Следствие 1. К.б.п.ф $f \sim (\mathbf{1}_1 | \mathbf{1}_{n-1}, t)$ зависит существенно от первой переменной тогда и только тогда, когда $k^2 \leqslant t < k^2 + 1$ для некоторого $k \in \{0, \ldots, n-1\}$.

Пример 1. К.б.п.ф. $f \sim (\mathbf{1}_1|\mathbf{1}_3, 2)$ зависит несущественно от первой переменной. Её таблица истинности и многочлен Жегалкина такие же, как для пороговой функции $((1,1,1),1)$, т. е. $x_2x_3 + x_2x_4 + x_3x_4$.

Пример 2. К.б.п.ф. $g_1 \sim (\mathbf{1}_2|\mathbf{1}_3, 8)$ имеет многочлен Жегалкина $x_3x_4x_5$, хотя при порогах 7 или 9 с той же матрицей квадратичной формы соответствующие функции g_2 и g_3 зависят существенно от всех пяти переменных и имеют многочлены Жегалкина $x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4x_5$ и $x_1x_3x_4x_5 + x_2x_3x_4x_5 + x_1x_2x_3x_4x_5$ соответственно. При этом функция g_1 является линейной пороговой со структурой $((0,0,1,1,1),2)$, а функции g_2 и g_3 — линейными пороговыми со структурами $((1,1,3,3,3),7)$ и $((1,1,3,3,3),9)$ соответственно. Кроме того, обе функции допускают декомпозиции $g_2 = x_1x_2(x_3x_4 + x_3x_5 + x_4x_5 + x_3x_4x_5)$ и $g_3 = (x_1 + x_2 + x_1x_2)x_3x_4x_5$.

Приведённые примеры показывают, что даже в случае очень простых квадратичных форм задаваемые ими к.б.п.ф. могут сильно отличаться в смысле существенной зависимости от переменных при небольших (последовательных) изменениях порога. Кроме того, интерес представляет нахождение пороговой степени (см. определение в [1]) к.б.п.ф. В заключение отметим, что даже для линейной пороговой булевой функции задача определения существенной зависимости переменной является NP-полной [6, теорема 9.26, с. 436], что повышает значимость разработки эвристических методов её решения.

ЛИТЕРАТУРА

1. *Подольский В. В.* Оценки весов персептронов (полиномиальных пороговых булевых функций): автореф. дис. ... канд. физ.-мат. наук. М.: МГУ им. М. В. Ломоносова, 2009.
2. *Шурупов А. Н.* О функциональной разделимости булевых пороговых функций // Дискретная математика. 1997. Т. 9. Вып. 2. С. 59–73.
3. *Хачиян Л. Г.* Полиномиальный алгоритм в линейном программировании // Докл. АН СССР. 1979. Т. 244. № 5. С. 1033–1096.
4. *Dreo J., Petrowski A., Siarry P., and Taillard E.* Metaheuristics for Hard Optimisation. Methods and Case Studies. Springer, 2006. 372 p.
5. *Хохлюк В. И.* Прямой метод целочисленной оптимизации. Новосибирск: Ин-т математики им. С. Л. Соболева, 2002. 38 с.
6. *Crama Y. and Hammer P.* Boolean Functions. Theory, Algorithms and Applications. Cambridge University Press, 2011.

УДК 519.7 DOI 10.17223/2226308X/8/19

О СВОЙСТВАХ МНОЖЕСТВА ЗНАЧЕНИЙ ПРОИЗВОЛЬНОЙ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ[1]

Г. И. Шушуев

Исследуются свойства множества значений производных векторной булевой функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$. Получены достаточные условия того, что множество всех значений производных некоторой булевой функции совпадает с $\mathbb{F}_2^n$. Этот результат связан с некоторым открытым вопросом о метрических свойствах APN-функций.

[1]Работа поддержана грантом РФФИ, проект № 15-31-20635.

Ключевые слова: *векторная булева функция, дифференциально δ-равномерная функция, APN-функция.*

В работе рассматриваются векторные булевы функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, которые также известны как S-блоки. Они играют центральную роль для криптографической стойкости блочных шифров.

В 1994 г. K. Nyberg [1] ввела понятие дифференциально δ-равномерных векторных булевых функций. Векторная булева функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *дифференциально δ-равномерной*, если для любого ненулевого вектора $a \in \mathbb{F}_2^n$ и любого вектора $b \in \mathbb{F}_2^n$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений, где δ — целое положительное число. *Порядком* дифференциальной равномерности функции F назовём минимальное возможное δ, такое, что F — дифференциально δ-равномерная функция.

Чем меньше порядок дифференциальной равномерности S-блока, который используется в шифре, тем выше стойкость шифра к дифференциальному криптоанализу [2]. Минимальное возможное значение, которое может принимать δ, — это 2. Если $\delta = 2$, то дифференциально δ-равномерная функция называется APN-функцией (*Almost Perfect Nonlinear*). Для векторной булевой функции F и любого ненулевого вектора $a \in \mathbb{F}_2^n$ определим множество

$$B_a(F) = \{F(x) \oplus F(x \oplus a) : x \in \mathbb{F}_2^n\}.$$

Максимальная достижимая мощность множества $B_a(F)$ равна 2^{n-1}. В частности, если при любом ненулевом векторе a выполнено $|B_a(F)| = 2^{n-1}$, то функция F является APN [3].

В работе [4] исследовалось расстояние между различными APN-функциями, в связи с этим была выдвинута следующая гипотеза.

Гипотеза 1. Если F — APN-функция от n переменных, то выполнено

$$\forall x' \in \mathbb{F}_2^n \left(\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} (B_a(F) \oplus F(x' \oplus a)) = \mathbb{F}_2^n \right).$$

Для доказательства этой гипотезы требуется рассматривать объединение множеств $B_a(F)$. В данной работе исследуются некоторые свойства множества значений произвольной векторной булевой функции из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$, а именно множество значений её производных. Полученные результаты помогут в изучении метрических свойств класса APN-функций.

Суммой двух множеств $A, B \subseteq \mathbb{F}_2^n$ назовём множество всех попарных сумм элементов этих множеств: $A \oplus B = \{a \oplus b : a \in A, b \in B\}$. Сумма вектора $x \in \mathbb{F}_2^n$ и множества $A \subseteq \mathbb{F}_2^n$ — сдвиг множества A: $x \oplus A = \{x \oplus a : a \in A\}$. Множество всех значений векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *образом* функции F и обозначается $\mathrm{im}(F)$.

Лемма 1. Пусть $A, B \subseteq \mathbb{F}_2^n$, $|A| \geqslant 2^{n-1}$ и $|B| \geqslant 2^{n-1} + 1$. Тогда $A \oplus B = \mathbb{F}_2^n$.

Теорема 1. Пусть $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — векторная булева функция. Тогда:

1) если $2^{n-1} < |\mathrm{im}(F)| < 2^n$, то

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} B_a(F) = \mathbb{F}_2^n;$$

2) если $|\mathrm{im}(F)| = 2^n$, т. е. F является перестановкой, то

$$\bigcup_{a\in\mathbb{F}_2^n, a\neq 0} B_a(F) = \mathbb{F}_2^n \backslash \{0\}.$$

Условие на мощность образа функции не может быть ослаблено. Существуют функции F, у которых мощность образа равна $|\mathrm{im}(F)| = 2^{n-1}$ и выполнено $\bigcup\limits_{a\in\mathbb{F}_2^n, a\neq 0} B_a(F) \neq \mathbb{F}_2^n$. Например, такова APN-функция $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$, заданная вектором значений $(0, 0, 1, 2, 1, 4, 2, 4)$. Для неё $|\mathrm{im}(F)| = 2^2$, а $\bigcup\limits_{a\in\mathbb{F}_2^n, a\neq 0} B_a(F) = \mathbb{F}_2^n \backslash \{7\}$.

Теорема показывает, как ведёт себя объединение множеств $B_a(F)$, при каких условиях на образ функции F объединение даёт всё пространство $\mathbb{F}_2^n$, а при каких нет.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
2. *Biham E. and Shamir A.* Differential cryptoanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
3. *Beth T. and Ding C.* On almost perfect nonlinear permutations // LNCS. 1994. V. 765. P. 65–76.
4. *Шушуев Г. И.* Векторные булевы функции на расстоянии один от APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 36–37.

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.113.6 DOI 10.17223/2226308X/8/20

ШИФРЫ С ВОДЯНЫМИ ЗНАКАМИ

Г. П. Агибалов

Для защиты конфиденциальности и легальности данных вводится понятие шифра с водяным знаком (называемого также w-шифром). Его основная идея следующая: преобразование открытого текста x композицией операций шифрования и расшифрования с использованием соответствующих ключей приводит к некоторому подходящему тексту x', сохраняющему информацию текста x и содержащему некоторый уникальный водяной знак w, идентифицирующий подлинного владельца x'. Ключи зашифрования и расшифрования в w-шифре должным образом связаны друг с другом и с заданным водяным знаком w. В отличие от шифров, обычно изучаемых в криптографии, функция шифрования в w-шифре не обязательно обратимая. Таким образом, фактически w-шифры не являются шифрами в известном смысле этого слова, но шифры суть w-шифры некоторого частного вида, и все термины, понятия и обозначения, относящиеся к шифрам, полностью применимы к w-шифрам. Показано, как применением w-шифра можно осуществить встраивание водяного знака в данные в процессе зашифрования открытого текста либо в процессе расшифрования шифртекста. Приводятся примеры w-шифров, построенных на базе симметричных поточных шифров.

Ключевые слова: *защита данных, шифрование, водяные знаки, шифры с водяными знаками, поточные шифры.*

Введение

Методы шифрования данных и внедрения в них водяных знаков принадлежат различным областям науки — криптографии [1, 2] и стеганографии [3, 4] соответственно. Первые применяются для защиты конфиденциальности информации, вторые — для защиты информации от её нелегального использования. Как правило, шифрование данных является обратимым преобразованием с ключом расшифрования, неизвестным злоумышленнику, а внедрение в данные водяного знака есть операция сокрытия последнего в данных для идентификации автора нелегальной копии данных. Предполагается, что это сокрытие производится без существенного искажения защищаемых данных, как это делается, например, при внедрении водяного знака в цифровое видео. Рассматривается проблема обеспечения защиты данных от обеих указанных угроз. Есть два тривиальных способа решить эту проблему: сначала внедрить водяной знак в данные и затем зашифровать полученный открытый текст, либо, наоборот, сначала зашифровать данные и затем после расшифрования внедрить в полученный текст нужный водяной знак. Имеются, однако, серьёзные ограничения к применению этих способов на практике [4]. В частности, второй способ предполагает доверенного получателя данных, каковым не является, например, покупатель тех же видеоданных.

В работе вводится понятие шифра с водяным знаком, называемого, для краткости, w-шифр, или, в англоязычной транскрипции, a watermarking cipher. В нём преобразование открытого текста x композицией алгоритмов зашифрования и расшифрования, использующих некоторые, должным образом подобранные ключи зашифрования и расшифрования, порождает текст x', содержащий заданный водяной знак w. Мы показываем, каким образом с помощью w-шифра возможно внедрение водяного знака в данные (в тайне от их получателя, естественно) как в процессе зашифрования данных отправителем, так и в процессе расшифрования данных их получателем. Функции зашифрования и расшифрования в w-шифре не обязательно связаны между собой отношением обратимости, как в криптографических шифрах. Это значит, что в действительности w-шифры не обязаны быть шифрами, но всякий шифр является частным случаем w-шифра (с вырожденным водяным знаком), и все термины, понятия и обозначения, относящиеся к шифрам, вполне уместны и в применении к w-шифрам.

Далее, прежде чем дать общее определение шифров с водяными знаками и описать некоторые конкретные примеры их, мы сформулируем некоторые допущения и предположения, необходимые для того, чтобы сделать это более или менее корректно и понятно.

1. Проблема w-шифрования

Прежде всего, предположим для простоты, что защищаемые данные представлены конечной последовательностью (строкой, словом) символов, являющихся элементами аддитивной группы G с операцией сложения $+$. Например, $G = \mathbb{Z}_n$ или $G = \mathbb{Z}_2^n$ для некоторого $n \geqslant 2$, и т. п. В частности, данные могут быть представлены последовательностью бит (возможно, с некоторой структурой). Для любых $a = a_1a_2 \dots a_r$ и $b = b_1b_2 \dots b_r$ в G^r пусть $a + b = (a_1 + b_1)(a_2 + b_2) \dots (a_r + b_r)$, $-b = (-b_1)(-b_2) \dots (-b_r)$ и $a - b = a + (-b)$.

Предполагается, что водяной знак является некоторой парой $w = (v, \eta)$, где $v = v_1v_2 \dots v_m \in (G \setminus \{0\})^m$ и $\eta = i_1i_2 \dots i_m$, $i_j \in \{1, \dots, l\}$, $j = 1, \dots, m$, $1 \leqslant i_1 < i_2 < \dots < i_m \leqslant l$ для некоторого $l \geqslant 1$. В случае необходимости он обозначается $(v, \eta)_l$. Водяной знак $w' = (v', \eta)$, в котором $v' = -v$, называется инверсией знака w и обозначается $-w$. Очевидно, $-(-w) = w$. В случае $|G| = 2$ считаем, что $G = \mathbb{Z}_2$. В этом случае в любом водяном знаке $w = (v, \eta)$ слово v есть вектор $11 \dots 1$, так что w однозначно определяется набором η, и мы пишем $w = \eta$.

Встраивание водяного знака w в строку данных $x = x_1x_2 \dots x_l \in G^l$ выполняется с помощью операции сложения, определённой на G. Результатом встраивания является строка данных $x' = x'_1x'_2 \dots x'_l$, в которой $x'_j = x_j + v_t$, если $j = i_t \in J = \{i_1, \dots, i_m\}$, и $x'_j = x_j$, если $j \in \{1, \dots, l\} \setminus J$. Говорим, что строка x' есть строка x с внедрённым знаком w, и обозначаем её $x + w$. Мы пишем также $x - w$ вместо $x + (-w)$. Строка v и набор η называются соответственно значением и местоположением знака w в x'. Фактически, числа $i_1, i_2, \dots, i_m$ в η указывают позиции в x для встраивания $v_1, v_2, \dots, v_m$ соответственно из значения v знака w. Набор η называется подходящим местоположением для w в x, если x' получается из x без заметной потери информации. В этом случае мы называем x' производной (или копией) от x с корректно (или приемлемо) встроенным (внедрённым) водяным знаком w.

Например, если x является битовой строкой цифрового видео и $v = 11 \dots 1 \in \mathbb{Z}_2^m$, то встраивание знака w в x состоит в инвертировании бит $x_{i_1}, x_{i_2}, \dots, x_{i_m}$. В этом случае если позиции бит $i_1, i_2, \dots, i_m$ выбраны так, что инверсия этих бит в x заметно не разрушает видео, то полученная битовая строка x' является копией строки x с при-

емлемо внедрённым водяным знаком w, обе x' и x могут равнозначно использоваться как цифровое видео, но x', кроме того, содержит водяной знак для идентификации потенциального злоумышленника.

Мы говорим, что водяной знак и строка данных взаимно подходящие, т. е. w подходит для x и наоборот, если x имеет экспоненциальное количество подходящих местоположений для w в x. Здесь под экпоненциальным количеством подразумевается экспоненциальная функция от длины m знака w. Такое число походящих местоположений предотвращает злоумышленника от атаки грубой силы перечислением всех возможных подходящих местоположений в x'. Так, цифровые аудио- и видеоданные являются двумя примерами битовой строки данных, для которой встраивание водяного знака путём инверсии битов в некоторых позициях является подходящим.

Кроме того, мы предполагаем, что существуют производитель (DP) строки данных x и её покупатели, или клиенты (DC). Производитель DP хочет передать строку x некоторому DC U так, что никто другой не может перехватить x или секретно получить её в своё собственное владение от U. С этой целью DP должен выбрать уникальный и подходящий водяной знак w и некоторый ключ шифрования k_e для некоторого w-шифра C, зашифровать x, применив C и k_e, и послать клиенту U полученный так шифртекст y и нужный ключ расшифрования k_d, построенный таким образом, что расшифрование y на этом ключе даёт в качестве результата некоторую строку данных x', которая является производной от x, с корректно внедрённым знаком w. При этом неважно, на какой стадии, во время шифрования или расшифрования, w встроен в x. Расшифровывая y на ключе k_d, клиент U получает уникальную и приемлемую копию x' данных x. Если U передаст её другому клиенту, то DP сможет однозначно идентифицировать U по значению v из w и его местоположению η в x'.

Поскольку U сам может быть мошенником, ключ расшифрования k_d должен быть связан с водяным знаком w так, что определить w по k_d и шифртексту y вычислительно невозможно за реальное время, т. е. не существует алгоритма вообще или с полиномиальной сложностью (как функции от m), вычисляющего w из k_d и y.

2. Определение w-шифра

Итак, мы приходим к следующему понятию w-шифра: для любых взаимно подходящих водяного знака w и открытого текста x преобразование последнего композицией операций зашифрования и расшифрования на соответствующих ключах, связанных некоторым образом друг с другом и с w, создаёт текст $x' = x + w$, представляющий собой результат внедрения w в x: На этом пути мы вводим два типа w-шифров:

1) w-шифр с w-расшифрованием — открытый текст x зашифровывается в зависимости только от ключа k w-шифра, а полученный шифртекст y расшифровывается в зависимости от k и подходящего водяного знака w. Таким образом, значение k_e ключа зашифрования может быть произвольным, ключ расшифрования k_d должен быть предопределён выбранными k_e и w, т. е. быть функцией от k и w;
2) w-шифр с w-зашифрованием — открытый текст x зашифровывается в зависимости от ключа k w-шифра и подходящего водяного знака w, а полученный шифртекст y расшифровывается в зависимости только от k. Таким образом, ключ зашифрования k_e должен быть функцией от k и w, ключ расшифрования k_d должен быть функцией только от k.

Формально w-шифр определяется набором из шести объектов $C = (X, K, W, h, E, D)$, где X есть множество строк данных, включая открытые тексты, шифртексты и тек-

сты с встроенными водяными знаками, $X = G^*$; K и W суть множества ключей и водяных знаков соответственно; h есть ключевая функция, $h : K \times W \to K$, и E и D суть алгоритмы зашифрования и расшифрования соответственно, являющиеся некоторыми отображениями $E : X \times K \to X$ и $D : X \times K \to X$, такими, что для любых взаимно подходящих $x \in X$ и $w \in W$ и для любого $k \in K$ удовлетворяются следующие условия:

1) в w-шифре с w-расшифрованием —

$$\text{если } E(x,k) = y, \text{ то } D(y, h(k,w)) = x' = x + w;$$

2) в w-шифре с w-зашифрованием —

$$\text{если } E(x, h(k,w)) = y, \text{ то } D(y,k) = x' = x + w.$$

В случае $h(k,w) = k$ для любых $k \in K, w \in W$ мы допускаем вместо k писать $h(k,w)$ в последних выражениях и Λ вместо h в C.

3. Примеры w-шифров

Тривиальный пример w-шифра (X, K, W, Λ, E, D) над G можно построить из симметричного шифра (X, Y, K, E', D') с $X = Y = G^*$ и множества W водяных знаков, положив $E(x,k) = E'(x + w, k)$ и $D(y,k) = D'(y,k)$ или $E(x,k) = E'(x,k)$ и $D(y,k) = D'(y,k) + w$.

Простейшим нетривиальным примером w-шифра является одноразовый блокнот с водяным знаком $C_1 = (X, K, W, h, E, D)$, где $X = K = G^*$. В этом w-шифре с w-расшифрованием для данного водяного знака $w = (v, \eta)$ шифртекст $y = y_1 y_2 \dots y_l \in X$ получается сложением открытого текста $x = x_1 x_2 \dots x_l \in X$ и ключа $k = z_1 z_2 \dots z_l \in K$, т. е. $y = x + k$, и расшифрование y в открытый текст $x' = x'_1 x'_2 \dots x'_l \in X$ с водяным знаком w производится вычитанием другого ключа $k' = k - w = z'_1 z'_2 \dots z'_l \in K$ из y, т. е. $x' = y - k'$.

Этот же w-шифр с w-зашифрованием описывается соотношениями $k' = k + w$, $y = x + k'$, $x' = y - k$.

Непосредственно проверяется, что в обоих случаях $x' = x + w$. В первом случае $k_e = k$, $k_d = h(k,w) = k'$ и знак w автоматически встраивается в x в процессе расшифрования. Во втором случае это делается в процессе зашифрования и $k_e = k' = h(k,w)$, $k_d = k$.

Другими словами, для любых $l \geqslant 1$, $x, k \in G^l$ и $w \in W$

1) в C_1 с w-расшифрованием —

$$E(x,k) = x + k = y,\ h(k,w) = k - w,\ D(y, h(k,w)) = y - h(k,w) = y - k + w = x';$$

2) в C_1 с w-зашифрованием —

$$h(k,w) = k + w,\ E(x, h(k,w)) = x + h(k,w) = x + k + w = y,\ D(y,k) = y - k = x'.$$

Ещё одним примером w-шифра является поточный шифр с водяным знаком $C_A = (X, K, W, h, E, D)$ над конечным полем F с $X = F^*$ и с генератором ключевого потока, являющимся некоторым конечным автономным автоматом A с нелинейной функцией выходов. Автомат A представляется четвёркой объектов $A = (Q, Z, g, f)$, где Q, Z суть множества состояний и выходных символов соответственно, $Q = F^n$, $n \geqslant 1$, $Z = F$ и g, f суть функции переходов и выходов автомата A, $g : Q \to Q$, $f : Q \to Z$. Предполагается, что функция выходов f является непременно частью ключа k w-шифра.

Иногда начальное состояние $q(1)$ автомата A и его функция переходов g могут быть другими частями этого ключа. Далее, для общности, произвольный ключ в K обозначается знаком $k[q(1), g, f]$, подразумевающим f обязательной и $q(1)$ и g опциональными составляющими ключа. Предполагается также, что в A для любого начального состояния $q(1) \in Q$ и целого $l \geqslant 1$ состояния $q(t) = g^{t-1}(q(1))$, $t = 1, 2, \ldots, l$, все различные. В этом случае для любого $w = (v, \eta)_l \in W$ с $v = v_1 v_2 \ldots v_m$ и $\eta = i_1 i_2 \ldots i_m$ можно определить функцию $\delta_{w,q(1),l} : Q \to Z$ таким образом, что для любого $s \in Q$, $\delta_{w,q(1),l}(s) = v_j$, если $s = q(i_j)$, $j \in \{1, 2, \ldots, m\}$, и $\delta_{w,q(1),l}(s) = 0$ в противном случае, т. е. если $s = q(t)$, $t \in \{1, 2, \ldots, l\} \setminus \{i_1, i_2, \ldots, i_m\}$. Ключевая функция h, алгоритмы шифрования и расшифрования E, D и ключи k_e, k_d в C_A определяются в каждом из двух возможных случаев следующим образом:

1) случай w-расшифрования —

$$E(x, k) = E(x_1 x_2 \ldots x_l, k[q(1), g, f]) = y_1 y_2 \ldots y_l = y,$$
$$\text{где } \; y = x + z, \; z = z_1 z_2 \ldots z_l, \; z_t = f(g^{t-1}(q(1))), \; t = 1, 2, \ldots, l;$$
$$h(k, w) = h(k[q(1), g, f], (v, \eta)_l) = k[q(1), g, f_1], \text{ где } \; f_1 = f - \delta_{w,q(1),l};$$
$$D(y, k[q(1), g, f_1]) = D(y_1 y_2 \ldots y_l, k[q(1), g, f_1]) = x'_1 x'_2 \ldots x'_l = x',$$
$$\text{где } \; x' = y - z', \; z' = z'_1 z'_2 \ldots z'_l, \; z'_t = f_1(g^{t-1}(q(1))), \; t = 1, 2, \ldots, l;$$

2) случай w-зашифрования —

$$h(k, w) = h(k[q(1), g, f], (v, \eta)_l) = k[q(1), g, f_2], \text{ где } \; f_2 = f + \delta_{w,q(1),l};$$
$$E(x, h(k, w)) = E(x_1 x_2 \ldots x_l, k[q(1), g, f_2]) = y_1 y_2 \ldots y_l = y,$$
$$\text{где } \; y = x + z', \; z' = z'_1 z'_2 \ldots z'_l, \; z'_t = f_2(g^{t-1}(q(1))), \; t = 1, 2, \ldots, l;$$
$$D(y, k) = D(y_1 y_2 \ldots y_l, k[q(1), g, f]) = x'_1 x'_2 \ldots x'_l = x',$$
$$\text{где } \; x' = y - z, \; z = z_1 z_2 \ldots z_l, \; z_t = f(g^{t-1}(q(1))), \; t = 1, 2, \ldots, l.$$

В обоих случаях непосредственно проверяется, что $x' = x + w$. Кроме того, в первом случае $k_e = k[q(1), g, f]$ и $k_d = k[q(1), g, f_1]$, во втором случае $k_e = k[q(1), g, f_2]$ и $k_d = k[q(1), g, f]$.

Наконец, опишем шифр с водяными знаками $C_R = (X, K, W, h, E, D)$, являющийся конкретизацией w-шифра C_A, в которой автомат $A = (Q, Z, g, f)$ представляет собой нелинейный фильтрующий генератор ключевого потока [2], построенный из регистра сдвига с линейной обратной связью (LFSR) R некоторой длины n с примитивным характеристическим полиномом $c_0 + c_1 u + \ldots + c_{n-1} u^{n-1} - u^n$ в $\mathbb{Z}_2[u]$ и нелинейной булевой фильтрующей функцией f от n переменных. Таким образом, $F = \mathbb{Z}_2$, $X = \mathbb{Z}_2^*$, в любом $w = (v, \eta) \in W$ строка v есть вектор $11\ldots1$, так что $w = \eta = i_1 i_2 \ldots i_m$, $Q = \mathbb{Z}_2^n$, $Z = \mathbb{Z}_2$ и для любого $s = s_0 s_1 \ldots s_{n-1} \in Q$ имеет место $g(s) = s_1 \ldots s_{n-1} s_n$, где $s_n = c_0 s_0 + c_1 s_1 + \ldots + c_{n-1} s_{n-1}$.

Поскольку в $\mathbb{Z}_2$ операции сложения и вычитания совпадают со сложением по mod 2 и сложение с 1 означает инверсию, следующие соотношения верны в C_R: 1) если $q(1) \neq \neq 00\ldots0$ и $l \leqslant 2^n - 1$, то $\delta_{w,q(1),l}(s) = \sum\limits_{j=1}^{m} s^{q(i_j)}$, где для $\sigma = \sigma_0 \sigma_1 \ldots \sigma_{n-1} \in \mathbb{Z}_2^n$ справедливо: $s^\sigma = s_0^{\sigma_0} \wedge s_1^{\sigma_1} \wedge \ldots \wedge s_{n-1}^{\sigma_{n-1}}$, $s_t^{\sigma_t} = \neg s_t$, если $\sigma_t = 0$, и $s_t^{\sigma_t} = s_t$, если $\sigma_t = 1$, $t = 0, 1, \ldots, n-1$; 2) $f_1 = f_2$; 3) алгоритмы зашифрования и расшифрования в случае w-зашифрования являются алгоритмами соответственно расшифрования и зашифрования в случае w-расшифрования.

w-Шифр C_R со встраиванием водяного знака в процессе расшифрования реализован и протестирован на MPEG-видеоданных. Информацию об этом см. в [5, 6].

ЛИТЕРАТУРА

1. *Stinson D. R.* Cryptography. Theory and Practice. CRC Press, 1995. 434 p.
2. *Menezes A., van Oorshot P., and Vanstone S.* Handbook of Applied Cryptography. CRC Press, 1997. 662 p.
3. *Langelaar G. C.* Real-time Watermarking Techniques for Compressed Video Data. Delft: Delft University of Technology, 2000. 155 p.
4. *Mistry D.* Comparison of digital water marking methods // Intern. J. Comp. Sci. Engin. 2010. V. 2. No. 9. P. 2905–2909.
5. *Анжин В. А.* Метод защиты от нелегального копирования в цифровых видеотрансляциях через внедрение водяных знаков при расшифровании // Прикладная дискретная математика. Приложение. 2014. №. 7. С. 73–74.
6. `https://github.com/anjin-viktor/mpeg2decwtrk/` — Method implementation for MPEG2 Video. 2014.

УДК 004.056.55 DOI 10.17223/2226308X/8/21

ПОСТРОЕНИЕ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ[1]

В. В. Егорова, Д. К. Чечулина

Работа посвящена изучению практической применимости схемы полностью гомоморфного шифрования, созданной в Лаборатории современных компьютерных технологий НИЧ НГУ. Рассмотрено приложение гомоморфного шифрования для построения криптосистемы с открытым ключом, основанной на алгоритме RSA. На примере этой криптосистемы продемонстрирована корректность выполнения арифметических операций над зашифрованными данными, а также отсутствие увеличения размерности зашифрованных сообщений при умножении.

Ключевые слова: *гомоморфное шифрование, криптосистема с открытым ключом, алгоритм RSA.*

В Лаборатории современных компьютерных технологий НИЧ НГУ в рамках проекта «Защищённая база данных» разработана и реализована схема полностью гомоморфного шифрования, позволяющая выполнять операции сложения и умножения над зашифрованными данными. Рассмотрим подробнее эту схему. Пусть требуется шифровать целые числа размера t бит. Для этого необходимо выбрать целое число — модуль m, по которому будут производиться все вычисления в схеме. Модуль является частью секретного ключа. Для того чтобы однозначно восстановить любое зашифрованное число, модуль должен удовлетворять условию $2^t < m$.

Кроме того, для шифрования требуется секретный вектор $k \in \mathbb{Z}^n$, который строится следующим образом. Сгенерируем матрицу W размера $n \times n$, обратимую по модулю m, а также вектор $u \in \mathbb{Z}^n$, компоненты которого по модулю не превосходят m. Вектор k определим как решение системы линейных уравнений

$$(W \cdot k) \bmod m = u,$$

которая всегда разрешима, так как матрица W обратима по модулю m. Таким образом, $k = (W^{-1} \cdot u) \bmod m$. Матрица W и вектор u также являются частью секретного ключа.

Перейдём к описанию алгоритма шифрования. Пусть $p < 2^t < m$ — целое число,

[1]Работа поддержана грантом Минобрнауки РФ, договор № 02.G25.31.0054.

которое требуется зашифровать. Алгоритм гомоморфного шифрования заключается в построении такого вектора $c \in \mathbb{Z}^n$, что

$$(c, k) \bmod m = p. \tag{1}$$

Заметим, что в процессе построения вектора k сформирован набор векторов w_i (строк матрицы W), $i = 1, \ldots, n$, таких, что $(w_i, k) \bmod m = u_i$.

Выберем из этого набора любые s, $s \in \{2, \ldots, n\}$, векторов $w_1, \ldots, w_s$, которые будем использовать для шифрования. Тогда вектор c, являющийся шифртекстом, будем строить как линейную комбинацию этих векторов:

$$c = \sum_{i=1}^{s} \alpha_i \cdot w_i.$$

Коэффициенты α_i найдём из диофантова уравнения

$$u_1\alpha_1 + \ldots + u_s\alpha_s = p.$$

Для того чтобы данное уравнение было разрешимо, необходимо существование как минимум двух взаимно простых компонент вектора u. Сформированный таким образом шифртекст c однозначно расшифровывается согласно формуле (1):

$$(c, k) \bmod m = \left(\sum_{i=1}^{s} \alpha_i w_i, k\right) \bmod m = \sum_{i=1}^{s} \alpha_i (w_i, k) \bmod m = \sum_{i=1}^{s} \alpha_i u_i \bmod m = p.$$

Описанная схема шифрования является гомоморфной по сложению и умножению в силу свойств скалярного произведения и модулярной арифметики [1]. Рассмотрим подробнее операцию умножения. Найдём шифртекст для произведения чисел p_1 и p_2, которым соответствуют шифротексты a и b:

$$\begin{gathered} p_1 \cdot p_2 (\bmod\ m) = (a, k)(b, k) = (a_1k_1 + \ldots + a_nk_n)(b_1k_1 + \ldots + b_nk_n) = \\ = a_1b_1k_1k_1 + a_1b_2k_1k_2 + \ldots + a_nb_{n-1}k_nk_{n-1} + a_nb_nk_nk_n = \\ = (a_1b_1, a_1b_2, \ldots, a_nb_{n-1}, a_nb_n)(k_1k_1, k_1k_2, \ldots, k_nk_{n-1}, k_nk_n). \end{gathered}$$

Таким образом, в результате умножения двух шифртекстов длины n получается шифртекст длины n^2:

$$c = a \cdot b = (a_1b_1, a_1b_2, \ldots, a_nb_{n-1}, a_nb_n) \in \mathbb{Z}^{n^2}.$$

Для решения этой проблемы предлагается использовать специальную таблицу умножения — матрицу (γ_{ijk}). С её помощью компоненты вектора $c = (c_1, \ldots, c_n)$ — результата произведения двух шифртекстов — вычисляются следующим образом:

$$c_k = \sum_i \sum_j \gamma_{ijk} \cdot a_i \cdot b_j, \ k = 1, \ldots, n.$$

Если таблица умножения несимметрична, то для операции умножения шифртекстов не выполняются свойства коммутативности и ассоциативности. За счёт этого гомоморфное шифрование является недетерминированным. Таблица умножения не является секретной и предъявляется в открытом виде недоверенной стороне, на которой выполняются вычисления над зашифрованными данными.

Далее рассмотрим применение гомоморфного шифрования для построения криптосистемы с открытым ключом, с помощью которой проверяется корректность вычисления полиномиальных функций над зашифрованными данными.

Описываемая криптосистема формируется на основе некоторого аналога известного алгоритма RSA [2], в котором модуль объявляется секретом. К сожалению, такая криптосистема является нестойкой, однако её можно модифицировать за счёт использования гомоморфного шифрования. Таким образом, предлагается возводить в степень предварительно зашифрованное исходное число.

Секретным ключом назовем модуль m и вектор k, которые используются в гомоморфном шифровании. В качестве открытого ключа возьмем векторы w_1, w_2 и соответствующие им взаимно простые числа u_1, u_2: $(w_i, k) \bmod m = u_i$, $i = 1, 2$, и, кроме того, выберем целое число e, обратимое по модулю $\phi(m)$, где $\phi(x)$ — функция Эйлера. В открытом ключе хранится также таблица умножения (γ_{ijk}).

Предположим, что требуется зашифровать целое число $p < 2^t < m$. Для этого сначала применим к p алгоритм гомоморфного шифрования, в результате чего получим шифртекст c. Затем подействуем на вектор c полиномиальной функцией $F(x) = x^e$:

$$F(c) = c^e = z.$$

Обратим внимание на то, что функцию F можно вычислять различными способами. Так как операция умножения шифртекстов не коммутативна и не ассоциативна, результат возведения шифртекста c в степень e определяется расстановкой скобок при выполнении умножения, например, $c{\cdot}(c{\cdot}\ldots{\cdot}c) \neq (c{\cdot}\ldots{\cdot}c){\cdot}c$. Благодаря этому алгоритм шифрования является недетерминированным.

При расшифровании необходимо сначала найти скалярное произведение (z, k) по модулю m:

$$(z, k) \bmod m = (c^e, k) \bmod m = p^e \bmod m.$$

Кроме этого, отметим, что так как вектор c получен с помощью гомоморфного шифрования, вычисление функции $F(c)$ эквивалентно вычислению функции $F(p)$. Далее для восстановления исходного числа, аналогично алгоритму RSA, результат скалярного произведения $(z, k) \bmod m$ возводится в степень $d = e^{-1} \bmod \phi(m)$:

$$(p^e \bmod m)^d = p^{ed} \bmod m = p.$$

Приведённую криптосистему с открытым ключом можно модифицировать за счёт использования более сложных полиномиальных функций, функций от нескольких переменных или за счёт операции замены переменных.

Помимо рассмотренной криптосистемы, исследована криптосистема с открытым ключом, построенная на основе шифра Хилла с использованием гомоморфного шифрования. Однако такая система сводится к описанной выше, если заменить линейное преобразование на полиномиальное и применить предложенные модификации. Поэтому в работе описан только полиномиальный вариант, который является более общим.

ЛИТЕРАТУРА

1. *Knuth D.* The Art of Computer Programming. V. 2. Seminumerical Algorithms. Addison-Wesley Pub. Co., 1981.
2. *Shamir A.* A polynomial time algorithm for breaking the basic Merkle — Hellman cryptosystem // Adv. Cryptology. 1983. P. 279–288.

УДК 519.7 DOI 10.17223/2226308X/8/22

СЛОЖЕНИЕ ПО МОДУЛЮ 2^n В БЛОЧНОМ ШИФРОВАНИИ

А. М. Карондеев

Произведён анализ криптографических свойств операции сложения по модулю 2^n. Предложены линейные и нелинейные аппроксимации данной операции, а также изучены особенности их использования при проведении криптоанализа. Приведены примеры использования аппроксимаций сложения по модулю 2^n для проведения атак с известным открытым текстом на шифры, в которых операция смешения с ключом реализована как операция сложения по модулю 2^n. Показано, что замена операции сложения по модулю 2 на сложение по модулю 2^n приводит к увеличению стойкости блочных шифров.

Ключевые слова: *сложение по модулю 2^n, блочные шифры, криптоанализ.*

Составной частью любого блочного шифра является процедура смешения с ключом. Обычно данная процедура представляет собой сложение по модулю 2 (XOR) промежуточного информационного блока с раундовым ключом (как в алгоритмах DES, AES и др.), однако ничто не мешает использовать любую другую операцию, например сложение по модулю 2^n (как в алгоритме ГОСТ 28147-89). С учётом современной элементной базы и структуры большинства блочных шифров замена операции XOR на сложение по модулю 2^n не приведёт к существенному возрастанию сложности как программной, так и аппаратной реализации шифра. Работа посвящена анализу стойкости алгоритмов блочного шифрования, в которых операция смешения с ключом реализована как операция сложения по модулю 2^n.

Произведён анализ криптографических свойств операции $A + B = D \bmod 2^n$, где $A = (a_{n-1}, \ldots, a_0)$, $B = (b_{n-1}, \ldots, b_0)$, $D = (d_{n-1}, \ldots, d_0)$. В частности, рассмотрены линейные и нелинейные аппроксимации для выходных битов d_i и доказано, что для любого $i > 0$ функции $a_i \oplus b_i \oplus a_{i-1}$ и $a_i \oplus b_i \oplus b_{i-1}$ являются наилучшими линейными аппроксимациями для d_i, а именно: если a_j, b_j, $j = 0, \ldots, n-1$, являются независимыми случайными величинами, принимающими все свои значения с равной вероятностью, то линейные соотношения

$$d_i = a_i \oplus b_i \oplus a_{i-1}, \tag{1}$$

$$d_i = a_i \oplus b_i \oplus b_{i-1} \tag{2}$$

выполняются с вероятностью 0,75.

Рассмотрим особенности использования данных линейных аппроксимаций при проведении линейного криптоанализа блочных шифров, в которых для смешения с ключом используется операция $Y = X + K \bmod 2^n$. При проведении линейного криптоанализа [1] считается, что ключ фиксирован и аналитик располагает некоторым количеством пар открытый текст/шифртекст (материалом), полученных на этом ключе. Показано, что при фиксированном ключе вероятность выполнения соотношений (1), (2) может сильно отличаться от 0,75, а именно она колеблется в интервале от 0,5 до 1, причём границы достижимы. Таким образом, если при проведении линейного криптоанализа использовать аппроксимации (1), (2) для конкретного ключа, вероятность их выполнения может оказаться равной 0,5, и анализ будет невозможен.

Предложено новое решение — нелинейные соотношения, выполняющиеся с преобладанием не меньше 0,25 для любого фиксированного ключа. Точнее, доказано:

$$\forall i > 0\ \forall K\ \exists z\ (\mathbf{P}\{y_i = x_i \oplus z x_{i-1}\} = 1/2 + \varepsilon,\ |\varepsilon| \geqslant 1/4; \tag{3}$$

$$\forall i > 0\ \forall K\ \exists z\ (\mathbf{P}\{y_i \oplus y_{i-1} = x_i \oplus z x_{i-1}\} = 1/2 + \varepsilon,\ |\varepsilon| \geqslant 1/4. \tag{4}$$

Изучена возможность применения соотношений (3), (4) для анализа блочных шифров, использующих операцию $+ \bmod 2^n$. Предложена модификация линейного метода криптоанализа, которая в ряде случаев позволяет провести более эффективные атаки.

В частности, аппроксимации (3), (4) использованы для проведения атаки с известным открытым текстом на конкретный шифр, имеющий структуру SP-сети, в котором для смешения с ключом используется операция $+ \bmod 2^n$. Эта атака позволяет восстановить ключ быстрее полного перебора, что подтверждено моделированием на ЭВМ. Далее был проанализирован шифр, имеющий аналогичное строение, но использующий для смешения с ключом операцию XOR. Сравнительный анализ показал, что замена операции XOR на $+ \bmod 2^n$ приводит к существенному увеличению стойкости шифра. При проведении атаки на шифр, использующий $+ \bmod 2^n$ вместо XOR, помимо S-блоков необходимо аппроксимировать блок смешения с ключом, поэтому в большинстве случаев абсолютная величина преобладания итогового соотношения, связывающего некоторые биты открытого текста, шифртекста и ключа, становится гораздо ниже, из-за чего для проведения атаки требуется существенно больше материала.

Проведена атака с известным открытым текстом на алгоритм ГОСТ 28147-89 с сокращённым числом раундов и S-блоками специального вида. В [2] доказана стойкость алгоритма ГОСТ 28147-89 с не менее чем пятью раундами шифрования относительно линейного метода криптоанализа. Предложенный метод позволил провести атаку на алгоритм ГОСТ 28147-89 с восемью раундами шифрования.

ЛИТЕРАТУРА

1. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1993. V. 765. P. 386–397.
2. *Shorin V. V., Jelezniakov V. V., and Gabidulin E. M.* Linear and differential cryptanalysis of Russian GOST // Proc. Int. Workshop Coding and Cryptography (Paris, France, January 8–12, 2001). P. 467–476.

УДК 519.723 DOI 10.17223/2226308X/8/23

НЕЭНДОМОРФНЫЕ СОВЕРШЕННЫЕ ШИФРЫ С ДВУМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Исследуются неэндоморфные совершенные по Шеннону (абсолютно стойкие к атаке по шифртексту) шифры в случае, когда мощность множества шифрвеличин равна двум. В терминах линейной алгебры на основе теоремы Биркгофа о классификации дважды стохастических матриц описаны матрицы вероятностей ключей данных шифров. Построено множество возможных значений априорных вероятностей шифробозначений совершенного шифра.

Ключевые слова: *совершенные шифры, неэндоморфные шифры, максимальные шифры, дважды стохастические матрицы.*

Впервые вероятностная модель шифра рассмотрена в фундаментальной работе К. Шеннона [1]. Пусть X, Y — конечные множества соответственно шифрвеличин и

шифробозначений, с которыми оперирует некоторый шифр замены, K — множество ключей, причём $|X| = \lambda$, $|Y| = \mu$, $|K| = \pi$, где $\mu \geqslant \lambda > 1$. Согласно [2, 3], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и расшифрования с заданными распределениями вероятностей на множествах ℓ-грамм открытых текстов, шифрованных текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*. Изучение неэндоморфных ($|X| < |Y|$) совершенных шифров в общем виде предполагает знание распределения вероятностей на множестве ℓ-грамм алфавита открытых текстов. В качестве стандартного аппарата исследования распределения вероятностей на ℓ-граммах используются дважды стохастические матрицы [4]. Шифры, содержащие все инъекции из X в Y, называются *максимальными*. В [5] показано, что неминимальный ($|K| > |Y|$) совершенный шифр вкладывается в максимальный совершенный шифр.

Данная работа является продолжением [5]. Здесь описаны матрицы вероятностей ключей неэндоморфных совершенных шифров и множества вероятностей шифробозначений в случае, когда мощность множества шифрвеличин равна двум.

Рассмотрим неэндоморфный максимальный совершенный шифр в случае, когда мощность множества шифрвеличин равна двум. Пусть $X = \{x_1, x_2\}$; $Y = \{y_1, y_2, \ldots, y_\mu\} = \{1, 2, \ldots, \mu\}$; $K = \{k_1, k_2, \ldots, k_\pi\}$. Здесь $|X| = \lambda = 2$, $|Y| = \mu \geqslant 2$, $|K| = \pi = \mu(\mu - 1)$.

Зашифрование открытого текста $x = x_{i_1} x_{i_2} \ldots x_{i_\ell}$, где $x_{i_j} \in X$, т. е. $i_j \in \{1, 2\}$, заключается в замене каждой шифрвеличины x_{i_j} некоторым шифробозначением y_{i_j} в соответствии со случайно выбранным одним из $|K| = A_{|Y|}^{|X|} = A_\mu^2 = \mu!/(\mu - 2)! = \mu(\mu-1) = \pi$ всех инъективных отображений $e_k : X \to Y$, индексированных ключами $k \in K$. Инъективное отображение e_k, $k \in K$, при котором $e_k(x_1) = y_s = s$ и $e_k(x_2) = y_t = t$, будем также обозначать e_{st}, где $s, t = 1, \ldots, \mu$.

Пусть P_{st} — вероятность того, что при зашифровании шифрвеличины x_{i_j}, $i_j \in \{1, 2\}$, будет выбрано инъективное отображение e_{st}: $P_{st} = \mathbf{P}\{e_{st}(x_1) = s \,\&\, e_{st}(x_2) = t\}$, где $s \neq t$. Если $s = t$, то, в силу инъективности, $P_{st} = 0$.

Обозначим через $P = ||P_{st}||_{s,t=1}^{\mu}$ квадратную матрицу порядка μ, такую, что

$$\forall s \ \left(\sum_{t=1}^{\mu} P_{st} = p_s\right), \ \forall t \ \left(\sum_{s=1}^{\mu} P_{st} = p_t\right), \ p_1 + \ldots + p_\mu = 1. \tag{1}$$

Отметим, что, как указано в [3], совершенный по Шеннону шифр является сильно совершенным, т. е. не зависит от распределения на множестве шифрвеличин. Поэтому распределения вероятностей на множестве шифробозначений, индуцированные априорными распределениями вероятностей на множестве ключей, будем называть априорными.

Требуется описать множество возможных значений априорных вероятностей шифробозначений $p_s = \mathbf{P}\{y = s\}$, $s = 1, \ldots, \mu$, и найти общий вид матрицы P, удовлетворяющей условию (1) совершенности шифра, в зависимости от значений вероятностей p_s. Согласно подходу [2, 3], для вероятностной модели Σ_B шифра это достаточно сделать при $\ell = 1$. Для решения поставленной задачи будем использовать критерий совершенности шифра (2.2.4) из [3], который равносилен условию (1).

В частности, в примере 2.2.10 из [3] $X = \{x_1, x_2\}$, $Y = \{y_1, y_2, y_3\} = \{1, 2, 3\}$, $K = \{k_1, k_2, \ldots, k_6\}$, т. е. при $\lambda = 2$, $\mu = 3$, $\pi = 6$ таблица зашифрования имеет следующий вид:

$K\backslash X$	x_1	x_2	$P_{st} = \mathbf{P}\{e_{st}(x_1) = s \ \& \ e_{st}(x_2) = t\}$
k_1	1	2	$P_{12} = \mathbf{P}\{k = k_1\} = 19/80$
k_2	1	3	$P_{13} = \mathbf{P}\{k = k_2\} = 3/20$
k_3	2	1	$P_{21} = \mathbf{P}\{k = k_3\} = 21/80$
k_4	2	3	$P_{23} = \mathbf{P}\{k = k_4\} = 1/10$
k_5	3	1	$P_{31} = \mathbf{P}\{k = k_5\} = 1/8$
k_6	3	2	$P_{32} = \mathbf{P}\{k = k_6\} = 1/8$

При этом выполняются равенства:

$$p_1 = \mathbf{P}\{y = 1|x = x_1\} = P_{12} + P_{13} = 31/80; \quad p_1 = \mathbf{P}\{y = 1|x = x_2\} = P_{21} + P_{31} = 31/80;$$
$$p_2 = \mathbf{P}\{y = 2|x = x_1\} = P_{21} + P_{23} = 29/80; \quad p_2 = \mathbf{P}\{y = 2|x = x_2\} = P_{12} + P_{32} = 29/80;$$
$$p_3 = \mathbf{P}\{y = 3|x = x_1\} = P_{31} + P_{32} = 1/4; \qquad p_3 = \mathbf{P}\{y = 3|x = x_2\} = P_{13} + P_{23} = 1/4,$$

т. е. априорные и апостериорные (условные) вероятности шифробозначений y_i, $i = 1, 2, 3$, равны. Это, согласно критерию (2.2.4) из [3], означает, что матрица

$$P = ||P_{st}||_{s,t=1}^{3} = \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix} = \begin{pmatrix} 0 & 19/80 & 3/20 \\ 21/80 & 0 & 1/10 \\ 1/8 & 1/8 & 0 \end{pmatrix}$$

удовлетворяет условию (1) совершенности шифра.

Для матрицы P с неотрицательными элементами, удовлетворяющей условию (1), в силу теоремы Биркгофа [4] справедливы равенства

$$P = \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ Z\neq\varnothing}} \rho_Z P_Z, \qquad \sum_{\substack{Z\subset\{1,2,\ldots,\mu\},\\ Z\neq\varnothing}} \rho_Z = 1, \tag{2}$$

где Z — непустое множество номеров строк и столбцов; $\rho_Z \geqslant 0$ и P_Z — главные подматрицы равновероятных распределений.

Теорема 1. Матрица P с неотрицательными элементами, удовлетворяющая условию (1), лежит в выпуклой оболочке главных подматриц P_Z равновероятных распределений и определяется формулой (2).

При $\lambda = 2$ и $\mu = 3$ матрица P в общем случае определяется формулой

$$P = \frac{a}{3}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \frac{b}{3}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + \frac{c}{2}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} +$$
$$+\frac{d}{2}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} + \frac{e}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a/3 + c/2c & b/3 + d/2 \\ b/3 + c/2 & 0 & a/3 + e/2 \\ a/3 + d/2 & b/3 + e/2 & 0 \end{pmatrix},$$

где $a, b, c, d, e \geqslant 0$ — произвольные параметры, такие, что $a + b + c + d + e = 1$.

Отметим, что для любых $a, e \geqslant 0$, где $2a + 3e = 3/5$, и однозначно по ним определённым параметрам $b = a + 3/40$, $c = e + 11/40$, $d = e + 1/20$, получаются числовые значения примера 2.2.10 из [3]. В частности, они получаются при крайних значениях параметров: $a = 0$, $e = 1/5$ и $a = 3/10$, $e = 0$.

Теорема 2. Набор чисел $p_1, \ldots, p_\mu$ при $\mu \geqslant 2$ может быть набором априорных вероятностей шифробозначений совершенного шифра в модели Σ_B с мощностью множества шифрвеличин, равной двум, тогда и только тогда, когда эти числа удовлетворяют условиям

$$p_1 + \ldots + p_\mu = 1, \quad 0 \leqslant p_i \leqslant \frac{1}{2} \quad (i = 1, \ldots, \mu).$$

Таким образом, описаны матрицы вероятностей ключей неэндоморфных совершенных шифров и множества вероятностей шифробозначений в случае, когда мощность множества шифрвеличин равна двум. Отметим, что при $\lambda > 2$ эта задача сильно усложняется ввиду отсутствия аналога теоремы Биркгофа о дважды стохастических матрицах.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Birkhoff G. D.* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.
5. *Медведева Н. В., Титов С. С.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.

УДК 519.7 DOI 10.17223/2226308X/8/24

ПРЕДВАРИТЕЛЬНАЯ ОЦЕНКА МИНИМАЛЬНОГО ЧИСЛА РАУНДОВ ЛЕГКОВЕСНЫХ ШИФРОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИХ УДОВЛЕТВОРИТЕЛЬНЫХ СТАТИСТИЧЕСКИХ СВОЙСТВ[1]

А. И. Пестунов

Для новых легковесных блочных шифров (и нескольких известных шифров) проведена экспериментальная оценка минимального числа раундов, при котором в режиме CTR эти шифры обеспечивают удовлетворительные статистические свойства выходной псевдослучайной последовательности. Эксперименты проводились с помощью статистического теста «стопка книг» при длине выборки 2^{26} байт. В зависимости от шифра блоки представлялись в виде двух, трёх или четырёх 32-битовых слов и в качестве элементов тестируемой выборки брались первые слова каждого выходного блока. На вход шифра подавались блоки, где все слова, кроме второго, равны нулю, а второе слово менялось от 0 до $2^{24} - 1$.

Ключевые слова: *блочный шифр, легковесный шифр, статистический анализ, статистический тест, число раундов, псевдослучайные числа.*

Одно из применений итеративных блочных шифров — это генерация псевдослучайных чисел. Для этой цели часто используется режим CTR, подразумевающий последовательное шифрование значений некоторого счётчика и формирование псевдослучайной последовательности из выходных блоков или их частей. При этом удовлетворительные статистические свойства выходной последовательности могут быть обеспечены значительно меньшим числом раундов (обозначим его $R_{\min}$), чем полное число раундов шифра (обозначим его R). Очевидно, что сокращение числа раундов увеличит производительность шифров и позволит генерировать псевдослучайные числа быстрее. Причём даже если такой усечённый шифр имеет высоковероятные характеристики (линейные, дифференциальные, интегральные и пр.), он сможет генерировать псевдослучайные последовательности с удовлетворительными статистическими свой-

[1]Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол_а).

ствами в силу того, что вероятность появления блоков с требуемыми на входе шифра свойствами может быть ничтожно малой.

Поскольку блочные шифры претендуют на универсальность, решая целый спектр прикладных задач (генерация псевдослучайных чисел является одной из них), то при создании новых шифров помимо R, возможно, имеет смысл указывать и $R_{\min}$, обеспечивающее удовлетворительные статистические свойства, не гарантируя криптографической стойкости. Уже сейчас при варьировании длины ключа задаётся различное число раундов у шифров, например AES, CLEFIA, Piccolo, SIMON или SPECK. В частности, для шифра AES предполагается, что 10 раундов должны обеспечивать отсутствие атак быстрее 2^{128}, 12 раундов — быстрее 2^{192}, а 14 раундов — быстрее 2^{256}.

В работе приводятся результаты статистического анализа легковесных итеративных блочных шифров (и нескольких известных), цель которого — осуществить предварительную оценку $R_{\min}$. Значительная часть реализаций шифров взята из библиотеки BLOC [1, 2].

Исследование проводилось при помощи статистического теста «стопка книг» [3, 4], который ранее уже применялся для анализа других блочных шифров [5 – 7]. Данный тест подразумевает вычисление статистики x^2, подчиняющейся распределению хи-квадрат, если элементы выборки равномерно распределены. Число степеней свободы в распределении хи-квадрат определяется параметром теста — количеством частей в структуре данных «стопка книг». В настоящей работе этот параметр равен 2, а число степеней свободы — 1.

При тестировании для каждого шифра варьировалось число раундов: 1, 2, 3 и т. д. Для каждого раунда генерировалось по 10 выборок (на 10 случайных мастер-ключах) размера 2^{26} байт (2^{24} 32-битовых слов) и по каждой из них вычислялась статистика x^2. Выборки генерировались следующим образом: в зависимости от шифра блоки представлялись в виде двух, трёх или четырёх 32-битовых слов и в качестве элементов выборки использовались первые слова каждого выходного блока; на вход шифра подавались блоки, где все слова, кроме второго, равны нулю, а второе слово менялось от 0 до $2^{24}-1$. Значения статистики x^2 сравнивались с квантилью хи-квадрат уровня значимости 0,05 с одной степенью свободы. При этом для каждой серии из 10 таких выборок подсчитывалось число $U_{0,05}$, означающее количество превышений статистикой x^2 данной квантили (табл. 1).

Таблица 1

Символические обозначения

$U_{0,05}$	0–2	3–5	6–7	8–10
Обозначение	—	$\mp$	$\pm$	+

Поскольку статистические свойства шифра улучшаются с ростом числа раундов, то при определённом числе раундов распределение выборки не отличается от равномерного. Данное число (обозначим его через $\hat{R}_{\min}$) возьмём в качестве предварительной оценки для $R_{\min}$. Результаты экспериментов показали, что в среднем рассмотренные блочные шифры сохраняют удовлетворительные статистические свойства при сокращении числа раундов в них до 10–30 % от полного числа раундов (табл. 2 и 3).

Статистический анализ, результаты которого представлены здесь, является предварительным в том смысле, что он даёт минимальную границу $R_{\min}$. В частности, более тщательный подбор входной последовательности и использование других статистических тестов может «забраковать» большее число раундов.

Таблица 2

Блочные шифры, для которых отклонения от равномерного распределения фиксируются при более чем 13 раундах

Раунды	1–14	15	16	17	18–24	25	26–27	28–29	30	$R_{\min}$	R	%
Simon	+	∓	—	∓	—	—	—	—	—	18	32–72	25–56
Katan64	+	+	+	+	+	+	—	+	—	30	254	12
Ktantan64	+	+	+	+	+	+	—	+	—	30	254	12

Таблица 3

Блочные шифры, для которых отклонения от равномерного распределения фиксируются не более чем при 13 раундах

Раунды	1	2	3	4	5	6	7	8	9	10–13	14	$\hat{R}_{\min}$	R	%
XTEA	+	+	—	—	—	—	—	—	—	—	—	3	32	6
SPECK	+	+	+	+	+	—	—	—	—	—	—	6	22–34	15–23
CLEFIA	+	+	+	+	+	—	—	—	—	—	—	6	18–26	19–28
Piccolo	+	+	+	+	+	—	—	—	—	—	—	6	25–31	16–20
KLEIN	+	+	∓	—	—	—	—	—	—	—	—	4	12–20	10–17
mCrypton	+	+	+	—	∓	—	—	—	—	—	—	6	12	25
LED	+	+	+	—	—	—	—	—	—	—	—	4	32–48	6–10
Noekeon	±	—	—	—	—	—	—	—	—	—	—	2	16	6
MIBS	+	—	—	—	—	—	—	—	—	—	—	2	32	3
IDEA	+	—	—	—	—	—	—	—	—	—	—	2	8.5	12
AES	+	+	+	—	—	—	—	—	—	—	—	4	10–14	21–30
DESXL	+	—	—	—	—	—	—	—	—	—	—	2	8	25
Lblock	+	+	+	+	+	+	+	±	—	—	—	9	32	25
Present	+	+	+	+	+	+	+	±	—	—	—	9	31	26
Twine	+	+	+	+	+	+	+	+	—	—	—	9	36	22
Hight	+	+	+	+	+	+	+	+	+	—	—	10	32	28
Sea	+	+	+	+	+	+	+	+	+	—	—	10	51	18
Skipjack	+	+	+	+	+	+	+	+	+	+	—	14	32	34

Более детальный анализ с подробным описанием экспериментов планируется опубликовать в одной из последующих работ.

ЛИТЕРАТУРА

1. *Cazorla M., Marquet K., and Minier M.* Survey and benchmark of lightweight block ciphers for wireless sensor networks // Proc. 10th Intern. Conf. SECRYPT-2013, July 2013, Reykjavik, Iceland. P. 543–548.
2. *Cazorla M., Gourgeon S., Marquet K., and Minier M.* BLOC Library: Implementations of lightweight block ciphers on a WSN430 sensor [Электронный ресурс]. `http://bloc.project.citi-lab.fr/library.html/`
3. *Рябко Б. Я., Пестунов А. И.* «Стопка книг» как новый статистический тест для случайных чисел // Проблемы передачи информации. 2004. Т. 40. № 1. С. 73–78.
4. *Пестунов А. И.* Теоретическое исследование свойств статистического теста «стопка книг» // Вычислительные технологии. 2006. Т. 11. № 6. С. 96–103.
5. *Рябко Б. Я., Монарев В. А., Шокин Ю. И.* Новый тип атак на блоковые шифры // Проблемы передачи информации. 2005. Т. 41. № 4. С. 385–394.
6. *Пестунов А. И.* Статистический анализ современных блочных шифров // Вычислительные технологии. 2007. Т. 12. № 2. С. 122–129.
7. *Pestunov A.* Statistical analysis of the MARS block cipher // Cryptology ePrint Archive. 2006. Report No. 2006/217. `https://eprint.iacr.org/2006/217/`

УДК 519.7 DOI 10.17223/2226308X/8/25

$\otimes_{\mathbf{W},\mathrm{ch}}$-МАРКОВОСТЬ И ИМПРИМИТИВНОСТЬ В БЛОЧНЫХ ШИФРСИСТЕМАХ

Б. А. Погорелов, М. А. Пудовкина

Рассмотрена связь между $\otimes_{\mathbf{W},\mathrm{ch}}$-марковостью итеративных алгоритмов блочного шифрования и методом гомоморфизмов. Для алгоритмов блочного шифрования и разбиений $\mathbf{W}$ алфавита текстов X, блоки которых являются смежными классами по некоторой подгруппе абелевой регулярной группы $(X, \otimes)$, доказана эквивалентность между $\otimes_{\mathbf{W},\mathrm{ch}}$-марковостью алгоритма и существованием нетривиального гомоморфизма. Показано, что класс $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских преобразований не ограничивается только упомянутыми разбиениями. Так, для разбиений $\mathbf{W}$, блоки которых не являются смежными классами по подгруппе аддитивной группы $(V_n^+, \oplus)$ векторного пространства V_n, описаны классы аффинных и нелинейных $\oplus_{\mathbf{W},\mathrm{ch}}$-марковских преобразований. Приведены условия на разбиения $\mathbf{W}$ пространства V_n, при которых аффинное преобразование является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковским. Получено, что для каждого разбиения $\mathbf{W}$ пространства V_n множество всех $\oplus_{\mathbf{W},\mathrm{ch}}$-марковских преобразований из AGL_n является группой. Приведены примеры таких групп. Тем самым показано, что для данного класса разбиений $\otimes_{\mathbf{W},\mathrm{ch}}$-марковость является обобщением рассмотренных гомоморфизмов.

Ключевые слова: *импримитивная группа, метод гомоморфизмов, XSL-алгоритмы блочного шифрования, сплетение групп подстановок.*

Пусть $(X, \otimes)$ — произвольная регулярная абелева группа на конечном множестве X с бинарной операцией $\otimes$ и единичным элементом e; $X^\times = X \setminus \{e\}$; $S(X)$ — симметрическая группа на X; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; AGL_n — полная аффинная группа над V_n; G_α — стабилизатор элемента $\alpha \in V_n$; $G \leqslant S(V_n)$; AG — аффинная подгруппы группы AGL_n при $G \leqslant GL_n$ и $G = AG_{\mathbf{0}}$. Пусть также $IG_{\mathbf{W}} = (S_w \wr S_r, \mathbf{W})$ — максимальная группа подстановок на $X = W_0 \cup \ldots \cup W_{r-1}$, сохраняющая разбиение $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, где $w = |W_0| = \ldots = |W_{r-1}|$. Эта группа называется сплетением группы подстановок S_w группой S_r.

Рассмотрим l-раундовый алгоритм блочного шифрования, у которого раундовая функция $g : X^2 \to X$ задана условием $g_k : x \mapsto (x \otimes k)^b$, где $b \in S(X)$, $k \in X$. К данному классу относятся XSL-алгоритмы блочного шифрования. Предположим существование такого разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X, что g_k сохраняет $\mathbf{W}$-разбиение для каждого $k \in X$, и $e \in W_0$. Так как $b \in S(X)$, то W_j — j-й смежный класс группы $(X, \otimes)$ по её подгруппе W_0, $j = 0, \ldots, r-1$. Справедливы включения

$$b \in IG_{\mathbf{W}},\ \langle g_k | k \in X\rangle \leqslant IG_{\mathbf{W}},\ \left\langle g_{k^{(1)}} \ldots g_{k^{(l)}} | (k^{(1)}, \ldots, k^{(l)}) \in X^l \right\rangle \leqslant IG_{\mathbf{W}}.$$

Очевидно, что существует бинарная операция $\odot$ на $\{0, \ldots, r-1\}$, удовлетворяющая равенству $W_i \otimes W_j = W_{i \odot j}$ для каждых $i, j \in \{0, \ldots, r-1\}$, где $i \odot j$ — номер смежного класса, содержащего произвольный представитель $\beta \in W_i \otimes W_j$. Заметим, что

$$\varphi_{\mathbf{W}}(\alpha \otimes k) = \varphi_{\mathbf{W}}(\alpha) \odot \varphi_{\mathbf{W}}(k), (\alpha, k) \in X^2.$$

Рассмотрим такое отображение $\varphi_{\mathbf{W}} : X \to \{0, \ldots, r-1\}$, что $\varphi_{\mathbf{W}} : \alpha \mapsto i$ тогда и только тогда, когда $\alpha \in W_i$, $i \in \{0, \ldots, r-1\}$. Ясно, что отображение $\varphi_{\mathbf{W}}$ задаёт гомоморфизм l-раундового алгоритма блочного шифрования с раундовой функцией

$g : X^2 \to X$ в l-раундовый алгоритм блочного шифрования с раундовой функцией $\bar{g} : \{0, \ldots, r-1\}^2 \to \{0, \ldots, r-1\}$, где

$$\bar{g}_{\varphi_{\mathbf{W}}(k)}\left(\varphi_{\mathbf{W}}(\alpha)\right) = \varphi_{\mathbf{W}}\left((\alpha \otimes k)^b\right) = \left(\varphi_{\mathbf{W}}(\alpha \otimes k)\right)^{\bar{b}} = \left(\varphi_{\mathbf{W}}(\alpha) \odot \varphi_{\mathbf{W}}(k)\right)^{\bar{b}} \qquad (1)$$

для каждых $(\alpha, k) \in X^2$. Заметим, что подстановка $\bar{b} \in S\left(\{0, \ldots, r-1\}\right)$ есть гомоморфный образ подстановки b.

Доказано, что $\mathbf{p}_{\mathbf{W}}(g) = \mathbf{p}(\bar{g})$, где $\mathbf{p}(\bar{g}) = (p_{\varepsilon,\lambda}(\bar{g}))$ — матрица вероятностей переходов разностей функции $\bar{g}$; $\mathbf{p}_{\mathbf{W}}(g)$ — матрица вероятностей переходов блоков разностей разбиения $\mathbf{W}$ функции g.

Определения $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских алгоритмов блочного шифрования и $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских преобразований приведены в [1].

Теорема 1. Пусть $l \in \mathbb{N}$, $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ — разбиение множества X, $e \in W_0$, $W_0 < X$, W_j — j-й смежный класс группы $(X, \otimes)$ по её подгруппе W_0, $j = 0, \ldots, r-1$. Отображение $\varphi_{\mathbf{W}}$, определённое равенством (1), задаёт гомоморфизм l-раундового алгоритма блочного шифрования с раундовой функцией $g : X^2 \to X$, $g_k : x \mapsto (x \otimes k)^b$, в l-раундовый алгоритм блочного шифрования с раундовой функцией $\bar{g} : \{0, \ldots, r-1\}^2 \to \{0, \ldots, r-1\}$, $\bar{g}_\kappa : \beta \mapsto (\beta \odot \kappa)^{\bar{b}}$ тогда и только тогда, когда алгоритм блочного шифрования с раундовой функцией g является $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским.

Заметим, что теорема 1 устанавливает соответствие между $\otimes_{\mathbf{W},\mathrm{ch}}$-марковостью и существованием гомоморфизма $\varphi_{\mathbf{W}}$ только для таких разбиений $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, для которых W_j — j-й смежный класс группы $(X, \otimes)$ по её подгруппе W_0, $W_0 < X$. Однако класс $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских алгоритмов шифрования и преобразований не ограничивается только такими разбиениями. Так, в [1] приведены $+_{\mathbf{W},\mathrm{ch}}$-марковские преобразования для аддитивной группы кольца вычетов $\mathbb{Z}_{2^n}$ для разбиений, отличных от приведённых в теореме 1.

Опишем ещё классы $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских преобразований, не удовлетворяющих теореме 1. Для этого рассмотрим сначала классы $\otimes_{\mathbf{W},\mathrm{ch}}$-марковских аффинных преобразований для разбиений $\mathbf{W}$ $\mathbb{Z}_{2^m}$-модуля $\mathbb{Z}_{2^m}^d$.

Для $a \in \mathbb{Z}$ через $a_{(d)}$ обозначим такой наименьший элемент $a_{(d)} \in \{0, \ldots, d-1\}$, что $a_{(d)} \equiv a \pmod{d}$. Для $m, d \in \mathbb{N}$ и $\alpha = (\alpha_{d-1}, \ldots, \alpha_0) \in \mathbb{Z}_{2^m}^d$, $\beta = (\beta_{d-1}, \ldots, \beta_0) \in \mathbb{Z}_{2^m}^d$ положим

$$\alpha +_{2^m} \beta = \left((\alpha_{d-1} + \beta_{d-1})_{(2^m)}, \ldots, (\alpha_0 + \beta_0)_{(2^m)}\right),$$

т. е. $+_{2^m}$ — операция покоординатного сложения в $\mathbb{Z}_{2^m}$-модуле $\mathbb{Z}_{2^m}^d$. Ясно, что при $m = 1$ выполняются равенства $d = n$, $\oplus = +_2$ и $V_n = \mathbb{Z}_2^n$.

Утверждение 1. Пусть $n = md$, $m, d \in \mathbb{N}$. Аффинное преобразование $h \in AGL_d(\mathbb{Z}_{2^m})$, где $h = (h_0, \lambda)$; $h : \alpha \mapsto \alpha^{h_0} +_{2^m} \lambda$; $h_0 \in GL_d\left(\mathbb{Z}_{2^m}\right)$; $\lambda \in \mathbb{Z}_{2^m}^d$, является $+_{2^m}\mathbf{W},\mathrm{ch}$-марковским для разбиения $\mathbf{W}$ $\mathbb{Z}_{2^m}$-модуля $\mathbb{Z}_{2^m}^d$ тогда и только тогда, когда h_0 сохраняет $\mathbf{W}$.

Из утверждения 1 следует, что преобразование h может являться $\oplus_{\mathbf{W},\mathrm{ch}}$-марковским и для разбиений $\mathbf{W}$ пространства V_n, блоки которых не являются смежными классами по некоторой подгруппе аддитивной группы V_n^+ векторного пространства V_n.

Приведём примеры примитивных групп $(AGL_n)_{\mathbf{W}}$ и соответствующих разбиений $\mathbf{W}$. Пусть $\Delta_j^{(n)}$ — множество всех векторов веса Хемминга $j \in \{0, \ldots, n\}$ из V_n; $\tilde{S}_n$ — группа подстановочных $(n \times n)$-матриц; $A\tilde{S}_n$ — аффинная подгруппа группы AGL_n,

подобная группе экспоненцирования $S_2 \uparrow S_n$. Стабилизатор $G_{\mathbf{0}}$ каждой не 2-транзитивной примитивной группы G, $A\tilde{S}_n \leqslant G \leqslant AGL_n$, сохраняет некоторое нетривиальное разбиение множества $V_n^\times$, блоками которого являются орбиты стабилизатора $G_{\mathbf{0}}$ на $V_n^\times$. Все такие разбиения описаны в [2], а классификация соответствующих групп — в [3, 4]. С применением теоремы 1, утверждения 1 и классификации надгрупп группы $A\tilde{S}_n$ описаны классы нелинейных $\oplus_{\mathbf{W},\mathrm{ch}}$-марковских преобразований для разбиений $\mathbf{W}$ пространства V_n, отличных от рассмотренных в теореме 1.

Очевидно, что $AGL_n = (AGL_n)_{\mathbf{W}}$ для $\mathbf{W} \in \left\{\{\Delta_0^{(n)}, V_n^\times\}, \{\alpha : \alpha \in V_n\}\right\}$.

Утверждение 2. Если 2-транзитивная группа $G < AGL_n$ такова, что $G_{\mathbf{0}}$ примитивна на $V_n^\times$, то $G \neq (AGL_n)_{\mathbf{W}}$ для каждого разбиения $\mathbf{W} \notin \left\{\{\Delta_0^{(n)}, V_n^\times\}, \{\{\alpha\} : \alpha \in V_n\}\right\}$.

В общем случае из $\oplus_{\mathbf{W},\mathrm{ch}}$-марковости преобразований $b_1, b_2 \in S(V_n)$ для некоторого разбиения $\mathbf{W}$ пространства V_n не следует $\oplus_{\mathbf{W},\mathrm{ch}}$-марковость преобразования $b_1 b_2$. Приведены условия на преобразования b_1, b_2, из которых вытекает $\oplus_{\mathbf{W},\mathrm{ch}}$-марковость преобразования $b_1 b_2$, а также условия того, что раундовая функция, задаваемая этими преобразованиями, является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковской.

Пусть раундовая функция $g : V_n^2 \to V_n$ задана условием $g : (x, k) \mapsto (x \oplus k)^{sh}$, где $s = (s_{d-1}, \ldots, s_0) \in S(V_m)^d$, $h \in GL_n$. Приведены условия на h, при которых раундовая функция $g : (x, k) \mapsto (x \oplus k)^{sh}$ является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковской для некоторого разбиения $\mathbf{W}$ пространства V_n.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* $\otimes_{\mathbf{W},\mathrm{ch}}$-марковские преобразования // Прикладная дискретная математика. Приложение. 2015. № 8. С. 17–20.
2. *Музычук М. Е.* Подсхемы схемы Хемминга // Исследования по алгебраической теории комбинаторных объектов. ВНИИ системных исследований. Труды семинара. 1985. С. 49–76.
3. *Погорелов Б. А.* Подметрики метрики Хемминга и теорема А.А. Маркова // Труды по дискретной математике. 2006. № 9. С. 190–219.
4. *Погорелов Б. А., Пудовкина М. А.* Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз // Труды по дискретной математике. 2007. № 10. С. 202–238.

УДК 510.52 DOI 10.17223/2226308X/8/26

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ РАСПОЗНАВАНИЯ КВАДРАТИЧНЫХ ВЫЧЕТОВ[1]

А. Н. Рыбалов

Генерический подход к алгоритмическим проблемам предложен А. Мясниковым, И. Каповичем, П. Шуппом и В. Шпильрайном в 2003 г. В рамках этого подхода рассматривается поведение алгоритмов на множествах почти всех входов. В данной работе изучается генерическая сложность проблемы распознавания квадратичных вычетов в группах вычетов. Доказывается, что её естественная подпроблема генерически трудноразрешима (то есть трудна для почти всех входов) при условии, что проблема распознавания квадратичных вычетов трудноразрешима в классическом смысле.

[1]Работа поддержана грантом РФФИ № 15-41-04312.

Ключевые слова: *генерическая сложность, квадратичный вычет, вероятностный алгоритм.*

В работе [1] развита теория генерической сложности вычислений. В рамках этого подхода алгоритмическая проблема рассматривается не на всем множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют так называемое генерическое множество. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения практики алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов.

С точки зрения современной криптографии интересны такие алгоритмические проблемы, которые, являясь (гипотетически) трудными в классическом смысле, остаются трудными и в генерическом смысле, т. е. для почти всех входов. Это объясняется тем, что при случайной генерации ключей в криптографическом алгоритме происходит генерация входа некоторой трудной алгоритмической проблемы, лежащей в основе алгоритма. Если проблема является генерически легко разрешимой, то для почти всех таких входов её можно быстро решить, и ключи почти всегда будут нестойкими. Поэтому проблема должна быть генерически трудной. Например, для проблемы дискретного логарифма такие результаты получены в работе [2].

Данная работа посвящена изучению генерической сложности классической проблемы распознавания квадратичных вычетов в группах вычетов. До сих пор не известно полиномиальных алгоритмов её решения. Более того, на предположении о её трудноразрешимости основаны некоторые криптографические алгоритмы [3].

Пусть I — некоторое множество входов. На множестве I определена функция размера $\mathrm{size} : I \to \mathbb{N}$, сопоставляющая каждому элементу $a \in I$ его размер $\mathrm{size}(a)$. Допустим, что для любого n множество I_n элементов из I размера n конечно. Для любого подмножества $S \subseteq I$ определим следующую последовательность:

$$\rho_n(S) = \frac{|S \cap I_n|}{|I_n|},\ n = 1, 2, 3, \ldots$$

Величина $\rho_n(S)$ — это вероятность получить вход из множества S при случайной и равномерной генерации элементов из I_n. *Асимптотической плотностью* S назовём следующий предел (если он существует):

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S)=1$, и *пренебрежимым*, если $\rho(S)=0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо. Понятие генерического множества является некоторой формализацией интуитивного понятия множества «почти всех» элементов множества I в том смысле, что при увеличении размера элемента вероятность попасть в генерическое множество при случайной и равновероятной генерации элементов стремится к 1.

Алгоритмическая проблема распознования множества $S \subseteq I$ *генерически полиномиально разрешима*, если существует множество $G \subseteq I$, такое, что

1) G — генерическое;
2) G — разрешимое за полиномиальное время;
3) $G \cap S$ — разрешимое за полиномиальное время.

Генерический алгоритм, решающий проблему S, работает на входе $x \in I$ следующим образом. Сначала определяет, принадлежит ли x генерическому множеству G.

Если да, то проверяет принадлежность входа S. Если нет, то отвечает НЕ ЗНАЮ. Такой алгоритм правильно решает проблему S на почти всех входах.

Пусть $\mathbb{Z}/(m)$ — мультипликативная группа вычетов по модулю $m \in \mathbb{N}$. Напомним, что квадратичным вычетом в группе $\mathbb{Z}/(m)$ называется любой элемент x, для которого существует $y \in \mathbb{Z}/(m)$, такой, что $x = y^2$. В противном случае элемент x называется квадратичным невычетом. Под проблемой распознавания квадратичных вычетов понимается проблема распознавания следующего множества:

$$QR = \{(m, x) \in \mathbb{N}^2 : m = pq, \text{ где } p, q \text{ — простые числа,}$$
$$x - \text{ квадратичный вычет в } \mathbb{Z}/(m)\}.$$

В настоящее время неизвестно полиномиальных алгоритмов (в том числе и вероятностных), решающих проблему распознавания квадратичных вычетов для всех таких модулей m.

Для изучения генерической сложности этой проблемы необходимо провести некоторую стратификацию на множестве входов. Рассмотрим любую бесконечную последовательность натуральных чисел $\mu = \{m_1, m_2, \ldots\}$, удовлетворяющую следующим условиям:

1) $2^n < m_n < 2^{n+1}$ для любого n;
2) m_n — произведение двух различных простых чисел для любого $n > 1$.

Будем называть такую последовательность *экспоненциальной*. Из знаменитого постулата Бертрана, доказанного П. Л. Чебышевым, следует, что экспоненциальные последовательности существуют. Определим алгоритмическую проблему $QR(\mu)$ как ограничение проблемы распознавания квадратичных вычетов QR на следующее множество входных данных:

$$I = \{(m, x) : m \in \mu, x \in \mathbb{Z}/(m)\}.$$

Под размером входа (m, x) понимается количество бит в двоичной записи числа m минус 1. Заметим, что множество I_n входов проблемы $QR(\mu)$ размера n состоит из всех пар (m, x), где m — единственное число $m \in \mu$, удовлетворяющее условию $2^n < m < 2^{n+1}$, а x — любой элемент из $\mathbb{Z}/(m)$.

Теорема 1. Если проблема $QR(\mu)$ генерически полиномиально разрешима, то существует полиномиальный вероятностный алгоритм, решающий $QR(\mu)$ для всех входов.

Теорема 2. Если для проблемы QR не существует полиномиального вероятностного алгоритма, то существует экспоненциальная последовательность μ, такая, что проблема $QR(\mu)$ не является генерически полиномиально разрешимой.

Более подробно полученные результаты представлены в [4].

ЛИТЕРАТУРА

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
2. *Blum M. and Micali S.* How to generate cryptographically strong sequences of pseudorandom bits // SIAM J. Computing. 1984. V. 13. No. 4. P. 850–864.
3. *Мао В.* Современная криптография: теория и практика. М.: Вильямс, 2005. 768 с.
4. *Рыбалов А. Н.* О генерической сложности проблемы распознавания квадратичных вычетов // Прикладная дискретная математика. 2015. № 2. С. 54–58.

УДК 519.7 DOI 10.17223/2226308X/8/27

NSUCRYPTO — СТУДЕНЧЕСКАЯ ОЛИМПИАДА ПО КРИПТОГРАФИИ: ИДЕЯ, ВОПЛОЩЕНИЕ, РЕЗУЛЬТАТ[1]

Н. Н. Токарева

Кратко представлен опыт проведения первой международной студенческой олимпиады по криптографии NSUCRYPTO. Рассмотрены принципы её организации и математические задачи, предложенные участникам.

Ключевые слова: *NSUCRYPTO, олимпиада, криптография, булевы функции.*

Идея провести студенческую олимпиаду по криптографии появилась несколько лет назад в Новосибирске. К тому времени существовало несколько школьных олимпиад по криптографии и информационной безопасности, вызывающих большой интерес. В первую очередь среди них стоит отметить олимпиаду по математике и криптографии, успешно проводимую ИКСИ уже более 20 лет подряд. Но студенческой олимпиады по криптографии не было, в том числе и за рубежом. Новая олимпиада сразу задумывалась как международная, поэтому её официальным языком стал английский. Чтобы максимально расширить географию участников, было принято решение проводить её дистанционно, через интернет. Ещё одной ключевой идеей стала идея о том, что в целом задачи олимпиады должны быть сложными (не игровыми), а часть из них и вовсе нерешёнными. Вместе с коллегами мы не ставили перед собой задачу популяризации криптографии как таковой; нам хотелось привлечь внимание студентов и молодых исследователей к современным математическим вопросам криптографии, возбудить научный интерес к криптографии.

В 2014 г., заручившись активной поддержкой руководства мехмата НГУ и Института математики СО РАН, обсудив формат олимпиады с нашими коллегами-криптографами из Томского и Белорусского университетов, лаборатории COSIC университета г. Лёвена (Бельгия), мы занялись её организацией. В программный комитет олимпиады NSUCRYPTO-2014 вошли: Г. П. Агибалов (профессор, заведующий кафедрой защиты информации и криптографии ТГУ); С. В. Агиевич (заведующий НИЛ проблем безопасности информационных технологий НИИ прикладных проблем математики и информатики, БГУ); Н. А. Коломеец (н.с. ИМ СО РАН, преподаватель НГУ); И. А. Панкратова (доцент кафедры защиты информации и криптографии ТГУ); Н. Н. Токарева (с.н.с. ИМ СО РАН, доцент НГУ); S. Nikova (сотрудник лаборатории COSIC университета г. Лёвена); B. Preneel (профессор лаборатории COSIC университета г. Лёвена, президент Международной ассоциации криптографических исследований (IACR)), V. Rijmen (сотрудник лаборатории COSIC университета г. Лёвена, один из двух создателей шифра AES). Организационный комитет олимпиады представили преподаватели и студенты НГУ: В. А. Виткуп, А. А. Городилова, Г. И. Шушуев, Д. П. Покрасенко и С. Ю. Филюзин.

Олимпиада NSUCRYPTO-2014 состояла из двух независимых интернет-туров: индивидуального (школьная и студенческая секции) и командного. Для участия достаточно было зарегистрироваться на сайте `www.nsucrypto.nsu.ru`, при этом стать участником мог каждый. Было зарегистрировано более 450 участников из 12 стран — России, Австрии, Бельгии, Белоруссии, Болгарии, Германии, Дании, Индии, Италии, Ка-

[1]Работа поддержана Новосибирским государственным университетом, грантами РФФИ № 15-07-01328 и НШ-1939.2014.1 Президента России для ведущих научных школ.

захстана, Сингапура, Украины. Более 280 участников — студенты, около 120 — школьники, остальные участники — любители криптографии и профессионалы.

Участникам олимпиады было предложено 15 задач. Математические задачи олимпиады посвящены вопросам исследования дифференциальных характеристик S-блоков; взаимосвязи простейших операций, использующихся для построения шифра: циклического сдвига и сложения по модулю 2^k; построению специальных линейных подпространств в $\mathbb{F}_2^n$; поиску числа решений уравнения $F(x)+F(x+a)=b$ над конечным полем $\mathbb{F}_{2^n}$ и APN-функциям. Были и игровые задачи, такие, как крипто-квест, дешифрование секретных сообщений, анализ музыкального шифра. Детально задачи и их решения обсуждаются в [1, 2]. При этом работа [2] содержит не только разбор всех задач, но и комментарии к решениям участников, организационные моменты олимпиады, списки призёров.

Победителями олимпиады стали участники из Новосибирска, Омска, Москвы, Санкт-Петербурга, Саратова, Минска (Беларусь) и Лёвена (Бельгия): 15 участников в первом туре и 11 команд-победительниц во втором туре. Награждение призёров состоялось в Новосибирском государственном университете в декабре.

NSUCRYPTO задумана как ежегодное мероприятие. В следующий раз она пройдёт в ноябре 2015 г. (см. `www.nsucrypto.nsu.ru`). Приглашаем всех желающих принять в ней участие! Например, участники конференции Sibecrypt могут выбрать категорию «любитель/профессионал».

ЛИТЕРАТУРА

1. *Agievich S., Gorodilova A., Kolomeec N., Nikova S., et al.* Mathematical problems of the First international student's Olympiad in cryptography NSUCRYPTO // IV Симпозиум «Современные тенденции в криптографии» CTCrypt'15, Казань, 3–5 июня 2015 г.
2. *Agievich S., Gorodilova A., Kolomeec N., Nikova S., et al.* Problems, solutions and experience of the first international student's Olympiad in cryptography // Прикладная дискретная математика. 2015. № 3(29).

УДК 519.95 DOI 10.17223/2226308X/8/28

АТАКА ПО ШИФРТЕКСТАМ НА ОДНУ ЛИНЕЙНУЮ ПОЛНОСТЬЮ ГОМОМОРФНУЮ КРИПТОСИСТЕМУ[1]

А. В. Трепачева

Описывается новая стратегия атаки по шифртекстам на одну линейную полностью гомоморфную криптосистему, чья защищённость обосновывается с привлечением сложности задачи факторизации больших чисел. Приводятся теоретические и практические оценки вероятности раскрытия секретного ключа с использованием данной атаки. Проводится анализ связи трудности факторизации чисел и защищённости криптосистемы против атаки по шифртекстам, на основе которого предлагается более эффективная модификация криптосистемы.

Ключевые слова: *полностью гомоморфное шифрование, задача факторизации чисел, атака по шифртекстам.*

Введение

В связи с распространением облачных сервисов задача построения полностью гомоморфных криптосистем (ПГК), позволяющих проводить произвольные вычисления

[1]Работа поддержана грантом РФФИ № 15-07-00597-а.

над данными в зашифрованном виде, приобрела большую актуальность. Основным направлением в данной области является построение ПГК, основанных на теории решёток и методике Джентри [1]. Однако существующие на данный момент ПГК этого типа обладают низкой вычислительной эффективностью и являются непригодными для практики [1]. Поэтому не прекращаются поиски альтернативного варианта ПГК, не использующей метод Джентри и являющейся эффективной и криптостойкой. В частности, активно предлагаются ПГК, основанные на задаче факторизации чисел. В данной работе анализируется одна недавно предложенная ПГК этого вида из [2]. Описывается атака по шифртекстам (АШ) на ПГК [2], основанная на решении системы линейных уравнений и не рассмотренная ранее в литературе. Приводятся оценки вероятности её успеха в зависимости от различных параметров.

1. Полностью гомоморфная криптосистема из [2] и её основные свойства

Опишем ПГК, предложенную в [2]. Для зашифрования открытого текста $m \in \mathbb{Z}_n$ составляется матрица $D = \mathrm{diag}(m, r) \in \mathbb{Z}_n^{2\times 2}$, где $n = pq$, p, q — простые числа, $\log(p) = \log(q) \geqslant 512$ (т. е. n трудно факторизовать), $r \in \mathbb{Z}_n$ выбран по равномерному распределению, $\mathrm{diag}(m, r)$ — диагональная матрица с m, r на главной диагонали. Шифртекст вычисляется как $C = K^{-1}DK \in \mathbb{Z}_n^{2\times 2}$, где $K \in \mathbb{Z}_n^{2\times 2}$ — секретный ключ. Ясно, что m — собственное число C, имеющее собственный вектор $v_1 = K^{-1}e_1 \in \mathbb{Z}_n^2$, где $e_1 = (1, 0)$. Для расшифрования вычисляется $s = Cv_1$, а затем $m = s_1/v_{1,1}$. Описанная криптосистема — ПГК, так как в ней произведению и сумме шифртекстов соответствуют произведение и сумма открытых текстов. При этом операции над шифртекстами вычислительно эффективны (умножение и сложение матриц). Это делает данную ПГК очень интересной с практической точки зрения. Однако ПГК [2] совершенно нестойка к атаке по известным открытым текстам. По перехваченной паре (m, C) можно составить систему линейных уравнений $(C - mI)x = \mathbf{0}$, множество решений которой имеет базис $\{v_1\}$ с вероятностью ≈ 1, и поэтому наличие даже одной пары (m, C) компрометирует [2]. Больше информации об атаке по известным открытым текстам на ПГК [2] можно найти в [3].

2. Атака по шифртекстам на ПГК [2]

Предположим, противник перехватил последовательность $C_i \in \mathbb{Z}_n^{2\times 2}$, $i = 1, \ldots, t$, шифрующих $m_i \in \mathbb{Z}_n$, $i = 1, \ldots, t$, на ключе K. Ясно, что m_i — корень характеристического полинома $\mathrm{char}_i(x) \in \mathbb{Z}_n[x]$, составленного для C_i. Так как n трудно факторизовать, нахождение корней $\mathrm{char}_i(x)$ в общем случае трудно. Этим свойством в [2] и обосновывается защищённость ПГК. Однако на самом деле это работает, только если вероятностное распределение $\mathbb{D}$, заданное на пространстве открытых текстов $P = \mathbb{Z}_n$, является близким к равномерному. Если же, к примеру, $\mathbb{D}$ таково, что $\mathbf{P}\{m_i > \sqrt{n}\} = 0$, то, согласно [3], m_i можно найти из $\mathrm{char}_i(x)$.

Рассмотрим другую стратегию АШ на ПГК [2]. Противнику предлагается решить систему линейных уравнений

$$(C_i - C_j)x = \mathbf{0} \tag{1}$$

для $i = 1, \ldots, t$, $j = 1, \ldots, t$, $i \neq j$. Ясно, что если существуют i, j, такие, что $m_i = m_j$, то соответствующая система уравнений (1) имеет решение $v_1 = K^{-1}e_1 \in \mathbb{Z}_n^2$. Оценим вероятность Pr_t того, что существует хотя бы одна пара i, j, такая, что $m_i = m_j$. Для этого понадобится следующая лемма.

Лемма 1. Вероятность появления $\tilde{m} \in \mathbb{Z}_n$ хотя бы дважды в последовательности $\{\tilde{m}_k : k = 1, \ldots, w\}$, где $\tilde{m}_k \in \mathbb{Z}_n$ сгенерированы по вероятностному распределению $\mathcal{D}$,

равна $\tilde{\Pr}_{\mathcal{D},w}(\tilde{m}) = 1 - (1 - p_{\tilde{m}})^w - w(1 - p_{\tilde{m}})^{w-1} p_{\tilde{m}}$, где $p_{\tilde{m}}$ — вероятность появления $\tilde{m}$ в соответствии с $\mathcal{D}$.

Распределение $\mathcal{D}$ здесь считается таким, что все m_i независимы друг от друга. Легко видеть тогда, что $\mathsf{Pr}_t = 1 - \prod\limits_{\alpha=0}^{n-1}(1 - \tilde{Pr}_{\mathcal{D},t}(\alpha)) = 1 - \prod\limits_{\alpha=0}^{n-1}((1-p_\alpha)^t + t(1-p_\alpha)^{t-1}p_\alpha)$, где p_α — вероятность появления $\alpha \in \mathbb{Z}_n$ согласно $\mathcal{D}$. Другие ненулевые решения, кроме v_1, у системы (1) появляются, только если $r_i - r_j \notin \mathbb{Z}_n^*$. Последнее может произойти с вероятностью $\Pr = 1 - \phi(n)/n$, так как $r_i - r_j$ — равномерно распределённая на $\mathbb{Z}_n$ величина. В силу выбора n можно считать, что $\Pr \approx 0$, поэтому вероятность успеха описанной атаки равна Pr_t.

Для любого $\mathcal{D}$ справедливо $\lim\limits_{t\to\infty} \mathsf{Pr}_t = 1$. Однако атака оказывается практичной не для любого $\mathcal{D}$ из-за большого размера $P = \mathbb{Z}_n$. Наилучшим образом она работает для дискретного гауссова распределения $\mathcal{D} = \mathcal{D}_{\mathbb{Z}_n,\mu,\sigma^2}$, где μ — математическое ожидание; σ^2 — дисперсия и $\sigma^2 \ll n$. В таблице приведены значения Pr_t для разных t при n с $\log(n) = 1024$ и $\sigma^2 \ll n$; указаны также практические оценки вероятности $\tilde{\mathsf{Pr}}_t$ найти v_1 с помощью описанной стратегии, полученные при тестировании реализации атаки. Для получения каждой $\tilde{\mathsf{Pr}}_t$ проводилось 10^4 независимых испытаний.

t	Pr_t	$\tilde{\mathsf{Pr}}_t$
50	0,88	0,85
70	0,955	0,945
90	0,998	0,99
120	1	0,99999

3. Связь трудности факторизации больших чисел и защищённости криптосистемы

В [2] доказано, что умение правильно расшифровывать $C \in \mathbb{Z}_n^{2\times 2}$ позволяет факторизовать n. Однако для того чтобы строго связать криптостойкость с задачей факторизации, необходимо и обратное утверждение. Но оно не выполняется, так как если известны p, q, то из этого не следует корректное расшифрование C. Действительно, по китайской теореме об остатках $\mathrm{char}(x)$ для C имеет четыре корня, и чтобы выбрать из них открытый текст, придётся привлечь $\mathcal{D}$. Исходя из этого, можно модифицировать ПГК [2]. Пусть n задается как $n = \prod\limits_{k=1}^{l} p_k^{d_k}$, где p_k — простые числа, $p_i \neq p_j$. Решить уравнение $\mathrm{char}(x) = 0$ теперь нетрудно, так как n можно факторизовать. Однако количество решений равно 2^l. При знании $\mathcal{D}$ для выбора открытого текста среди этих решений необходимо $\geqslant 2^l$ операций. Если положить $l = 120$, то перебор окажется настолько велик, что атака на $\mathrm{char}(x)$ будет нереализуемой. Причём вычислительная сложность этого перебора эквивалентна сложности факторизации 1024-битного RSA модуля (с использованием метода решета числового поля), т. е. сложность атаки на $\mathrm{char}(x)$ остаётся такой же. При этом размер n можно уменьшить, подобрав нужным образом p_k, $k = 1, \ldots, l$; в результате ПГК [2] становится более эффективной.

Заключение

Предложена атака по шифртекстам на ПГК [2], основанная на решении системы линейных уравнений. Её практичность обусловлена распределением $\mathcal{D}$ на пространстве открытых текстов. Если $\mathcal{D}$ сильно отлично от равномерного, например $\mathcal{D}$ — гауссово распределение с небольшой дисперсией, то атака работает успешно. Для практики

это представляет интерес, так как в реальных приложениях $\mathcal{D}$ часто является именно таким. Обнаружено, что отсутствие строгой сводимости криптостойкости ПГК [2] к задаче факторизации позволяет использовать модуль n более скромных размеров без ухудшения защищённости. Это делает ПГК [2] более быстродействующей.

ЛИТЕРАТУРА

1. *Guellier A.* Can Homomorphic Cryptography ensure Privacy? PhD thesis, Inria; IRISA; Supélec Rennes, équipe Cidre; Université de Rennes 1, 2014.
2. *Kipnis A. and Hibshoosh E.* Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification // IACR Cryptology ePrint Archive. 2012. No. 637.
3. *Vizár D. and Vaudenay S.* Analysis of chosen symmetric homomorphic schemes // Central European Crypto Conference, Budapest, Hungary, 2014, EPFL-CONF-198992.

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.75 DOI 10.17223/2226308X/8/29

О ЗАЩИЩЁННОМ РАСПРЕДЕЛЁННОМ ПРОТОКОЛЕ В КОНКУРЕНТНОЙ СРЕДЕ НА ПРИМЕРЕ ПРОВЕДЕНИЯ СОРЕВНОВАНИЙ CTF

Н. И. Анисеня

Демонстрируется возможность создания и применения распределённого протокола в конкурентной среде на примере разработки математического метода проведения соревнований CTF (Captur The Flag), основанных на решении заданий, при угрозе DDoS-атак на сервер организаторов. Предлагается распределённый протокол проведения соревнований, который перекладывает часть функций организаторов на участников. Участники соревнования конкурируют друг с другом и не хотят помогать командам-соперникам, поэтому к протоколу предъявляются требования устойчивости к атакам со стороны самих участников. Предложенный протокол удовлетворяет поставленным требованиям. Рассмотрены атаки на протокол, исследована его устойчивость к ним, предложены модификации протокола. Сообщается о возможных направлениях дальнейших исследований в данной области.

Ключевые слова: *распределённые протоколы, защищённые вычисления, отказоустойчивые системы.*

Цель работы — предложить математический способ обеспечения доступности соревнования CTF, проводимого в формате Jeopardy, при угрозе DDoS-атаки на организаторов.

Под *централизованным сетевым взаимодействием*, или просто *централизованным взаимодействием*, участников будем понимать такое их взаимодействие, которое полагается на некоторый известный всем участникам узел сети — посредника, имеющего отличную от прочих участников и незаменимую по отношению к ним роль.

Злоумышленником назовём нечестного участника соревнования, который преследует хотя бы одну из следующих целей:

1) нарушение работоспособности системы, с высокой вероятностью приводящее к невозможности участия в соревновании всех участников;
2) нарушение работоспособности системы, с высокой вероятностью приводящее к искажению собственных результатов;
3) нарушение работоспособности системы, с высокой вероятностью приводящее к искажению результатов другого конкретного участника.

Активным участием некоторого узла назовём такое его поведение в сети, при котором он отправляет в сеть данные.

Для достижения указанной цели ставится следующая задача: разработать протокол распределённого проведения соревнований CTF, основанных на решении заданий.

Требования к протоколу следующие:

1) в результате работы протокола должна формироваться таблица результатов, позволяющая восстановить очерёдность получения ответов;
2) протокол не должен требовать активного участия организаторов во время проведения соревнования;
3) протокол не должен полагаться на централизованное взаимодействие участников во время проведения соревнования;
4) протокол должен позволять проводить соревнование даже при отключении большого количества участников;
5) протокол должен позволять проводить соревнование даже при большом количестве злоумышленников (нечестных участников).

При разработке протокола не рассматривались следующие ситуации и проблемы:

1) проблемы подготовительного этапа (регистрации команд);
2) ситуация распада графа сети на компоненты связности;
3) недостаточная точность временных расчётов с учётом выбранного временного окна.

Пусть на момент начала соревнования имеется сеть участников, описанная в [1], в которую команда организаторов входит как равноправный участник. Полагаем, что в этой сети для передачи сообщений используется безотказная луковая маршрутизация, описанная в [1]. Каждый участник на момент начала соревнования имеет:

1) алгоритмы цифровой подписи sign и verify;
2) алгоритм симметричного шифрования на ключе E_x;
3) множество идентификаторов участников U;
4) ключи проверки ответов $g_1, \ldots, g_m$;
5) псевдослучайную функцию $G(y)$ с параметрами k, t;
6) зашифрованный набор заданий.

Началом соревнования считается момент рассылки организаторами ключа для расшифрования списка заданий, после чего команда организаторов перестаёт принимать активное участие.

Пусть некоторый участник u с идентификатором ID_u получил ответ f на задание. Рассмотрим протокол, согласно которому должен действовать участник u:

1) $y = \mathrm{sign}_f(t_u, ID_u)$, t_u — текущее время пользователя u.
2) Для всех пользователей с идентификатором $id \in G(y)$:
   а) $u \to id : z = E_x(y, t_u, ID_u)$, x — сеансовый ключ;
   б) $id \to u : t_{id}, \mathrm{sign}_{\widehat{id}}(z, t_{id})$, t_{id} — текущее время пользователя с идентификатором id.
3) Каждому пользователю с идентификатором $id \in U$ выслать:
   t_u, ID_u, $y = \mathrm{sign}_f(t_u, ID_u)$, $z = E_x(y, t_u, ID_u)$, x, $\{t_i, \mathrm{sign}_{\widehat{id_i}}(z, t_i) : i \in G(y)\}$.

Соревнование завершается в установленное организаторами время. Таблица результатов, имеющаяся у организаторов в этот момент, считается итоговой.

Атаки, улучшения и дальнейшие направления исследований описаны в [1].

ЛИТЕРАТУРА

1. *Анисеня Н. И.* Разработка безопасного протокола распределённой системы проведения соревнований CTF // Прикладная дискретная математика. 2015. № 2(28). С. 59–70.

УДК 004.94 DOI 10.17223/2226308X/8/30

НЕОБХОДИМЫЕ УСЛОВИЯ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ ПО ВРЕМЕНИ В РАМКАХ МРОСЛ ДП-МОДЕЛИ

П. Н. Девянин

В рамках мандатной сущностно-ролевой ДП-модели, ориентированной на реализацию в отечественной защищённой операционной системе специального назначения (ОССН) *Astra Linux Special Edition*, формулируется теорема о необходимых условиях нарушения безопасности информационных потоков по времени (создания таких потоков «сверху вниз»), из которой следует, что эти условия легко устранить на практике, после чего для безопасности управления доступом ОССН в целом достаточно обеспечить в ней безопасность информационных потоков по памяти в смысле Белла — ЛаПадулы и мандатный контроль целостности.

Ключевые слова: *компьютерная безопасность, формальная модель, информационный поток, Linux.*

Анализ условий безопасности информационных потоков по времени (или, наоборот, её нарушения) при построении формальных моделей механизмов управления доступом часто является наиболее сложной задачей, решение которой начинается после того, как исследованы условия безопасности информационных потоков по памяти. Этим традиционным путём разрабатывалась мандатная сущностно-ролевая ДП-модель (сокращённо МРОСЛ ДП-модель) [1 – 3], большая часть элементов которой уже реализована в отечественной защищённой ОССН *Astra Linux Special Edition* [4]. После задания в модели элементов состояния системы, описания порядка функционирования мандатного и ролевого управления доступом и мандатного контроля целостности, де-юре и де-факто правил преобразования состояний системы и обоснования их корректности была сформулирована и доказана базовая теорема безопасности (БТБ-ДП) о достаточных условиях безопасности в смысле Белла — ЛаПадулы (предотвращения возможности реализации информационных потоков по памяти «сверху вниз») и мандатного контроля целостности (предотвращения возможности захвата контроля недоверенными субъект-сессиями над доверенными субъект-сессиями) [5], которые определяются следующим образом (с использованием обозначений из [1] даётся определение трёх смыслов нарушения безопасности, под безопасностью в каждом из этих смыслов понимается отсутствие соответствующего её нарушения).

Определение 1. Пусть G_0 — безопасное начальное состояние системы $\Sigma(G^*, OP, G_0)$ и существует траектория без кооперации доверенных и недоверенных субъект-сессий $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 1$. Будем говорить, что в состоянии G_N произошло нарушение безопасности системы, когда в нём выполняется одно из следующих условий, при этом они не выполняются в состояниях G_i траектории для $0 \leqslant i < N$:

— существуют недоверенная субъект-сессия $x \in N_{S_N}$ и доверенная субъект-сессия $y \in de\_facto\_own_N(x) \cap L_{S_N}$, такие, что $i_{s_N}(y) = i\_high$ (нарушение безопасности в смысле мандатного контроля целостности);

— существует информационный поток по памяти $(x, y, write_m) \in F_N$, такой, что $x, y \in E_N$ и неверно неравенство $f_{e_N}(x) \leqslant f_{e_N}(y)$ (нарушение безопасности в смысле Белла — ЛаПадулы);

— существует информационный поток по времени $(x, y, write_t) \in F_N$, такой, что $x, y \in$ $\in E_N$ и неверно неравенство $f_{e_N}(x) \leqslant f_{e_N}(y)$ (нарушение безопасности в смысле контроля информационных потоков по времени).

Для формулирования теоремы о необходимых условиях нарушения безопасности в смысле контроля информационных потоков по времени потребовалось уточнить заданные в модели условия использования имеющихся в реальной защищённой ОССН некоторых «особенных» сущностей. Изначально сущности — специальные объекты-«дырки», не позволяющие хранить данные или быть использованными для создания информационных потоков по памяти (например, сущности, соответствующие портам вывода на графические устройства, «слушающие» сокеты), в модели были включены в множество E_HOLE. Однако практическая реализация модели потребовала разделения этого множества на объекты-«дырки» первого вида (например, файлы `dev/null` или `dev/zero`), которые полностью не сохраняют данных, их нельзя использовать для создания любых информационных потоков (сущности из множества MT_HOLE), и объекты-«дырки» второго вида (сущности из множества M_HOLE), которые изначально входили в множество E_HOLE (таким образом, стало $E\_HOLE = MT\_HOLE \cup$ $\cup\, M\_HOLE$, $MT\_HOLE \cap M\_HOLE = \varnothing$).

Теорема 1. Пусть G_0 — безопасное начальное состояние системы $\Sigma(G^*, OP, G_0)$. Пусть на всех траекториях системы без кооперации доверенных или недоверенных субъект-сессий $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 1$, каждое состояние G_i безопасно в смыслах условия 1 и 2 определения 1, где $1 \leqslant i \leqslant N$, и безопасно в смысле условия 3 определения 1, где $1 \leqslant i < N$. Пусть также в состоянии G_N происходит нарушение безопасности в смысле условия 3 определения 1. Тогда выполняется одно из условий:

— существуют субъект-сессия $x \in N_{S_N} \cup NF_{S_N}$ и сущность $y \in M\_HOLE$, такие, что $(x, y, write_a) \in A_N$ и верно неравенство $f_{s_N}(x) < f_{e_N}(y)$ (найдётся недоверенная или некорректная относительно информационных потоков по времени доверенная субъект-сессия с низким уровнем доступа, имеющая доступ на запись к объекту-«дырке» второго вида с высоким уровнем доступа, через который возможно создание информационных потоков по времени);

— существуют сущность-контейнер $c \in C_N$ и сущность $e \in E_N$, такие, что $CCR_N(c) =$ $= CCRI_N(c) =$ `true`, $e < c$ и $f_{e_N}(e) < f_{e_N}(c)$ (найдётся сущность-контейнер с мандатными атрибутами конфиденциальности CCR и целостности $CCRI$, равными `true`, в состав которого входит сущность с меньшим уровнем конфиденциальности, что может позволить недоверенной субъект-сессии, изменяя параметры этой сущности-контейнера, через входящую в него сущность создавать информационные потоки по времени).

Из теоремы следует, что для предотвращения запрещённых информационных потоков по времени «сверху вниз» в реальной ОССН достаточно обеспечения её безопасности в смыслах условия 1 и 2 определения 1, исключения создания (особенно при установке или администрировании ОССН) сущностей-контейнеров с мандатными атрибутами конфиденциальности и целостности, равными `true`, в состав которых входят сущности с меньшим уровнем конфиденциальности, а также либо полный запрет на использование сущностей из множества M_HOLE (задание $M\_HOLE = \varnothing$), либо такую реализацию этих сущностей, когда их нельзя будет применять для создания информационных потоков по времени.

Таким образом, закончен очередной этап разработки комплексного научно-обоснованного технического решения [6], направленный на создание отечественной защи-

щённой ОССН *Astra Linux Special Edition* и заключающийся в теоретическом обосновании алгоритмически проверяемых и реализуемых на практике условий безопасности в ОССН информационных потоков по памяти и по времени.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учеб. пособие для вузов. 2-е изд., испр. и доп. М.: Горячая линия — Телеком, 2013. 338 с.
2. *Девянин П. Н.* Адаптация мандатной сущностно-ролевой ДП-модели к условиям функционирования ОС семейства Linux // Системы высокой доступности. 2013. № 3. С. 98–102.
3. *Девянин П. Н.* Администрирование системы в рамках мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux // Прикладная дискретная математика. 2013. № 4(22). С. 22–40.
4. Операционные системы Astra Linux. `http://www.astra-linux.ru/`
5. *Девянин П. Н.* Условия безопасности информационных потоков по памяти в рамках МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2014. № 7. С. 82–85.
6. *Девянин П. Н., Куликов Г. В., Хорошилов А. В.* Комплексное научно-обоснованное решение по разработке отечественной защищенной ОССН Astra Linux Special Edition // Методы и технические средства обеспечения безопасности информации: Материалы 23-й науч.-технич. конф. 30 июня–03 июля 2014 г. СПб.: Изд-во Политехн. ун-та, 2014. С. 29–33.

УДК 004.94 DOI 10.17223/2226308X/8/31

О ВОМОЖНОСТИ РЕАЛИЗАЦИИ СКРЫТЫХ КАНАЛОВ ПО ВРЕМЕНИ НА ОСНОВЕ ЗАГОЛОВКОВ КЭШИРОВАНИЯ ПРОТОКОЛА HTTP В ОБЛАЧНЫХ СЕРВИСАХ ХРАНЕНИЯ ФАЙЛОВ

Д. Н. Колегов, О. В. Брославский, Н. Е. Олексов

Показывается, как скрытые каналы по времени на основе заголовков кэширования протокола HTTP могут быть реализованы в облачных сервисах хранения файлов.

Ключевые слова: *HTTP, скрытые каналы, безопасность веб-приложений, ботсети.*

В [1] впервые предложено семейство скрытых каналов по времени на основе заголовков кэширования протокола HTTP, а также базовые сценарии их реализации. В [2] исследуются практические вопросы реализации таких скрытых каналов в современных компьютерных системах. Одним из сценариев реализации рассматриваемых скрытых каналов является сценарий в модели M_1, в рамках которой рассматривается взаимодействие доверенного веб-сервера и двух субъектов-нарушителей, кооперирующих друг с другом путём обращения к этому серверу с целью обмена вредоносными данными. Данный сценарий обеспечивает свойство анонимности скрытого канала, но может обеспечить лишь пропускную способность не более 1 бит/с. В данной работе в рамках рассматриваемого сценария предлагается метод реализации скрытого канала по времени, позволяющий повысить его пропускную способность и сохранить свойство анонимности.

Основным фактором, существенно ограничивающим пропускную способность скрытого канала в рамках модели M_1, является частота обновления заголовков кеширования веб-сервером. В результате проведенных экспериментов установлено, что веб-серверы облачных сервисов хранения файлов обновляют заголовки кэширования с более высокой частотой, чем традиционные веб-серверы. Это связано с необходимостью поддержание актуальной информации в файлах и их метаданных. Большинство крупных облачных файловых хостингов предоставляют программный интерфейс (API), облегчающий загрузку и скачивание файлов, а также управление уже размещённой на сервере информацией: изменение параметров и прав доступа к файлам, их систематизацию и обновление метаданных. Возможность обновления метаданных, в частности времени последнего изменения файла, позволяет говорить о реализации скрытого канала по времени на основе заголовков кеширования.

Рассмотрим схему реализации данного скрытого канала (рис. 1). Пусть e_1 — сущность-файл, содержащая передаваемую информацию и доступная на чтение субъекту s_1; e_3 — сущность-ресурс, расположенная на серверах облачного файлового хостинга и доступная на запись субъекту s_1 через предоставляемый программный интерфейс файлового хостинга s_2; e_2 — сущность HTTP-запрос; e_4 — сущность HTTP-ответ; e_5 — сущность-файл, доступная на запись субъекту s_3.

Для передачи одного бита информации из e_1 субъект s_1 осуществляет HTTP-запрос к программному интерфейсу сервиса хранения файлов s_2, обновляющий время последней модификации сущности-ресурса e_3. В тот же временной интервал субъект s_3 при помощи HTTP-запроса к программному интерфейсу или непосредственно к сущности e_3 получает значение используемого заголовка либо иным из описанных в [2] способов определяет факт модификации сущности e_3. Субъект s_3 интерпретирует полученные сведения о модификации в соответствии с выбранным способом кодирования и записывает полученный бит в e_5. Процесс передачи повторяется через выбранный интервал времени.

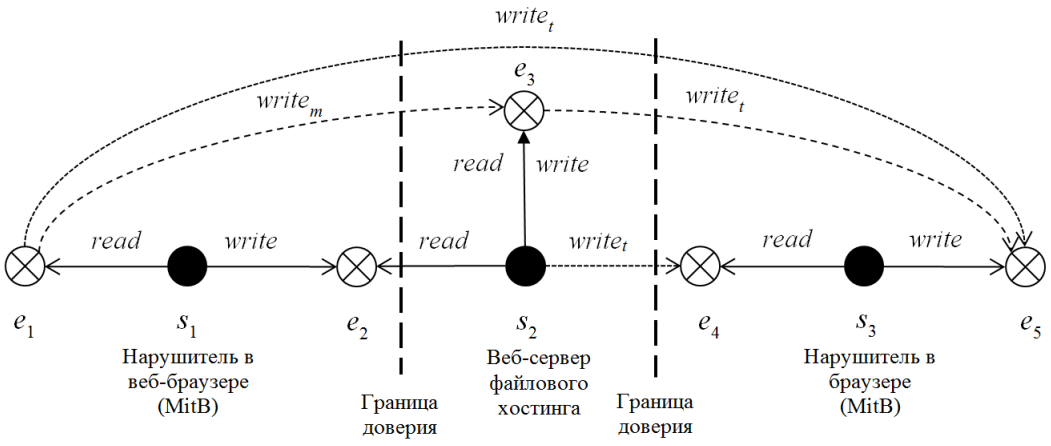

Рис. 1. Схема функционирования скрытых каналов по времени на основе заголовков кэширования HTTP в облачном файловом сервисе

Предложенный метод реализации скрытых каналов по времени на основе заголовков кеширования протокола HTTP позволяет существенно повысить пропускную способность скрытых каналов, сохраняя высокий уровень анонимности: крупные файловые сервисы, как правило, являются доверенными с точки зрения сетевых средств

контроля, а обнаружение скрытого канала, реализованного подобным образом, также затруднительно, так как им используется только стандартная функциональность, предоставляемая API сервиса. Теоретическая пропускная способность такого скрытого канала составляет 1 бит за $(L + S)$ секунд, где L — время, необходимое s_3 для выполнения запроса к e_3, а S — время, уходящее на обработку запроса на серверах хостинга.

Рассмотрим пример реализации предложенного метода на примере облачного сервиса хранения файлов Google Drive. Субъект s_1 через заданные промежутки времени осуществляет чтение одного бита из сущности e_1 и, в зависимости от полученных данных, совершает или не совершает POST-запрос e_2 по адресу `www.googleapis.com/drive/v2/files/`**fileId**`/touch`, где **fileId** — идентификатор сущности e_3. Данный запрос обновляет время последней модификации сущности-ресурса e_3. В тот же временной интервал субъект s_3 выполняет GET-запрос по адресу `www.googleapis.com/drive/v2/files/`**fileId** и получает ответ e_4, содержащий значение entity-tag сущности e_3. Субъект s_3 записывает в e_5 бит 1, если ресурс был модифицирован с момента последнего запроса, и бит 0 в противном случае.

В результате тестирования реализации скрытого канала через сервис Google Drive достигнута пропускная способность 3 бит/с при точности передачи 99,8 %, где под точностью понимается отношение числа правильно переданных бит к общему числу бит. Установлено, что основным фактором, влияющим на пропускную способность реализации, является время обработки запроса серверами сервиса. Таким образом, можно говорить о достижении в эксперименте максимальной пропускной способности канала.

ЛИТЕРАТУРА

1. *Колегов Д. Н., Брославский О. В., Олексов Н. Е.* Об информационных потоках по времени, основанных на заголовках кэширования протокола HTTP // Прикладная дискретная математика. Приложение. 2014. № 7. С. 89–91.
2. *Колегов Д. Н., Брославский О. В., Олексов Н. Е.* Исследование скрытых каналов по времени на основе заголовков кэширования протокола HTTP // Прикладная дискретная математика. 2015. № 2. С. 71–85.

УДК 004.94 DOI 10.17223/2226308X/8/32

НЕИНВАЗИВНЫЙ МЕТОД КОНТРОЛЯ ЦЕЛОСТНОСТИ COOKIE В ВЕБ-ПРИЛОЖЕНИЯХ

Д. Н. Колегов, О. В. Брославский, Н. Е. Олексов

Предлагается метод контроля целостности cookie в веб-приложениях, построенный на основе криптографических протоколов с ключевыми хеш-функциями. Метод может быть использован для реализации неинвазивных механизмов защиты от атак на веб-приложения через cookie.

Ключевые слова: *криптографические протоколы, хеш-функции, веб-приложения, web cookie.*

Термином *cookie* в протоколе HTTP обозначается набор данных, хранимый веб-клиентом (веб-браузером) и отправляемый на сервер в специальном заголовке Cookie в HTTP-запросах. Cookie первоначально могут быть сгенерированы на веб-сервере и переданы веб-клиенту в заголовке Set-Cookie в HTTP-ответе либо сгенерированы

на стороне веб-клиента с помощью переданного веб-сервером Javascript. Cookie, как правило, используются веб-приложением для идентификации и аутентификации пользователей, а также для хранения произвольных данных, настроек и т. п. Таким образом, если веб-приложение имеет уязвимость, связанную с недостаточной обработкой данных, передаваемых в cookie (например, уязвимость к атаке внедрения операторов SQL), то злоумышленник может модифицировать полученные cookie для эксплуатации данной уязвимости. Примеры атак на веб-приложения через механизм cookie описаны, например, в [1].

Одним из методов защиты от атак на веб-приложения является использование ключевых хеш-функций для аутентификации HTTP сообщений. Первоначально данный метод использовался лишь для контроля целостности атрибутов HTML (например, атрибутов href, src, action) и полей форм [2, 3]. В работе [4] метод обобщён и показано, как он может быть применён для защиты веб-приложений от широкого класса атак (например, CSRF, утечка токенов, HPP и др.). Одним из достоинств данного метода является возможность его неинвазивной реализации на уровне веб-приложения — реализации, не требующей изменения исходного кода веб-приложения.

Ввиду существенных отличий в структуре данных и принципах функционирования механизма cookie метод [4] не может быть применен к последнему в том же виде. В данной работе исследуется возможность неинвазивного контроля целостности cookie на основе хеш-фунций.

Структура данных cookie может быть представлена в виде набора $c = (k_c, v_c, p_c, d_c, e_c, f_c)$, где k_c — ключ (имя cookie); v_c — значение cookie; p_c — значение атрибута path; d_c — значение атрибута domain; e_c — значения атрибута expires; f_c — список флагов (например, *secure* — передача cookie возможна только по HTTPS; *session* — cookie является сессионной; *httponly* — доступ к cookie средствами Javascript запрещён).

При установке cookie веб-сервер отправляет веб-клиенту в заголовках HTTP-ответа весь необходимый набор атрибутов, которые сохраняются веб-клиентом, после чего больше никогда не отправляются в HTTP-запросах к серверу. Таким образом, обеспечение целостности всех атрибутов cookie представляется более сложной задачей, чем тривиальное хеширование всех контролируемых атрибутов. Алгоритмы обеспечения целостности cookie, предложенные в [5], решают данную задачу лишь частично, обеспечивая целостность только для значения cookie и времени жизни. Подходы, описанные в работах [6, 7], решают задачи, связанные с реализацией защищённого контейнера на основе cookie для «sessionless»-веб-приложений.

Предлагаемый метод контроля целостности cookie обладает следующими свойствами:

— обеспечение целостность значения cookie;
— защита cookie от удаления или продления, т. е. от изменения атрибута expires или установки флага *session*;
— обеспечение целостности значений атрибутов path и domain;
— контроль передачи cookie по защищённому соединению при установленном флаге *secure*;
— возможность неинвазивной реализации.

Будем использовать следующие обозначения: $x|y$ — конкатенация строк x и y; $hmac$ — ключевая хеш-функция, построенная по алгоритму HMAC; $hmac(k, s)$ — результат применения алгоритма $hmac$ с ключом k к строке s.

Пусть C — множество всех cookie, используемых веб-приложением, а $S \subseteq C$ — множество защищаемых (контролируемых) cookie. Для каждой защищаемой cookie $c = (k_c, v_c, p_c, d_c, e_c, f_c) \in S$ построим парную ей cookie $c\_s = (k_s, v_s, p_s, d_s, e_s, f_s)$, где:

1) e_s — максимально возможное значение, что позволяет получать из cookie c актуальную информацию о cookie c_s, даже если последняя устарела;
2) $p_s = p_c$ и $d_s = d_c$, что обеспечивает одновременную отправку веб-клиентом cookie c и c_s до истечения времени expires;
3) $v_s = hmac(k, v_c|e_c)|e_c$, где k — ключ, уникальный для каждой сессии веб-приложения; данное построение позволяет контролировать целостность значений v_c и e_c и, кроме того, проверять, не истекло ли время жизни cookie c;
4) $f_s = f_c \cup \{httponly\}$.

Аутентификатором множества S будем называть строку $auth$, полученную конкатенацией значений k_c, p_c, d_c, f_c для всех cookie c из S.

Для определения легитимности отправки каждой защищаемой cookie по значениям атрибутов path и domain дополнительно введём вспомогательную cookie $\alpha = (k_\alpha, v_\alpha, p_\alpha, d_\alpha, e_\alpha, f_\alpha)$, в которой:

1) $v_\alpha = hmac(k, auth)|auth$, где $auth$ — аутентификатор S;
2) p_α и d_α выбираются наиболее общими для рассматриваемого веб-приложения, что гарантирует отправку cookie α при любом запросе к веб-севрверу;
3) e_α — максимально возможное значение;
4) $f_\alpha = \{httponly\}$.

Рассмотрим основные действия протокола взаимодействия веб-клиента и веб-сервера. При первом запросе к веб-серверу пользователю устанавливается α с некоторым начальным значением. Все последующие запросы к веб-приложению обрабатываются в соответствии с приведённым ниже методом. Если в ответе веб-сервера устанавливается одна или несколько защищаемых cookie, то для каждой такой cookie c в HTTP-ответ добавляется заголовок Set-Cookie, устанавливающий парную ей cookie c_s, а данные о c заносятся в α. После обработки всех защищаемых cookie в HTTP-ответе значение $hmac$ в α пересчитывается и в HTTP-ответ добавляется заголовок Set-Cookie, устанавливающий обновлённую α. При необходимости выставляются заголовки, удаляющие отмеченные на удаление cookie.

Метод обработки запроса к веб-приложению

Условия применения метода: задано множество S защищаемых cookie веб-приложения.

Для каждого HTTP-запроса h выполнить следующие шаги:

1) Если в HTTP-запросе h отсутствует cookie α, то удалить из запроса h все защищаемые cookie $c \in S$ и отправить модифицированный запрос h веб-серверу.
2) Проверить целостность значения cookie α. Для этого по значению v_α вычислить $hmac' = hmac(k, auth')$. При несовпадении $hmac'$ и $hmac$ запрос следует считать запрещённым.
3) Удалить из запроса h все защищаемые cookie $c \in S$, которые отсутствуют в α.
4) Для каждой защищаемой cookie $c \in S$, присутствующей в запросе h, проверить выполнение следующих условий:
   а) запрос h содержит для c парную cookie c_s;
   б) атрибут p_c, полученный из cookie α, допускает отправку cookie c в запросе h;

в) атрибут d_c, полученный из cookie α, допускает отправку cookie c в запросе h;
г) для cookie c с флагом *secure* запрос h передан по HTTPS;
д) выполняется равенство $v_s = hmac(k, v_c|e_c)$ и e_c меньше текущего времени.

При невыполнении любого из условий запрос следует считать запрещённым.

5) Пометить на удаление все cookie c_s, для которых в запросе h отсутствуют парные им cookie c.

В случае, если HTTP-запрос к веб-приложению признан запрещённым, его обработка приложением может привести к эксплуатации уязвимости, а потому нежелательна. В связи с этим предлагаются следующие варианты обработки таких HTTP-запросов:

1) Блокирование HTTP-запроса.
2) Перенаправление пользователя на некоторый URL-адрес.
3) Завершение сессии пользователя веб-приложения путём отправления на веб-сервер специального HTTP-запроса и последующего удаления парных cookie и выставления начального значения cookie α.
4) Модификация HTTP-запроса путём удаления из него всех некорректных cookie и последующей отправки этого запроса на веб-сервер.

Таким образом, описанный метод контролирует целостность всех атрибутов cookie, защищает их от несанкционированного удаления на клиентской стороне, позволяет определить необходимость отправки cookie на заданный путь и домен веб-приложения, а также обеспечивает аутентичность cookie. В то же время данный метод предполагает добавление $|S| + 1$ дополнительных cookie. Количество последних можно существенно сократить, отказавшись от введения парных cookie и вычисляя значение v_α следующим образом: $v_\alpha = hmac(k, m)|m$, где m — строка, полученная конкатенацией значений $domain_i$, $path_{ij}$, $hmac_{ij}$. Значение $hmac_{ij} = hmac(k, m_{ij})$, где m_{ij} — конкатенация значений k_c и v_c для всех cookie c, которые могут быть отправлены на домен $domain_i$ и путь $path_{ij}$. В данном варианте реализации для всех защищаемых cookie $c \in S$ должны быть известны p_c и d_c.

В этом случае обработка HTTP-запроса h происходит следующим образом:

1) Если в HTTP-запросе h отсутствует cookie α, то удалить из запроса h все защищаемые cookie $c \in S$ и отправить модифицированный запрос h веб-серверу.
2) Проверить целостность значения cookie α. Для этого по значению v_α вычислить $hmac' = hmac(k, m')$. При несовпадении $hmac'$ и $hmac$ запрос следует считать запрещённым.
3) Вычислить $hmac(k, m)'$ для v'_α, используя для формирования m значения защищаемых cookie, полученных в h. При несовпадении $hmac(k, m)'$ и соответствующего текущему пути и домену значения $hmac_{ij}$ в v_α запрос следует считать запрещённым.

Обработка HTTP-ответа происходит следующим образом:

1) Если HTTP-запрос был запрещён, то выставить в ответе заголовки, удаляющие на стороне клиента все защищаемые cookie $c \in S$ и α.
2) Если в HTTP-ответе присутствуют заголовки, устанавливающие защищаемые cookie, то следует обновить значение $hmac_{ij}$ для всех пар $(domain_i; path_{ij})$, соответствующих текущему пути и домену.

Данный метод обеспечивает целостность значений cookie, требует меньшего количества служебных cookie, но накладывает следующие существенные ограничения на веб-приложение:

— невозможность выставления cookie c с атрибутами path и domain, отличными от пути и домена HTTP-запроса, в котором выставляется cookie c;
— невозможность пересчёта значения $hmac$ по истечении времени жизни или при удалении cookie;
— инициализация новой сессии при любом некорректном запросе.

Реализация данных методов не требует изменения исходного кода веб-приложения и может быть выполнена на уровне гибридных WAF (например, ModSecurity), модульных фрэймворков (например, Django, Ruby on Rails) и сетевых WAF (например, F5 BIG-IP ASM). Прототип системы, реализующей эти методы, разработан на базе Django Middleware [8].

ЛИТЕРАТУРА

1. *Barnett R.* The Web Application Defender's Handbook: Battling Hackers and Protecting Users. Indianapolis: John Wiley & Sons, 2013. 522 p.
2. Reducing Web Application Attack Surface. `http://blog.spiderlabs.com/2012/07/reducing-web-apps-attack-surface.html`
3. ModSecurity Advanced Topic of the Week: HMAC Token Protection. `http://blog.spiderlabs.com/2014/01/modsecurity-advanced-topic-of-the-week-hmac-token-protection.html`
4. *Колегов Д. Н.* Общий метод аутентификации HTTP-сообщений в веб-приложениях на основе хеш-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 85–89.
5. *Fu K., Sit E., Smith K., and Feamster N.* Dos and Don'ts of client authentication on the Web // Proc. 10th USENIX Security Symp., Washington, 2001. P. 251–268.
6. *Liu A., Kovacs J., Huang C., and Gouda M.* A secure cookie protocol // Proc. 14th Intern. Conf. Computer Communications and Networks, 2005. P. 333–338.
7. *Murdoch S.* Hardened Stateless Session Cookies. `http://www.cl.cam.ac.uk/~sjm217/papers/protocols08cookies.pdf`
8. Прототип модуля неинвазивного контроля целостности cookie на базе Django. `https://github.com/tsu-iscd/django-HTTPauth`

УДК 004.94 DOI 10.17223/2226308X/8/33

НЕИНВАЗИВНАЯ РЕАЛИЗАЦИЯ МАНДАТНОГО УПРАВЛЕНИЯ ДОСТУПОМ В ВЕБ-ПРИЛОЖЕНИЯХ НА УРОВНЕ СУБД

Д. Н. Колегов, Н. О. Ткаченко

Предлагается неинвазивный метод (метод, не изменяющий исходный код самого приложения) устранения уязвимостей в механизмах логического управления доступом и информационными потоками в веб-приложениях на уровне СУБД. Задача ставится следующим образом: имеется многоуровневое веб-приложение, в котором реализована подсистема базового управление доступом (как правило, ролевого), возможно, имеющая некоторое множество уязвимостей. Необходимо устранить как можно более широкий класс данных уязвимостей без изменения исходного кода самого приложения или обеспечить реализацию новой политики мандатного управления доступом. Метод включает выполнение следующих

шагов: идентификация субъектов веб-приложения с помощью специального интегрируемого модуля и передачи полученных идентификаторов в SQL-запросах; обработка SQL-запросов с учётом формальной политики мандатного управления доступом на уровне прокси-сервера; переписывание SQL-запросов для предотвращения несанкционированного доступа к данным.

Ключевые слова: *управление доступом, веб-приложения, безопасность СУБД.*

Управление доступом в системах управления базами данных (СУБД) в большинстве случаев реализуется на уровне ядра системы. Однако такой подход имеет ряд недостатков. Во-первых, в подавляющем большинстве случаев реализуется управление доступом на основе дискреционной политики. Исключением являются специализированные защищённые СУБД, такие, как RUBIX [1], Линтер [2] или расширения для СУБД общего назначения, например пакет Oracle Label Security для СУБД Oracle [3], где реализуется политика мандатного управления доступом типа MLS. Во-вторых, в реализованных механизмах управления доступом, как и в любом другом программном обеспечении, могут содержаться ошибки. К примеру, сравнительно недавно в популярной СУБД MySQL была найдена уязвимость, позволяющая обойти процедуру аутентификации [4]. При этом ошибки могут быть не только в реализации системы, но и в её модели безопасности [5], особенно если речь идёт о достаточо сложном мандатном или ролевом управлении доступом.

В то же время с точки зрения управления доступом СУБД, как правило, является отдельной информационной системой и функционирует независимо от приложения пользователя, которое её использует. В качестве примера можно рассмотреть типовое веб-приложение, которое содержит множество пользователей на уровне веб-сервера, но все они выполняют операции в СУБД от имени одной её учётной записи, соответствующей этому веб-приложению. Так как все операции на уровне СУБД выполняются от имени одной учётной записи, можно считать, что управление доступом на уровне СУБД отсутствует и в случае наличия ошибок в реализации управления доступом в коде веб-приложения злоумышленник может получить доступ к данным любого пользователя приложения, хранящимся в СУБД.

В работе предлагается неинвазивный метод реализации управления доступом в веб-приложении на уровне СУБД MySQL, основанный на формальных моделях безопасности для СУБД MySQL [6, 7] и реализации монитора безопасности на уровне прокси-сервера для SQL-запросов [8]. Метод позволяет получить информацию об идентификаторах пользователей веб-приложения и передать их (прозрачно для веб-приложения) в SQL-запросах, а затем на уровне SQL-прокси реализовать заданную политику управления доступом. Процедура идентификации субъектов осуществляется с помощью технологии тэгирования — добавления к SQL-запросу идентификатора пользователя в форме комментария. После того как мы идентифицировали субъектов веб-приложения, необходимо идентифицировать сущности СУБД. В СУБД MySQL минимальной единицей доступа являются столбцы, поэтому стандартными средствами возможно реализовать управление доступом лишь до уровня столбцов, что недостаточно для современных защищённых веб-приложений. Для обеспечения возможности идентификации строк таблиц СУБД предложен метод определения принадлежности записи из защищаемой таблицы СУБД пользователю веб-приложения.

Рассмотрим последний метод более детально. В некоторых СУБД, в том числе в СУБД MySQL и в порождённых от нее, например, в СУБД MariaDB, управление доступом не позволяет задать право доступа к строке таблицы. Наименьшим контей-

нером, к которому право доступа может быть задано, выступает столбец. Типовые веб-приложение часто используют таблицу для хранения однотипных записей всех пользователей. В этом случае отсутствие проверок допустимых значений входных данных пользователяей веб-приложения, влияющих на генерируемый SQL-запрос, может привести к несанкционированному доступу к данным. Предлагаемый метод включает анализ генерируемого SQL-запроса и добавление в него дополнительных условий. Анализ запроса состоит в проверке наличия защищаемой таблицы в списке таблиц, к которым осуществляется доступ. *Защищаемой таблицей* называется таблица, для столбца которой активирован описываемый механизм. Если такая таблица присутствует в запросе, то он модифицируется путём добавления условия в раздел WHERE или HAVING исходного SQL-запроса. Добавляемое условие формируется в момент анализа запроса из шаблона, описанного администратором в конфигурационном файле. Шаблон представляет собой кортеж из трёх объектов:

— полного пути до защищаемого столбца в формате «БАЗА_ДАННЫХ.ТАБЛИЦА.СТОЛБЕЦ»;
— регулярного выражения, поддерживаемого СУБД MySQL и соответствующего уникальному значению идентификатора пользователя;
— пути, связывающего столбец с идентификаторами пользователей и столбец из защищаемой таблицы, если такой может быть построен.

Второй и третий объекты решают задачу определения принадлежности записи конкретному пользователю. При этом возможны следующие варианты. Если защищаемая таблица содержит столбец с идентификаторами пользователей, то третий объект не обязателен для заполнения и может быть построено регулярное выражение с использованием предопределённых параметров, таких, как идентификатор пользователя, определяющий принадлежность записи. Если же защищаемая таблица содержит столбец, по которому возможно определить принадлежность записи пользователю через связи с другими таблицами, то третий объект может быть использован для описания этих связей. Например, если в защищаемой таблице хранятся зарплатные ведомости и первичным ключом является инкрементируемое числовое значение, то для связи владельца заработной платы и её значения может быть построен путь от первичного ключа защищаемой таблицы через промежуточную таблицу, реализующую связь многие ко многим, до столбца с идентификаторами пользователей.

Основой прототипа является MySQL-proxy, реализующий политику мандатного управления доступом типа MLS и TE на основе разработанной ранее формальной ДП-модели [7]. Механизмы, позволяющие определить принадлежность записи из защищаемой таблицы СУБД пользователю веб-приложения, и идентификация пользователей веб-приложения реализованы в виде модулей веб-фреймворка Django. Общая схема полученного прототипа изображена на рис. 1.

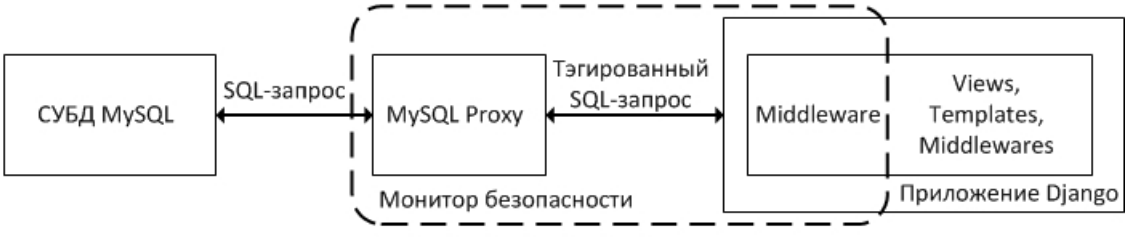

Рис. 1. Общая схема прототипа системы

Рассмотрим процесс прохождения запроса пользователя веб-приложения к СУБД. Аутентифицированный пользователь веб-приложения отправляет HTTP-запрос на выполнение какого-либо действия. Это приводит к генерации SQL-запроса к СУБД MySQL. Перед отправкой запрос тэгируется идентификатором пользователя, инициировавшим его выполнение, с использованием модуля Django фреймворка. Основная функция модуля состоит в модификации некоторых методов класса-обёртки CursorWrapper, который используется для перехвата некоторых исключений класса Cursor. В результате модификации SQL-запросы пользователя, генерируемые слоем Object-Relational Mapping фреймворка Django или написанные пользователем вручную, будут перехвачены и обработаны. Далее запрос, содержащий идентификатор пользователя, поступает на MySQL-proxy. Если механизм контроля записей сконфигурирован, то осуществляется анализ SQL-запроса. В результате анализа определяется возможность получения пользователем записей, ему не принадлежащих; если это возможно, к запросу добавляется дополнительное условие, гарантирующее получение пользователем только его записей. Затем запрос отправляется на обработку в СУБД MySQL.

ЛИТЕРАТУРА

1. Trusted DBMS Rubix. `http://rubix.com/cms`
2. СУБД Линтер. `http://linter.ru`
3. Oracle Database. Oracle Label Security. `http://www.oracle.com/technetwork/database/options/label-security/index.html`
4. CVE-2012-2122. `https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2122`
5. *Девянин П. Н., Захаренков П. С.* Способ реализации информационного потока по времени в операционных системах с мандатным управлением доступом через clipboard // Методы и технические средства обеспечения безопасности информации: материалы Юбилейной 20-й науч.-технич. конф. 27 июня–01 июля 2011 г. СПб.: Изд-во Политехн. ун-та, 2011. С. 76–77.
6. *Колегов Д. Н., Ткаченко Н. О., Чернов Д. В.* Разработка и реализация мандатных механизмов управления доступом в СУБД MySQL // Прикладная дискретная математика. Приложение. 2013. № 6. С. 62–67.
7. *Колегов Д. Н., Ткаченко Н. О., Чернов Д. В.* Основные элементы разработки механизма мандатного управления доступом в СУБД MySQL на основе ДП-моделей // Безопасность информационных техологий. 2014. № 3. С. 102–107.
8. *Ткаченко Н. О.* Реализация монитора безопасности СУБД MySQL в DBF/DAM-системах // Прикладная дискретная математика. Приложение. 2014. № 7. С. 99–101.

УДК 004.056.5 DOI 10.17223/2226308X/8/34

РЕАЛИЗАЦИЯ АТАКИ DNS REBINDING

Т. И. Милованов

Исследована акутальность атаки DNS Rebinding в современных браузерах. Атака направлена на обход концепции одинакового источника (Same Origin Policy). Цель работы — исследование применимости атаки для доступа к узлам локальной сети пользователя. Составлен список браузеров, наиболее подверженных атаке. В инструмент для тестов на проникновение BeEF встроено расширение, позволяющее реализовать атаку на практике. Сформулированы условия, при которых данная атака успешно реализуется, и рекомендации по защите.

Ключевые слова: *HTTP, pentesting, веб-приложения.*

Существует важная концепция веб-безопасности, которой руководствуются современные браузеры при исполнении сценариев — концепция одинакового источника (Same Origin Policy) [1]. Сценарий — это программа, исполняемая на стороне пользователя. Пользователь получает сценарий при обращении к некоторому веб-серверу, который будем называть источником. Обычно сценарии написаны на языке JavaScript и предназначены для оформления веб-страниц или выполнения на стороне пользователя обработки перед отправкой данных на сервер. Концепция разрешает сценарию доступ к данным источника, если и только если сценарий получен с этого источника. Источник характеризуется тремя признаками: доменным именем, портом, протоколом. Два источника считаются одинаковыми, если у них совпадают все три признака.

При запросе к веб-серверу браузер пользуется системой DNS, преобразующей доменное имя веб-сервера в его сетевой адрес (IP-адрес). DNS реализуется распределённой системой серверов, выполняющих данное преобразование. Владелец веб-сервера может иметь собственный DNS-сервер, отвечающий за доменное имя веб-сервера.

Основная идея атаки DNS Rebinding в том, что в концепции одинакового источника в характеристики источника не входит сетевой адрес. Злоумышленник может выполнить свой сценарий с данными другого источника, будем называть его целевым, если доменному имени веб-сервера злоумышленника будет соответствовать не один, а два сетевых адреса — адрес веб-сервера злоумышленника и адрес целевого веб-сервера. Заметим, что система DNS позволяет такое неоднозначное соответствие. В данной работе рассматривается возможность доступа к целевым веб-серверам, находящимся в локальной сети пользователя. Таковыми могут быть, например, роутеры, практически все из которых имеют веб-интерфейс. Приведём общую схему атаки.

1) Пользователь обращается к веб-серверу злоумышленника с помощью доменного имени.
2) Браузер пользователя формирует запрос к DNS-серверу злоумышленника с целью получить сетевой адрес, соответствующий доменному имени. DNS-сервер отвечает парой сетевых адресов.
3) Браузер пользователя обращается по первому сетевому адресу, который считает основным, и получает веб-страницу злоумышленника вместе со сценарием.
4) Злоумышленник блокирует дальнейшие обращения пользователя к своему веб-серверу (например, с помощью межсетевого экрана).
5) Сценарий в браузере пользователя инициирует повторное обращение к веб-серверу злоумышленника с помощью доменного имени, но вследствие блокировки веб-сервера не получает ответа по первому сетевому адресу и обращается по второму, который является адресом целевого веб-сервера в локальной сети пользователя. Браузер пользователя разрешает это обращение, поскольку не изменился ни один из трёх признаков источника.

В современных браузерах существует два типа реакций на полученный от DNS-сервера ответ, содержащий локальный IP-адрес. Некоторые браузеры считают его основным, некоторые — второстепенным. Первый тип реакции более безопасен, он предотвращает приведённую выше схему атаки, поскольку исключает получение сценария с веб-сервера злоумышленника. Протестированы реакции современных веб-браузеров на получение подобных запросов:

Браузер	Версия	Тип реакции
Opera	27.0	Второй
Android Browser	4.2	Второй
Google Chrome	40	Второй
Google Chrome	41	Первый
Firefox	35.0.1	Первый

Атака реализована в инструменте для тестов на проникновение — BeEF (The Browser Exploitation Framework). Это проект с открытым исходным кодом. Похожая реализация атаки была сделана на языке C в виде отдельного приложения [2].

BeEF состоит из двух основных частей. Первая часть — серверная и устанавливается на компьютере тестировщика на проникновение, будем называть его исследователем. Вторая часть — JavaScript-сценарий на компьютере пользователя, локальная сеть которого является объектом исследования. Для реализации атаки написаны модуль (module) и расширение (extension). Это предусмотренные разработчиками BeEF средства для добавления новой функциональности в проект. Модуль отвечает за то, как действует JavaScript в браузере пользователя (вторая составная часть BeEF). Расширение отвечает за то, как реагирует на эти действия BeEF (первая составная часть BeEF). Написанные части вместе позволяют исследователю взаимодействовать с целевым веб-сервером из локальной сети пользователя так же, как если бы исследователь имел прямой доступ к серверу. Написанное расширение состоит из двух частей — веб-сервера и прокси-сервера. Веб-сервер при обращении к нему возвращает сценарий пользователю и блокирует дальнейшие его обращения, то есть реализует п. 3 и 4 приведённой схемы атаки. Прокси-сервер необходим для интерактивной двусторонней связи исследователя со сценарием, выполняющимся в браузере пользователя. С помощью этого сервера исследователь может отправлять или получать данные с целевого веб-сервера в локальной сети пользователя.

Главная часть модуля — это JavaScript-сценарий. Он состоит из трёх асинхронных запросов. Первый запрос регулярно обращается к прокси-серверу за очередным запросом исследователя к целевому серверу. Второй отправляет полученный запрос к целевому серверу и обрабатывает ответ. Третий отправляет результат обратно прокси-серверу. Вторая задача модуля — это занесение в DNS-сервер исследователя соответствия «доменное имя веб-сервера исследователя — сетевые адреса», необходимого для реализации п. 2 атаки.

Для того чтобы проведение исследования было возможным, должны выполняться следующие условия:

1) браузер пользователя не должен содержать открытых соединений с целевым веб-сервером;
2) браузер пользователя не должен содержать TCP-соединений с состоянием TIME WAIT с сетевым адресом целевого веб-сервера;
3) браузер пользователя не должен содержать в DNS-кэше других сетевых адресов, связанных с доменом веб-сервера исследователя.

При невыполнении хотя бы одного из этих условий не будет выполнен п. 3 схемы атаки. Браузер пользователя будет считать сетевой адрес целевого веб-сервера основным и не сможет получить сценарий.

Для защиты от данной атаки необходимо правильно настроить веб-сервер, который может оказаться атакуемым. Для того чтобы нарушить п. 5 схемы атаки, веб-сервер не должен отвечать на запросы, у которых заголовок Host содержит произвольный сетевой адрес.

ЛИТЕРАТУРА

1. `https://tools.ietf.org/html/rfc6454` — The Web Origin Concept.
2. `http://code.google.com/p/rebind/` — DNS Rebinding Tool.

УДК 004.65, 004.056.52 DOI 10.17223/2226308X/8/35

АТРИБУТНОЕ УПРАВЛЕНИЕ ДОСТУПОМ К ХРАНИЛИЩУ ДАННЫХ ТИПА «КЛЮЧ — ЗНАЧЕНИЕ»

С. В. Овсянников, В. Н. Тренькаев

Предлагается способ разграничения доступа пользователей к хранилищу данных типа «ключ — значение», когда право на доступ вычисляется в зависимости от параметров запроса (тип операции, идентификатор данных, пароль). Данный способ апробирован при разработке NoSQL СУБД с сервером управления доступом и удалённым хранилищем данных.

Ключевые слова: *атрибутное управление доступом, хранилище данных типа «ключ — значение», NoSQL база данных.*

В современных СУБД нередко отсутствует реализация так называемого мелко гранулированного управления доступом к данным (fine-grained access control), когда требуется ограничить доступ пользователей к отдельным строкам таблицы (как в случае реляционной БД) или к отдельной паре «ключ — значение» (как в случае NoSQL-хранилища данных). В данной работе для этих целей предлагается использовать подход, который можно отнести к атрибутной модели управления доступом [1], когда субъект имеет право доступа к сущности, если истинен предикат, вычисленный от атрибутов субъекта и/или сущности. При этом рассмотрена ситуация, когда имеется возможность пользователям самим настраивать политику безопасности СУБД, определяя правила задания разграничительной политики доступа к ресурсам БД.

Далее будем иметь дело с хранилищем данных типа «ключ — значение» (key — value), т. е. когда база данных представляет собой набор записей, идентифицируемых по ключу. Формально ключ будем рассматривать как слово в заданном алфавите. В простейшем случае каждый ключ ставится в соответствие значению в виде произвольных данных, в усложнённом варианте значение связано с определённым типом данных (целые, строки, списки, множества). Хранилище пар «ключ — значение» отличается упрощённой моделью запросов, используется малый набор операций: установка (set), получение (get), удаление (delete) значений по ключу.

Предлагается задавать политику безопасности хранилища данных с помощью функции управления доступом $C : K \times O \times P \to \{Allow, Deny, Pass\}$, где K — множество префиксов ключей; $O = \{set, get, delete, access\}$ — множество операций, P — множество парольных слов. Значение функции C, равное $Allow$, изначально определяется не менее чем для одной тройки $(k, access, p) \in K \times O \times P$, и тот, кто знает пару (k, p), может условно считаться администратором хранилища данных. Кроме запросов к хранилищу на обработку данных по ключу $(set, get, delete)$, возможны также запросы на изменение политики безопасности $(access)$, т. е. на задание (изменение) значений функции C.

Пусть запрос к хранилищу данных имеет следующие параметры: key (идентификатор данных), $value$ (значение данных), op (операция), pas (пароль). С точки зрения управления доступом запрос обрабатывается, следуя двум правилам.

П р а в и л о 1. Инициатору запроса разрешено произвести операцию $op \in O$, если существует префикс pk слова key, такой, что $C(pk, op, pas) = Allow$, и при этом выполняется условие: если функция C определена для некоторого префикса $prefix$ слова pk, то $C(prefix, op, pas) = Pass$.

П р а в и л о 2. Инициатору запроса запрещено произвести операцию $op \in O$, если существует префикс pk слова k, такой, что $C(pk, op, pas) = Deny$, и при этом выполняется условие: если функция C определена для некоторого префикса $prefix$ слова pk, то $C(prefix, op, pas) = Pass$.

Считается, что префикс слова может совпадать с самим словом. Если условия правила 1 или правила 2 не выполняются, например, из-за того, что функция управления доступом не определена на параметрах запроса, то запрос не выполняется.

В таблице приведён простой пример задания функции управления доступом с использованием псевдокода. Для запросов с паролем «p1» разрешается выполнять любые операции над данными с ключами, которые начинаются с «a». Для запросов с ключом «ab» разрешается чтение данных всем, а запись только тем, кто знает пароль «p2».

Префиксы ключей	Псевдокод вычисления значения функции управления доступом
a	IF password = p1 return ALLOW; ELSE return PASS;
ab	IF operation = get return ALLOW; IF operation = set IF password = p2 return ALLOW; ELSE return DENY;

ЛИТЕРАТУРА

1. *Чернов Д. В.* О моделях логического управления доступом на основе атрибутов // Прикладная дискретная математика. Приложение. 2012. №. 5. С. 79–82.

УДК 004.62 DOI 10.17223/2226308X/8/36

THE CAPACITY OF A PACKET LENGTH COVERT CHANNEL

A. V. Epishkina, K. G. Kogos

Covert channels are used for information hiding and realize one of the most serious security threat. Widespread IP networks allow for designing such channels on the basis of special properties of packet data transfer. Packet length covert channels are resistant to traffic encryption, but some difficulties to detect them are known. It makes significant an investigation of capacity limitation methods. This work presents a technique to estimate and limit the capacity of the covert channels based on the packet length modulation by traffic padding.

Keywords: *covert channel, packet length, dummy packet, capacity limitation.*

A covert channel is a communication channel which is not intended for information transfer at all, such as the service program's effect on the system load [1]. At present the most popular covert channels are in packet networks because of some features available in the TCP/IP protocol suite. There is a number of undetectable packet length covert channels in IP networks that may be constructed even if an encryption is used at any OSI model level. This paper describes a technique to estimate and limit the capacity of such covert channels using dummy packets generation.

The design of the considered network covert channel and of a counteraction technique is as follows. Let the lengths of transferred packets have the natural values from l_{fix} to $l_{\text{fix}} + L$; $\{L_0, L_1\}$ is a partition of the set $N_{l_{\text{fix}}+L} \setminus N_L$ where $|L_0| = |L_1|$, N_a stands for the

set of positive integers from 1 to a. Further, we consider a method to build a binary covert channel. In order to transfer «0» the sender communicates a packet of a length of $l \in L_0$, to transfer «1» the sender communicates a packet of the length $l \in L_1$. It is obvious that the capacity of such channel without counteraction is equal to 1 bit per packet. To build such a covert channel the sender must have the following possibilities: to modify lengths of transmitted packets, to form packets of an undefined length, to buffer packets to be sent and to transfer them at a specified moment.

The authors propose a technique to limit the capacity of covert channel based on traffic padding. After k data packets have been sent, a random length dummy packet is created where k is the parameter of a counteraction tool. Let μ be the capacity of a communication channel, then a counteraction tool decreases the capacity of a communication channel to $k\mu/(k+1)$.

After dummy packet receiving, the mismatch between the hidden sender and the hidden receiver takes place. To negotiate this fact SOF packets [2] are utilized after $T-1$ packets transferring within the covert channel. The receiver fixes $T-1$ packets gained after SOF packet and waits for the next SOF packet. Thus T is the covert channel parameter which estimates the synchronization frequency. As the identification of bits received after the mismatch happened is wrong, in order to build the covert channel the inequality $T < k+1$ is required. The corresponding choice of parameters is explained in Fig. 1.

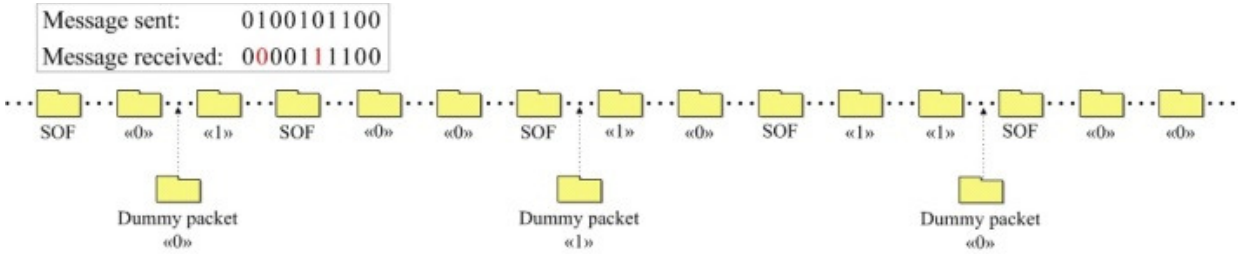

Fig. 1. The scheme of data transfer in the covert channel ($T = 3$, $k = 5$).

The capacity C of the investigated covert channel is $C = \max\limits_{X} I(X,Y)$ where $I(X,Y)$ is the mutual information of random variables X and Y describing respectively the input and output data of the channel properly. Since each T-th packet sent via the covert channel is not a data packet but is a synchronization one, the mutual information can be calculated using the following formula:

$$I(X,Y) = \frac{T-1}{T} I^*(X,Y),$$

where $I^*(X,Y) = H(Y) - H(Y|X)$ is a mutual information of random variables describing the input and output data of the covert channel without synchronization.

The sizes of sets L_0 and L_1 are equal and lengths of dummy packets passing through the covert channel are chosen randomly and equiprobable. Therefore, $H(Y) = 1$. Since the values of conditional probabilities $p(y|x)$ for $x, y \in \{0,1\}$ depend on the number of packets sent via a covert channel from the moment of synchronization to the moment of a dummy packet receiving, the mutual information $I^*(X,Y)$ can be found using the following formula:

$$I^*(X,Y) = \frac{k - (T-1) + \sum\limits_{i=0}^{T-2} \Big(1 - H_i(Y|X)\Big)}{k},$$

where $H_i(Y|X)$ is the conditional entropy of Y compared to X evaluated when i packets are received between the synchronization and dummy packet arrival moments.

Then the approximate value of the mutual information for X and Y is

$$I(X,Y) \approx \frac{T-1}{T} - \frac{(T-1)^2}{kT} + \frac{(2T-3)(T-1)}{2kT} \log_2 \frac{2T-3}{T-1} - \frac{(T-2)(T-1)}{2kT \ln 2}.$$

Note, that if k is a continuous variable, $k \in [T; +\infty)$, then $I(X,Y) \approx A(T)/k + B(T)$ is a hyperbola as a function of k where

$$A(T) = \frac{(T-1)^2}{T} + \frac{(2T-3)(T-1)}{2T} \log_2 \frac{2T-3}{T-1} - \frac{(T-2)(T-1)}{2T \ln 2}$$

is negative strictly decreasing, $B(T) = (T-1)/T$ is positive strictly increasing, and they are functions of T. To build a covert channel the parameter T is chosen to maximize $I(X,Y)$. For example when $k \in \{2,3,4\}$ the parameter T should be equal to 2, when $k \in \{5,6,7,8\}$ the parameter T should be equal to 3 and when $k \in \{9,10,11,12,13,14\}$ the parameter T should be equal to 4. Graphs for function $I(X,Y)$ of k and $T = 2,3,4,5$ are illustrated in Fig. 2.

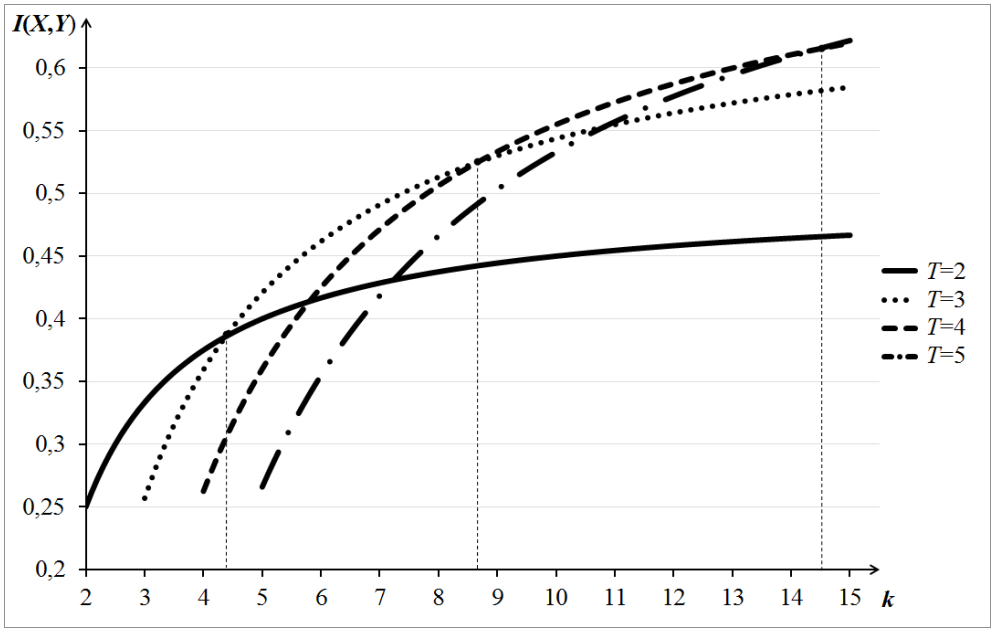

Fig. 2. Graphs for $I(X,Y)$ as the function of k and $T = 2,3,4,5$.

Let $v_{\max}$ be the value of the covert channel capacity such that the functioning of the covert channel with a capacity less than $v_{\max}$ has no influence upon security. Then a value T_0 can be defined satisfying the following inequalities:

$$\begin{cases} v_{\max} - C_{\min}(T_0) > 0, \\ C_{\min}(T_0) > C_{\min}(T), \end{cases}$$

for every $T \geqslant 2$, $T \neq T_0$ where $C_{\min}(T)$ is the capacity of the covert channel when the value k is taken the smallest for each fixed value T.

In fact, the parameter of counteraction tool k can be computed as $k = \left\lfloor \dfrac{B(T_0)}{v_{\max} - A(T_0)} \right\rfloor$.

The results of the work are useful for constructing secure IP networks. The authors have suggested a technique to select the parameter of the counteraction tool when an allowable covert channel capacity is given. The novelty of the method is that the capacity of the covert channel is limited in contrast to the other approaches which detect and destroy the active covert channels. The topic of the further work is to research the techniques to limit the packet length covert channel capacity by random increasing the lengths of packets before sending them.

BIBLIOGRAPHY

1. *Lampson B. W.* A note on the confinement problem // Comm. ACM. 1973. No. 16. P. 613–615.
2. *Cabuk S., Brodley C. E., and Shields C.* IP covert timing channels: design and detection // Proc. CCS'04, October 25–29, 2004, Washington, DC, USA. P. 178–187.

Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

УДК 519.718 DOI 10.17223/2226308X/8/37

НЕНАДЁЖНОСТЬ СХЕМ ПРИ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ НА ВХОДАХ И ВЫХОДАХ ЭЛЕМЕНТОВ[1]

М. А. Алехина

Рассматривается реализация булевых функций схемами из ненадёжных функциональных элементов в базисе, содержащем только штрих Шеффера. Предполагается, что каждый из элементов схемы подвержен неисправностям типа 0 или типа 1 на входах или выходах (с различными вероятностями). Получена верхняя асимптотическая оценка ненадёжности этих схем. Для почти любой булевой функции найдена нижняя асимптотическая оценка ненадёжности, и обе асимптотические оценки оказались равны.

Ключевые слова: *ненадёжные функциональные элементы, ненадёжность схемы, константные неисправности.*

Впервые задачу синтеза надёжных схем из ненадёжных функциональных элементов рассматривал Дж. фон Нейман [1]. Он также предполагал, что все базисные элементы подвержены инверсным неисправностям на выходах и переходят в неисправные состояния независимо друг от друга. Задача синтеза надёжных схем при константных неисправностях одного типа (например, только типа 0 на входах элементов) решена в базисах из двухвходовых элементов [2]. В [3] приведены результаты о ненадёжности схем при инверсных неисправностях и отказах элементов. В этой работе впервые исследуется модель, в которой каждый элемент схемы может быть подвержен константным неисправностям четырёх типов: типа 0 или типа 1 на входах или выходах (с различными вероятностями). Заметим также, что инверсные неисправности элементов являются частным случаем в рассматриваемой модели неисправностей.

Рассмотрим реализацию булевых функций схемами из ненадёжных функциональных элементов в базисе $\{x|y\}$ (где $x|y = \overline{x\&y}$ — штрих Шеффера). Схема из ненадёжных элементов реализует функцию $f(x_1, \ldots, x_n)$ $(n \in \mathbb{N})$, если при поступлении на входы схемы набора $\tilde{a}^n = (a_1, \ldots, a_n)$ при отсутствии неисправностей в схеме на её выходе появляется значение $f(\tilde{a}^n)$. Предполагаем, что в каждый такт работы схемы на любом из входов и выходе любого из её элементов независимым образом могут происходить константные неисправности: типа 0 на входах с вероятностью $\gamma_0 \in (0, 1/8)$, или типа 1 на входах с вероятностью $\gamma_1 \in (0, 1/4)$, или типа 0 на выходах с вероятностью $\varepsilon_0 \in (0, 1/4)$, или типа 1 на выходах с вероятностью $\varepsilon_1 \in (0, 1/4)$.

Неисправности типа 0 *на входах элементов* характеризуются тем, что в исправном состоянии функциональный элемент реализует функцию $x|y$, а в неисправном поступающий на его вход нуль не искажается, а поступающая на вход единица с ве-

[1]Работа поддержана грантом РФФИ, проект № 14-01-00273.

роятностью γ_0 может превратиться в нуль. Аналогично определяются неисправности типа 1 на входах.

Неисправности типа 0 *на выходах элементов* характеризуются тем, что в исправном состоянии функциональный элемент реализует функцию $x|y$, а в неисправном — с вероятностью ε_0 константу 0. Аналогично определяются неисправности типа 1 на выходах.

Пусть схема S реализует булеву функцию $f(\tilde{x}^n)$. Обозначим через $P_{\overline{f(\tilde{a}^n)}}(S, \tilde{a}^n)$ вероятность появления значения $\overline{f(\tilde{a}^n)}$ на выходе схемы S при входном наборе $\tilde{a}^n$. *Ненадёжность* $P(S)$ схемы S определяется как максимальное из чисел $P_{\overline{f(\tilde{a}^n)}}(S, \tilde{a}^n)$ по всем входным наборам $\tilde{a}^n$ схемы S. *Надёжность* схемы S равна $1 - P(S)$.

Учитывая характер рассматриваемых неисправностей, вычислим вероятности появления ошибок на выходе базисного элемента E при всех входных наборах этого элемента: $P_0(E,(00)) = \gamma_1^2(1-\varepsilon_1) + (1-\gamma_1^2)\varepsilon_0$, $P_0(E,(01)) = P_0(E,(10)) = \gamma_1(1-\gamma_0)(1-\varepsilon_1) + (1-\gamma_1(1-\gamma_0))\varepsilon_0$, $P_1(E,(11)) = (1-\gamma_0)^2\varepsilon_1 + (2\gamma_0 - \gamma_0^2)(1-\varepsilon_0)$.

Замечание 1. Отметим, что 1) если $\gamma_0 = \gamma_1 = \varepsilon_1 = 0$, то получим неисправности типа 0 на выходах элементов с вероятностью ε_0; 2) если $\gamma_0 = \gamma_1 = \varepsilon_0 = 0$, то получим неисправности типа 1 на выходах элементов с вероятностью ε_1; 3) если $\gamma_1 = \varepsilon_1 = \varepsilon_0 = 0$, то получим неисправности типа 0 на входах элементов с вероятностью γ_0; 4) если $\gamma_0 = \varepsilon_1 = \varepsilon_0 = 0$, то получим неисправности типа 1 на входах элементов с вероятностью γ_1; кроме того 5) если $\gamma_0 = \gamma_1 = 0$ и $\varepsilon_0 = \varepsilon_1$, то получим инверсные неисправности на выходах элементов с вероятностью ε_0; 6) если $\gamma_0 = \gamma_1$ и $\varepsilon_0 = \varepsilon_1 = 0$, то получим инверсные неисправности на входах элементов с вероятностью γ_0.

Обозначим $P_0(E,(00)), P_0(E,(01)), P_0(E,(10)), P_1(E,(11))$ через $\alpha, \beta, \delta, \tau$ соответственно. Поскольку в нашем случае $\beta = \delta$, ненадёжность элемента E равна $P(E) = \max\{\alpha, \beta, \tau\} \leqslant \max\{\gamma_1 + \varepsilon_0, 2\gamma_0 + \varepsilon_1\}$. Обозначим через $\varepsilon = \max\{\gamma_1 + \varepsilon_0, 2\gamma_0 + \varepsilon_1\}$. Очевидно, что $P(E) \leqslant \varepsilon$.

Справедлива теорема 1 об асимптотической верхней оценке ненадёжности схем.

Теорема 1. Любую булеву функцию можно реализовать схемой, ненадёжность которой асимптотически не больше, чем $2\varepsilon_0 + 2\gamma_1^2 + 2\gamma_0 + \varepsilon_1$ при $\gamma_0, \gamma_1, \varepsilon_0, \varepsilon_1 \to 0$.

Доказательство такое же, как и в случае, когда базисный элемент подвержен только одному типу неисправностей.

Пусть $h(\tilde{x}^n)$ — произвольная булева функция, а $K(n)$ — множество булевых функций вида $f(\tilde{x}^n) = (\bar{x}_i \vee h(\tilde{x}^n))^a$, где $i \in \{1, \ldots, n\}$; $a \in \{0, 1\}$. Нетрудно проверить, что число функций в классе $K(n)$ не больше $2n2^{2^{n-1}}$, что мало по сравнению с общим числом 2^{2^n} булевых функций от n переменных. Обозначим $K = \bigcup\limits_{n=1}^{\infty} K(n)$. Справедлива теорема 2 об асимптотической нижней оценке ненадёжности схем.

Теорема 2. Если функция $f \notin K$, а S — любая схема, реализующая f, то ненадёжность $P(S)$ схемы S асимптотически не меньше, чем $2\varepsilon_0 + 2\gamma_0 + \varepsilon_1 + 2\gamma_1^2$ при $\gamma_0, \gamma_1, \varepsilon_0, \varepsilon_1 \to 0$.

Доказательство такое же, как и в случае, когда базисный элемент подвержен только одному типу неисправностей.

Выводы:

1) любую булеву функцию можно реализовать схемой, ненадёжность которой асимптотически не больше $2\varepsilon_0 + 2\gamma_0 + \varepsilon_1 + 2\gamma_1^2$ при $\gamma_0, \gamma_1, \varepsilon_0, \varepsilon_1 \to 0$;

2) для почти любой функции f ($f \notin K$) такая схема функционирует с ненадёжностью, асимптотически равной $2\varepsilon_0 + 2\gamma_0 + \varepsilon_1 + 2\gamma_1^2$ при $\gamma_0, \gamma_1, \varepsilon_0, \varepsilon_1 \to 0$, т. е. оценку $2\varepsilon_0 + 2\gamma_0 + \varepsilon_1 + 2\gamma_1^2$ нельзя понизить для функций $f \notin K$.

ЛИТЕРАТУРА

1. *Von Neuman J.* Probabilistic logics and the synthesis of reliable organisms from unreliable components // Automata Studies. C. Shannon and J. Mc. Carthy (eds). Princeton University Press, 1956. (Рус. пер.: Автоматы. М.: ИЛ, 1956.)
2. *Алехина М. А.* Синтез асимптотически оптимальных по надёжности схем. Пенза: ИИЦ ПГУ, 2006. 156 с.
3. *Алехина М. А, Барсукова О. Ю.* Об оценках ненадёжности схем при инверсных неисправностях и отказах функциональных элементов // Прикладная дискретная математика. Приложение. 2013. № 6. С. 50–51.

УДК 519.718 DOI 10.17223/2226308X/8/38

НИЖНЯЯ ОЦЕНКА НЕНАДЁЖНОСТИ СХЕМ В БАЗИСЕ, СОСТОЯЩЕМ ИЗ ФУНКЦИИ ВЕББА[1]

М. А. Алехина, О. Ю. Барсукова

Рассматривается реализация функций трёхзначной логики схемами из ненадёжных функциональных элементов в базисе, состоящем из функции Вебба. Предполагается, что все базисные элементы независимо друг от друга переходят в такие неисправные состояния, что любой базисный элемент на любом входном наборе с вероятностью $1 - 2p$ выдаёт правильное значение и с вероятностью, равной p, может выдать любое из двух неправильных значений. Получена нижняя оценка ненадёжности схем, реализующих функции из некоторого класса.

Ключевые слова: *функции трёхзначной логики, схема из ненадёжных функциональных элементов, надёжность и ненадёжность схемы.*

Пусть $n \in \mathbb{N}$, P_3 — множество всех функций трёхзначной логики, т. е. функций $f(x_1, \ldots, x_n) : \{0,1,2\}^n \to \{0,1,2\}$. Обозначим через $\tilde{x}$ набор $(x_1, \ldots, x_n)$, тогда $f(x_1, \ldots, x_n) = f(\tilde{x})$.

Рассмотрим реализацию функций из множества P_3 схемами из ненадёжных функциональных элементов в базисе, состоящем из функции Вебба $V_3(x_1, x_2) = (\max(x_1, x_2) + 1) \bmod 3$. Будем считать, что схема из ненадёжных элементов реализует функцию $f(\tilde{x})$, если при поступлении на входы схемы набора $\tilde{a}$ при отсутствии неисправностей в схеме на её выходе появляется значение $f(\tilde{a})$.

Предполагается, что все базисные элементы ненадёжны, переходят в неисправные состояния независимо друг от друга, подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что на произвольном входном наборе (a_1, a_2) базисного элемента, $V_3(a_1, a_2) = \nu$, этот элемент с вероятностью $1 - 2\varepsilon$ ($\varepsilon \in (0, 1/4)$) выдаёт значение ν, с вероятностью ε — значение $(\nu + 1) \bmod 3$ и с вероятностью ε — значение $(\nu + 2) \bmod 3$.

Пусть схема S реализует функцию $f(\tilde{x})$, $\tilde{a}$ — произвольный входной набор схемы S, $f(\tilde{a}) = \tau$. Обозначим через $P_{f(\tilde{a}) \neq \tau}(S, \tilde{a})$ вероятность появления ошибки на выходе схемы S при входном наборе $\tilde{a}$. Ясно, что $P_{f(\tilde{a}) \neq \tau}(S, \tilde{a}) = P_{\tau+1}(S, \tilde{a}) + P_{\tau+2}(S, \tilde{a})$. Например,

[1]Работа поддержана грантами РФФИ № 14-01-00273 и 14-01-31360.

если входной набор $\tilde{a}$ схемы S такой, что $f(\tilde{a}) = 0$, то вероятность ошибки на этом наборе равна $P_{f(\tilde{a})\neq 0}(S, \tilde{a}) = P_1(S, \tilde{a}) + P_2(S, \tilde{a})$.

Ненадёжностью схемы S будем называть число $P(S) = \max\{P_{f(\tilde{a})\neq\tau}(S, \tilde{a})\}$, где максимум берется по всем входным наборам $\tilde{a}$ схемы S. *Надёжность* схемы S равна $1 - P(S)$.

Теорема 1 [1]. Любую функцию $f \in P_3$ можно реализовать такой схемой D, что $P(D) \leqslant 8\varepsilon + 268\varepsilon^2$ при всех $\varepsilon \in (0, 1/10^4]$.

Из теоремы 1 следует, что любую функцию из P_3 можно реализовать схемой, функционирующей с ненадёжностью, асимптотически (при $\varepsilon \to 0$) не больше 8ε.

Обозначим через $K(n)$ множество функций трёхзначной логики, каждая из которых зависит от переменных $x_1, \ldots, x_n$ ($n \geqslant 3$), принимает все три значения $0, 1, 2$ и не представима в виде $\max\{x_k, h(\tilde{x}^n)\} + c$ ($k \in \{1, 2, \ldots, n\}$, $c \in \{0, 1, 2\}$, $h(\tilde{x}^n)$ — произвольная функция трёхзначной логики).

Обозначим через K множество $K = \bigcup\limits_{n=3}^{\infty} K(n)$.

Справедлива теорема 2 о нижней оценке ненадёжности, доказательство которой аналогично доказательству теоремы о нижних оценках [2] (кратко в [3]).

Теорема 2. Пусть функция $f \in K$. Тогда для любой схемы S, реализующей f, при $\varepsilon \in (0, 1/10^4]$ верно неравенство $P(S) \geqslant 6\varepsilon - 16\varepsilon^2 + 12\varepsilon^3$.

Утверждение 1. $|K(n)| \geqslant 3^{3^n} - n3^{1+2\cdot 3^{n-1}} - 3 \cdot 2^{3^n}$.

Из утверждения 1 следует, что класс K содержит почти все функции из P_3, поскольку

$$\lim_{n\to\infty} \frac{3^{3^n} - n3^{1+2\cdot 3^{n-1}} - 3 \cdot 2^{3^n}}{3^{3^n}} = 1.$$

Из теоремы 2 следует, что функцию из класса K (содержащего почти все функции множества P_3) нельзя реализовать схемой с ненадёжностью, асимптотически (при $\varepsilon \to 0$) меньше 6ε.

Таким образом, получаем следующий результат: в базисе $\{V_3(x_1, x_2)\}$ почти любую функцию трёхзначной логики можно реализовать надёжной схемой, функционирующей с ненадёжностью, асимптотически не больше 8ε и асимптотически не меньше 6ε при $\varepsilon \to 0$.

ЛИТЕРАТУРА

1. *Алехина М. А., Барсукова О. Ю.* Верхняя оценка ненадежности схем в базисе, состоящем из функции Вебба // Известия высших учебных заведений. Математика. Казань: Изд-во Казанского (Приволжского) федерального университета, 2015. № 3. С. 15–27.
2. *Алехина М. А., Барсукова О. Ю.* Оценки ненадежности схем в базисе Россера — Туркетта // Известия высших учебных заведений. Поволжский регион. Физ.-мат. науки. Пенза: ИИЦ ПГУ, 2014. № 1. С. 33–50.
3. *Алехина М. А., Барсукова О. Ю.* Ненадёжность схем в базисе Россера — Туркетта // Прикладная дискретная математика. Приложение. 2014. № 7. С. 109–110.

УДК 519.718 DOI 10.17223/2226308X/8/39

НИЖНИЕ ОЦЕНКИ НЕНАДЁЖНОСТИ СХЕМ В БАЗИСЕ РОССЕРА — ТУРКЕТТА (В P_4)[1]

М. А. Алехина, С. П. Каргин

Рассматривается реализация функций четырёхзначной логики схемами из ненадёжных функциональных элементов в базисе Россера — Туркетта. Предполагается, что все элементы схемы независимо друг от друга с вероятностью p подвержены инверсным неисправностям на выходах, т. е. каждый базисный элемент на любом входном наборе с вероятностью p выдаёт каждое из трёх неверных значений, с вероятностью $1 - 3p$ выдаёт верное значение. Найден класс функций K, содержащий почти все четырёхзначные функции, и показано, что любая схема, реализующая функцию из класса K, функционирует с ненадёжностью, которая асимптотически (при малых значениях p) не меньше $9p$.

Ключевые слова: *функции четырёхзначной логики, ненадёжные функциональные элементы, ненадёжность схемы, инверсные неисправности на выходах элементов.*

Многозначная логика предоставляет широкие возможности для разработки различных алгоритмов во многих областях. Она позволяет уменьшить как вычислительную сложность, так и размеры, число соединений в различных арифметико-логических устройствах, повысить плотность размещения элементов на схемах, найти альтернативные методы решения задач. Уже сейчас многозначная логика с успехом применяется при решении многих задач и во множестве технических разработок. Среди них различные арифметические устройства, системы искусственного интеллекта и обработки данных, обработка сложных цифровых сигналов и т. д.

В [1] описан функционально полный в P_3 базис, в котором на компромиссной основе согласованы математические и технические (МДП-техники) требования и интересы, а также рассмотрены некоторые аспекты синтеза электронных схем в этом базисе. В [2] построен функционально полный в P_4 базис, реализуемый в МОП-структурах.

Таким образом, определённый интерес представляет задача исследования надёжности функционирования схем в полном конечном базисе из k-значных функций ($k \geqslant 3$). Задача построения надёжных схем в произвольном полном базисе из трёхзначных функций ($k = 3$) решена в [3].

В работе получена нижняя оценка ненадёжности схем в базисе Россера — Туркетта при $k = 4$. Нижняя оценка ненадёжности схем в том же базисе при $k = 3$ опубликована в [4].

Пусть $n \in \mathbb{N}$, а P_4 — множество всех функций четырёхзначной логики, т. е. функций $f(x_1, \ldots, x_n) : \{0, 1, 2, 3\}^n \to \{0, 1, 2, 3\}$. Рассмотрим реализацию функций из множества P_4 схемами из ненадёжных функциональных элементов в базисе Россера — Туркетта $\{0, 1, 2, 3, J_0(x_1), J_1(x_1), J_2(x_1), J_3(x_1), \min\{x_1, x_2\}, \max\{x_1, x_2\}\}$ ($\min\{x_1, x_2\}$ будем также обозначать через $\&$, а $\max\{x_1, x_2\}$ — через $\vee$ [1]).

Будем считать, что схема из ненадёжных элементов реализует функцию $f(\tilde{x}^n)$ ($\tilde{x}^n = (x_1, \ldots, x_n)$), если при поступлении на входы схемы набора $\tilde{a}^n$ при отсутствии неисправностей в схеме на её выходе появляется значение $f(\tilde{a}^n)$.

Пусть схема S реализует функцию $f(\tilde{x}^n)$, $\tilde{a}^n$ — произвольный входной набор схемы S, $f(\tilde{a}^n) = \tau$. Обозначим через $P_i(S, \tilde{a}^n)$ вероятность появления значения i ($i \in$

[1]Работа поддержана грантом РФФИ, проект № 14-01-00273.

$\in \{0,1,2,3\}$) на выходе схемы S при входном наборе $\tilde{a}^n$, а через $P_{f(\tilde{a}^n)\neq\tau}(S,\tilde{a}^n)$ — вероятность появления ошибки на выходе схемы S при входном наборе $\tilde{a}^n$. Ясно, что $P_{f(\tilde{a}^n)\neq\tau}(S,\tilde{a}^n) = P_{\tau+1}(S,\tilde{a}^n) + P_{\tau+2}(S,\tilde{a}^n) + P_{\tau+3}(S,\tilde{a}^n)$. (В выражениях $\tau+1$, $\tau+2$ и $\tau+3$ сложение осуществляется по mod 4.)

Например, если входной набор $\tilde{a}^n$ схемы S такой, что $f(\tilde{a}^n)=0$, то вероятность появления ошибки на этом наборе равна $P_{f(\tilde{a}^n)\neq 0}(S,\tilde{a}^n) = P_1(S,\tilde{a}^n)+P_2(S,\tilde{a}^n)+P_3(S,\tilde{a}^n)$.

Ненадёжностью схемы S, реализующей функцию $f(\tilde{x}^n)$, будем называть число $P(S)$, равное наибольшей из вероятностей появления ошибки на выходе схемы S. *Надёжность* схемы S равна $1-P(S)$.

Предполагается, что элементы схемы независимо друг от друга с вероятностью $\varepsilon \in (0,1/6)$ подвержены инверсным неисправностям на выходах, т. е. каждый базисный элемент с функцией $\varphi(\tilde{x}^k)$ ($k \in \{1,2\}$) на любом входном наборе $\tilde{a}^k$, таком, что $\varphi(\tilde{a}^k)=\tau$, с вероятностью ε выдаёт значение $(\tau+1) \bmod 4$, с вероятностью ε — значение $(\tau+2) \bmod 4$ и с той же вероятностью — значение $(\tau+3) \bmod 4$. Очевидно, что ненадёжность любого базисного элемента равна 3ε, а надёжность равна $1-3\varepsilon$.

Обозначим через $K(n)$ множество таких функций четырёхзначной логики, зависящих от переменных $x_1,\ldots,x_n$ ($n \geqslant 3$), что каждая из этих функций принимает все четыре значения $0,1,2,3$ и не представима ни в виде $x_k \vee h(\tilde{x}^n)$, ни в виде $x_k \& h(\tilde{x}^n)$ ($k \in \{1,2,\ldots,n\}$, $h(\tilde{x}^n)$ — произвольная функция четырёхзначной логики). Пусть $K = \bigcup\limits_{n=3}^{\infty} K(n)$.

Теорема 1. $|K(n)| \geqslant 4^{4^n} - 2n4^{3\cdot 4^{n-1}} - 4\cdot 3^{4^n}$.

Доказательство проводится с использованием представления функции из класса $K(n)$ в совершенной ДНФ.

Из теоремы 1 следует, что класс $K(n)$ содержит почти все функции четырёхзначной логики из $P_4(n)$, поскольку

$$\lim_{n\to\infty} \frac{2n4^{3\cdot 4^{n-1}} + 4\cdot 3^{4^n}}{4^{4^n}} = 0.$$

Справедлива теорема о нижней оценке ненадёжности схем, реализующих функции из класса K.

Теорема 2. Пусть функция $f \in K$. Тогда для любой схемы S, реализующей f, при $\varepsilon \in (0,1/1000]$ верно неравенство $P(S) \geqslant 9\varepsilon - 33\varepsilon^2 + 36\varepsilon^3$.

Из теоремы 2 следует, что любая схема, реализующая функцию $f \in K$, функционирует с ненадёжностью, которая асимптотически (при $\varepsilon \to 0$) не меньше 9ε.

Таким образом, функцию из класса K (содержащего почти все функции из P_4) нельзя реализовать схемой с ненадёжностью, асимптотически (при $\varepsilon \to 0$) меньше 9ε.

ЛИТЕРАТУРА

1. *Виноградов Ю. А.* О синтезе трехзначных МДП-схем // Математические вопросы кибернетики. Вып. 3. М.: Наука, 1991. С. 187–198.
2. *Виноградов Ю. А.* О синтезе четырехзначных квазикомплементарных МОП-схем // Математические вопросы кибернетики. Вып. 8. М.: Наука, 1999. С. 298–300.
3. *Барсукова О. Ю.* Синтез надежных схем, реализующих функции двузначной и трехзначной логик: дис. ... канд. физ.-мат. наук. Пенза, 2014. 87 с.
4. *Алехина М. А., Барсукова О. Ю.* Ненадёжность схем в базисе Россера — Туркетта // Прикладная дискретная математика. Приложение. 2014. № 7. С. 109–110.

УДК 519.71 DOI 10.17223/2226308X/8/40

ВЕРХНЯЯ ОЦЕНКА НЕНАДЁЖНОСТИ НЕВЕТВЯЩИХСЯ ПРОГРАММ С НЕНАДЁЖНЫМ СТОП-ОПЕРАТОРОМ[1]

С. М. Грабовская

Рассматривается реализация булевых функций неветвящимися программами с оператором условной остановки в произвольном полном конечном базисе. Предполагается, что вычислительные операторы программы с вероятностью $\varepsilon \in \in (0, 1/2)$ подвержены однотипным константным неисправностям на выходах, а стоп-операторы — с вероятностями $\delta \in (0, 1/2)$ и $\eta \in (0, 1/2)$ неисправностям 1-го и 2-го рода соответственно. Найдены верхние оценки ненадёжности неветвящихся программ во всевозможных полных конечных базисах.

Ключевые слова: *булева функция, неветвящаяся программа, оператор условной остановки, надёжность, константные неисправности.*

Программы с оператором условной остановки [1] характеризуются наличием управляющей команды — команды условной остановки, дающей возможность досрочного прекращения работы программы при выполнении определённого условия, а именно при поступлении единицы на вход оператора условной остановки (который ещё называют стоп-оператором).

Будем считать, что все вычислительные операторы независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$ подвержены константным неисправностям либо типа 0, либо типа 1 на выходах [2]. Константные неисправности типа 0 (типа 1) характеризуются тем, что в исправном состоянии вычислительный оператор реализует приписанную ему булеву функцию φ, а в неисправном — функцию 0 (функцию 1).

Предполагается, что операторы условной остановки ненадёжны и независимо друг от друга подвержены неисправностям двух типов: первого и второго рода [3]. Неисправность первого рода характеризуется тем, что при поступлении единицы на вход стоп-оператора он с вероятностью $\delta \in (0, 1/2)$ не срабатывает и, следовательно, работа программы продолжается. Неисправность второго рода такова, что при поступлении нуля на вход стоп-оператора он с вероятностью $\eta \in (0, 1/2)$ срабатывает и, следовательно, работа программы прекращается. Обозначим $\mu = \max\{\varepsilon, \delta, \eta\}$.

Замечание 1. Заметим, что схему из функциональных элементов (ФЭ) [2] можно считать частным случаем неветвящихся программ, а именно неветвящейся программой, в которой нет стоп-операторов.

Определение 1. Ненадёжностью $N_\mu(Pr)$ программы Pr назовём максимальную вероятность ошибки на выходе программы Pr при всевозможных входных наборах.

Надёжность программы Pr равна $1 - N_\mu(Pr)$.

Определение 2. Особенной функцией называется функция вида $x_1x_2 \oplus x_2x_3 \oplus \oplus x_1x_3 \oplus \beta_1x_1 \oplus \beta_2x_2 \oplus \beta_3x_3 \oplus \beta_0$ ($\beta_i \in \{0, 1\}$, $i = 0, 1, 2, 3$).

Известно [4], что из всякой нелинейной функции от трёх или более переменных отождествлением и/или переименованием переменных можно получить либо некоторую нелинейную функцию двух переменных $\phi(x_1, x_2) = x_1x_2 \oplus \alpha_1x_1 \oplus \alpha_2x_2 \oplus \alpha_0$, либо некоторую особенную функцию $\varphi(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus \beta_1x_1 \oplus \beta_2x_2 \oplus \beta_3x_3 \oplus \beta_0$,

[1]Работа поддержана грантом РФФИ, проект № 14-01-31360.

где $\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, \beta_2, \beta_3 \in \{0, 1\}$. Поскольку в любом полном конечном базисе содержится нелинейная функция, далее без ограничения общности будем считать, что рассматриваемый полный базис B содержит либо нелинейную функцию двух переменных, либо особенную функцию.

Для нелинейной функции двух переменных $(x_1^{\alpha_1} \& x_2^{\alpha_2})^{\alpha_3}$ $(\alpha_1, \alpha_2, \alpha_3 \in \{0, 1\})$ возможны два случая: 1) $\alpha_3 = 0$, тогда функция принимает вид $x_1^{\bar{\alpha_1}} \vee x_2^{\bar{\alpha_2}}$, и будем называть её обобщённой дизъюнкцией; 2) $\alpha_3 = 1$, в этом случае функция принимает вид $x_1^{\alpha_1} \& x_2^{\alpha_2}$, будем называть её обобщённой конъюнкцией.

Таким образом, рассмотрим три вида базисов, содержащих 1) особенную функцию; 2) обобщённую дизъюнкцию; 3) обобщённую конъюнкцию. Получены следующие результаты.

1. Пусть полный конечный базис B содержит особенную функцию.

Теорема 1. В полном конечном базисе, содержащем особенную функцию, любую булеву функцию f можно реализовать такой неветвящейся программой Pr_f при однотипных константных неисправностях на выходах вычислительных операторов, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство $N_\mu(Pr_f) \leqslant \max\{\varepsilon, \eta\} + 68\mu^2$.

2. Пусть полный конечный базис содержит обобщённую дизъюнкцию. Здесь возможны два варианта: вычислительные операторы подвержены константным неисправностям на выходах либо типа 0, либо типа 1.

Теорема 2. В полном конечном базисе, содержащем обобщённую дизъюнкцию, любую булеву функцию f можно реализовать такой неветвящейся программой Pr_f при константных неисправностях типа 0 на выходах вычислительных операторов, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство $N_\mu(Pr_f) \leqslant \varepsilon + 78\mu^2$.

Теорема 3. В полном конечном базисе, содержащем обобщённую дизъюнкцию, любую булеву функцию f можно реализовать такой неветвящейся программой Pr_f при константных неисправностях типа 1 на выходах вычислительных операторов, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство $N_\mu(Pr_f) \leqslant 80\mu^2$.

3. Пусть полный конечный базис содержит обобщённую конъюнкцию. Так же, как и в предыдущем случае, рассмотрим два варианта: вычислительные операторы подвержены константным неисправностям типа 0 либо типа 1 на выходах.

Теорема 4. В полном конечном базисе, содержащем обобщённую конъюнкцию, любую булеву функцию f можно реализовать такой неветвящейся программой Pr_f при константных неисправностях типа 0 на выходах вычислительных операторов, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство $N_\mu(Pr_f) \leqslant 80\mu^2$.

Теорема 5. В полном конечном базисе, содержащем обобщённую конъюнкцию, любую булеву функцию f можно реализовать такой неветвящейся программой Pr_f при константных неисправностях типа 1 на выходах вычислительных операторов, что при всех $\varepsilon \in (0, 1/960]$ справедливо неравенство $N_\mu(Pr_f) \leqslant \varepsilon + 78\mu^2$.

Таким образом, в произвольном полном конечном базисе верхняя оценка ненадёжности неветвящихся программ при однотипных константных неисправностях на выходах вычислительных операторов составляет $\max\{\varepsilon, \eta\} + 78\mu^2$ для всех $\varepsilon \in (0, 1/960]$ и $\mu = \max\{\varepsilon, \delta, \eta\}$. Однако в некоторых случаях эта оценка может быть существенно улучшена. Например, в базисе, содержащем обобщённую дизъюнкцию (конъюнкцию),

любую булеву функцию можно реализовать неветвящейся программой при константных неисправностях типа 1 (0) на выходах вычислительных операторов с ненадёжностью не больше $80\mu^2$ при всех $\varepsilon \in (0, 1/960]$.

В качестве сравнения, для схем из ФЭ известно [2], что в произвольном полном конечном базисе любую булеву функцию f можно реализовать схемой из ФЭ при тех же типах неисправностей с ненадёжностью не больше $3\varepsilon + 100\varepsilon^2$ при всех $\varepsilon \in$ $\in (0, 1/960]$. Однако в некоторых базисах данную верхнюю оценку можно улучшить. Например, в базисе $\{x_1 \vee x_2, \bar{x}_1\}$ она составляет $2\varepsilon + 42\varepsilon^2$ при всех $\varepsilon \in (0, 1/140]$; в базисе $\{x_1 \& \bar{x}_2, x_1 \sim x_2\}$ имеем $\varepsilon + 6\varepsilon^2$ при всех $\varepsilon \in (0, 1/320]$. Заметим, что для неветвящихся программ без стоп-операторов (см. замечание 1) $\delta = \eta = 0$, следовательно, $\mu = \varepsilon$. Тогда верхняя оценка ненадёжности таких программ составляет $\varepsilon + 78\varepsilon^2$ при всех $\varepsilon \in (0, 1/960]$, а в некоторых базисах $80\varepsilon^2$, что в общем случае лучше, чем для схем из ФЭ.

ЛИТЕРАТУРА

1. *Чашкин А. В.* О среднем времени вычисления значений булевых функций // Дискретный анализ и исследование операций. 1997. Т. 4. № 1. С. 60–78.
2. *Алехина М. А.* Синтез асимптотически оптимальных по надежности схем из ненадежных элементов. Пенза: ИИЦ ПГУ, 2006.
3. *Алехина М. А., Грабовская С. М.* Асимптотически оптимальные по надежности неветвящиеся программы с оператором условной остановки. Пенза: ИИЦ ПГУ, 2013.
4. *Редькин Н. П.* О полных проверяющих тестах для схем из функциональных элементов // Математические вопросы кибернетики. 1989. Вып. 2. С. 198–222.

УДК 519.718 DOI 10.17223/2226308X/8/41

О ДЛИНЕ, ВЫСОТЕ И НАДЁЖНОСТИ СХЕМ, РЕАЛИЗУЮЩИХ ФУНКЦИИ ВЫБОРА v_{2i}[1]

А. В. Рыбаков

Рассматриваются клеточные (плоские) схемы, реализующие функции выбора v_{2i}. Предполагается, что коммутационные элементы абсолютно надёжны, а функциональные подвержены инверсным неисправностям на выходах, причём переходят в неисправные состояния независимо друг от друга. Найдены соотношения для длины и высоты, а также получена оценка ненадёжности таких схем.

Ключевые слова: *булевы функции, клеточные (плоские) схемы, инверсные неисправности функциональных элементов, ненадёжность схемы, функция выбора.*

Впервые задачу синтеза надёжных схем из ненадёжных функциональных элементов рассматривал Дж. фон Нейман. Он предполагал, что все элементы схемы независимо друг от друга с вероятностью $\varepsilon \in (0; 1/2)$ подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию ϕ, а в неисправном — функцию $\overline{\phi}$. С помощью итерационного метода Дж. фон Нейман установил [1], что в произвольном полном базисе при $\varepsilon \in (0; 1/6]$ любую булеву функцию можно реализовать схемой, вероятность ошибки, на выходе которой при любом

[1]Работа поддержана грантом РФФИ, проект № 14-01-31360.

входном наборе значений переменных не превосходит $c\varepsilon$ (c — некоторая положительная константа, зависящая от базиса). Затем схемы с инверсными неисправностями на выходах элементов исследовались в работах [2, 3] и некоторых других, причём главное внимание уделялось сложности надёжных схем.

Асимптотически оптимальные по надёжности схемы из функциональных элементов, реализующие булевы функции, в базисе $\{x_1\&x_2, x_1 \vee x_2, \bar{x}_1\}$ при инверсных неисправностях на выходах элементов построены в работе [4], а в [5] доказано, что сложность таких схем превышает сложность схем, построенных из абсолютно надёжных элементов, асимптотически не более чем в 3 раза.

В работе [6] впервые предложен класс клеточных схем (КС; ещё их называют плоскими схемами). В [7] получены оценки сложности КС в предположении, что все элементы схемы абсолютно надёжны, а в [8] рассмотрена задача построения клеточных схем из надёжных коммутационных и ненадёжных функциональных элементов, реализующих произвольные булевы функции, и получены оценки ненадёжности и сложности таких схем.

В данной работе рассматриваются клеточные схемы, реализующие функции специального класса, называемые функциями выбора:

$$v_{2i}(x_1, x_2, \ldots, x_{2i}, y_0, y_1, \ldots, y_{2^{2i}-1}) = \bigvee_{\widetilde{\sigma}} K_{\widetilde{\sigma}}(\widetilde{x}) y_{|\widetilde{\sigma}|},$$

где $\widetilde{\sigma} = (\sigma_1, \ldots, \sigma_{2i})$; $K_{\widetilde{\sigma}}(\widetilde{x}) = x_1^{\sigma_1} \ldots x_{2i}^{\sigma_{2i}}$; $|\widetilde{\sigma}| = \sum\limits_{j=1}^{2i} \sigma_i 2^{2i-j}$ (т. е. $|\widetilde{\sigma}|$ — число, двоичной записью которого является набор $\widetilde{\sigma}$). Поскольку $K_{\widetilde{\sigma}}(\widetilde{\alpha})$ обращается в нуль при $\widetilde{\sigma} \neq \widetilde{\alpha}$ и в единицу при $\widetilde{\sigma} = \widetilde{\alpha}$, то при подстановке $\alpha_1, \ldots, \alpha_{2i}$ вместо переменных $x_1, \ldots, x_{2i}$ в функцию выбора $v_{2i}(\widetilde{x}, \widetilde{y})$ эта функция обращается в $y_{|\widetilde{\alpha}|}$.

Схемы этих функций используются при построении схем, обладающих достаточно высокой надёжностью.

Как и в [6], предполагается, что базис содержит два типа элементов: функциональные и коммутационные. Каждый из этих элементов может быть повёрнут на плоскости на угол $k\pi/2$ ($k = 0, 1, 2, 3$). Предполагается, что коммутационные элементы абсолютно надёжны, а на любом из двух выходов каждого из функциональных элементов с вероятностью $\varepsilon \in (0; 1/2)$ независимым образом появляются инверсные неисправности. Считаем, что КС, содержащая ненадёжные элементы, реализует булеву функцию $f(\tilde{x}^n)$ ($\tilde{x}^n = (x_1, \ldots, x_n)$), если она реализует $f(\tilde{x}^n)$ при отсутствии неисправностей. Пусть КС S реализует функцию $f(\tilde{x}^n)$. Обозначим через $P_{\overline{f(\tilde{a}^n)}}(S, \tilde{a}^n)$ вероятность появления ошибки на входном наборе $\tilde{a}^n$ схемы S. Ненадёжность $P(S)$ клеточной схемы S определяется как максимальная вероятность ошибки на выходе схемы при всевозможных входных наборах схемы (т. е. так же, как и для схемы из функциональных элементов). Надёжность схемы S равна $1 - P(S)$.

Обозначим $l(S)$ длину клеточной схемы S, $h(S)$ — её высоту. Тогда сложность $L(S)$ клеточной схемы равна её площади ($L(S) = l(S)h(S)$) и числу элементов в ней.

Возьмём три экземпляра схемы S и соединим их выходы со входами схемы, реализующей функцию голосования $x_1x_2 \vee x_1x_3 \vee x_2x_3$. Построенную схему обозначим $\psi(S)$. Схема $\psi(S)$ используется для повышения надёжности исходных схем.

Теорема 1. Функция выбора $v_2(x_1, x_2, y_0, y_1, y_2, y_3)$ может быть реализована схемой V_2 длины $l = 6$ и высоты $h = 10$.

Теорема 2. Функцию выбора v_{2i} можно реализовать схемой, длина которой $l(V_{2i}) = 7 \cdot 2^{2(i-1)} + 2i - 3$, а высота $h(V_{2i}) = h(V_{2(i-1)}) + 4 + 2i + 2^{2(i-1)}$, где $h(V_{2(i-1)})$ — высота схемы $V_{2(i-1)}$, реализующей функцию выбора $v_{2(i-1)}$.

Для длины, ширины и ненадёжности схемы $\psi(V_{2i})$, реализующей функцию выбора v_{2i}, справедливы следующие соотношения.

Теорема 3. $l(\psi(V_{2i})) = 21 \cdot 2^{2(i-1)} + 6i - 2$, $h(\psi(V_{2i})) = 2^{2i}/3 + 2i^2 + 13i - 13/3$, $P(\psi(V_{2i})) \leqslant 8\varepsilon$, $\varepsilon \in (0; 1/200]$.

Заметим, что нетрудно найти сложность схемы $\psi(V_{2i})$ из теоремы 3 (для этого достаточно умножить длину на ширину).

ЛИТЕРАТУРА

1. *Von Neuman J.* Probabilistic logics and the synthesis of reliable organisms from unreliable components // Automata Studies. C. Shannon, J. Mc. Carthy (eds). Princeton University Press, 1956. (Рус. пер.: Автоматы. М.: ИЛ, 1956. С. 68–139.)
2. *Ортюков С. И.* Об избыточности реализации булевых функций схемами из ненадежных элементов // Труды семинара по дискретной математике и её приложениям (Москва, 27–29 января 1987 г.). М.: Изд-во МГУ, 1989. С. 166–168.
3. *Uhlig D.* Reliable networks from unreliable gates with almost minimal complexity // LNCS. 1987. V. 278. P. 462–469.
4. *Васин А. В.* Об асимптотически оптимальных схемах в базисе $\{\&, \vee, \neg\}$ при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. 2008. № 4. С. 3–17.
5. *Алехина М. А., Аксенов С. И.* О сложности надежных схем при инверсных неисправностях // Материалы IX Междунар. семинара «Дискретная математика и её приложения», посвящённого 75-летию со дня рождения О. Б. Лупанова (Москва, 18–23 июня 2007 г.). М.: Изд-во мех.-мат. фак-та МГУ, 2007. С. 56–59.
6. *Кравцов С. С.* О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. 1967. Вып. 19. С. 285–292.
7. *Улесова А. Ю.* Сложность реализации булевых функций в некоторых моделях клеточных схем: дипломная работа. М.: МГУ им. Ломоносова, фак-т ВМиК, каф. математической кибернетики, 2010.
8. *Рыбаков А. В.* Сложность асимптотически оптимальных по надежности клеточных схем // Сб. статей XVIII Междунар. науч.-методич. конф. «Университетское образование (МКУО-2014)», Пенза, 10–11 апреля 2014 г. Пенза: Изд-во Пенз. ун-та, 2014. С. 310–311.

Секция 6

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ, АВТОМАТОВ И ГРАФОВ

УДК 519.17 DOI 10.17223/2226308X/8/42

О ТОЧНЫХ ОЦЕНКАХ ЧИСЛА ДОПОЛНИТЕЛЬНЫХ ДУГ МИНИМАЛЬНОГО ВЕРШИННОГО 1-РАСШИРЕНИЯ ТУРНИРА

М. Б. Абросимов, О. В. Моденова

Получены нижняя и верхняя оценки для числа дополнительных дуг минимального вершинного 1-расширения произвольного турнира. Показывается, что оценки являются точными, и описываются турниры, для которых оценки достигаются.

Ключевые слова: *турнир, минимальное вершинное расширение, отказоустойчивость.*

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным вершинным k-расширением* (k — натуральное, в данной работе $k = 1$) n-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1) G^* является вершинным k-расширением G, то есть граф G вкладывается в каждый подграф графа G^*, получающийся удалением любых его k вершин;
2) G^* содержит $n + k$ вершин, то есть $|V^*| = |V| + k$;
3) α^* имеет минимальную мощность при выполнении условий 1 и 2.

Понятие минимального вершинного k-расширения введено на основе понятия оптимальной k-отказоустойчивой реализации, которое предложено Хейзом в [1] при построении модели отказоустойчивости, основанной на графах. Основные определения используются согласно [2].

Через $ec(G)$ обозначим количество дополнительных рёбер (дуг) в минимальном вершинном 1-расширении графа G по сравнению с самим графом G.

В работе [3] доказываются некоторые результаты о связи между минимальными вершинными k-расширениями неориентированных и ориентированных графов.

Лемма. Пусть орграф G^* есть минимальное вершинное k-расширение орграфа G. Тогда симметризация орграфа G^* является вершинным k-расширением симметризации орграфа G.

Следствие. Число дополнительных дуг минимального вершинного k-расширения орграфа G не меньше числа дополнительных рёбер минимального вершинного k-расширения симметризации орграфа G.

Легко убедиться, что единственным минимальным вершинным 1-расширением графа K_n является граф K_{n+1}, причём $ec(K_n) = n$.

Нижняя оценка

Граф $G^* = (V^*, \alpha^*)$ называется *точным вершинным k-расширением* n-вершинного графа $G = (V, \alpha)$, если граф G изоморфен каждому подграфу графа G^*, получающемуся из графа G^* путём удаления любых его k вершин и всех связанных с ними дуг (рёбер).

Можно заметить, что минимальное вершинное 1-расширение графа K_n является и его точным вершинным 1-расширением.

Если ориентировать каждое ребро полного графа K_n, то получим некоторый турнир $\overrightarrow{T}_n$. Согласно следствию можно сделать следующий вывод:

$$ec(\overrightarrow{T}_n) \geqslant n,$$

то есть число дополнительных дуг минимального вершинного 1-расширения произвольного турнира $\overrightarrow{T}_n$ не может быть меньше n, причём в этом случае минимальное вершинное 1-расширение является и точным вершинным 1-расширением. Такие турниры существуют, например транзитивные, вершинно-симметрические и некоторые другие [4], и относительно хорошо изучены. Большинство турниров не имеют точного вершинного 1-расширения, поэтому для них

$$ec(\overrightarrow{T}_n) > n.$$

Удалось доказать, что не существует турниров с числом дополнительных дуг в минимальном вершинном 1-расширении равном $n + 1$.

Теорема 1. Если минимальное вершинное 1-расширение турнира $\overrightarrow{T}_n$ не является его точным вершинным 1-расширением, то справедливо неравенство

$$ec(\overrightarrow{T}_n) > n + 1.$$

Данная оценка является достижимой.

Теорема 2. Турнир, получающийся из транзитивного заменой ориентации одной дуги из источника в сток, имеет минимальное вершинное 1-расширение с $(n + 2)$ дополнительными дугами.

Верхняя оценка

Граф $G_t = (V_t, \alpha_t)$ называется *тривиальным k-расширением* графа $G = (V, \alpha)$, если G_t получается из G добавлением k вершин, соединением их со всеми вершинами графа G и друг с другом. Граф G_t можно представить как соединение G и полного графа $K_k = (V_k, \alpha_k)$: $G_t = (V_t, \alpha_t) = (V \cup Vk, \alpha \cup \alpha_k \cup V \times V_k \cup V_k \times V)$. Очевидно, что тривиальное k-расширение графа является и его вершинным k-расширением, что позволяет получить общую верхнюю оценку для числа дополнительных дуг произвольного орграфа:

$$ec(\overrightarrow{T}_n) \leqslant 2n.$$

Оказалось, что для турниров эта оценка является достижимой.

Теорема 3. Турнир с числом вершин $n = 4k + 2$, все вершины которого имеют степени $(3k + 1, k)$ или $(k, 3k + 1)$, имеет минимальное вершинное 1-расширение с $2n$ дополнительными дугами.

Таким образом, получается общий результат.

Теорема 4. Если минимальное вершинное 1-расширение турнира $\overrightarrow{T}_n$ не является его точным вершинным 1-расширением, то справедливо неравенство

$$n + 2 \leqslant ec(\overrightarrow{T}_n) \leqslant 2n,$$

причём верхняя и нижняя оценки являются достижимыми.

ЛИТЕРАТУРА

1. *Hayes J. P.* A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. C25. No. 9. P. 875–884.
2. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192 с.
3. *Абросимов М. Б.* Минимальные вершинные расширения направленных звезд // Дискретная математика. 2011. Т. 23. № 2. С. 93–102.
4. *Абросимов М. Б., Долгов А. А.* Семейства точных расширений турниров // Прикладная дискретная математика. 2008. № 1. С. 101–107.

УДК 519.6 DOI 10.17223/2226308X/8/43

УСЛОВИЯ ПРИМИТИВНОСТИ СИСТЕМЫ ДВУХ ГРАФОВ

Я. Э. Авезова, В. М. Фомичев

Получены достаточные условия примитивности системы двух n-вершинных орграфов в случае, когда один из орграфов не содержит ациклических вершин, в частности, когда содержит гамильтонов контур. Получена оценка экспонента системы двух орграфов через экспонент их произведения. Результаты могут быть использованы для оценки перемешивающих свойств итеративных функций, построенных на основе разветвления преобразования на два заданных преобразования.

Ключевые слова: *примитивный граф, экспонент графа, гамильтонов цикл.*

Пусть $S = \{A, B\}$ — система двух неотрицательных матриц порядка n. Получим условия, при которых система S является примитивной. По определению система S примитивная, если мультипликативная полугруппа $\langle A, B\rangle$ содержит положительную матрицу. Длина наименьшего слова в алфавите S, соответствующего положительной матрице, называется экспонентом системы S, обозначается $\exp S$. Далее слово $w = C_1 \cdot \ldots \cdot C_l$ в алфавите S (то есть $C_i \in S$, $i = 1, \ldots, l$) отождествляется с матрицей, равной произведению $C_1 \cdot \ldots \cdot C_l$.

Один из способов получения оценки $\exp S$ состоит в построении примитивного слова w. Если длина слова w равна l, то $\exp S \leqslant l \cdot \exp w$. Получим условия на матрицы A и B, при которых слово AB примитивное. Воспользуемся аппаратом теории графов, что при исследовании примитивности равносильно. Если Γ_1 есть часть графа Γ_2, то обозначим это $\Gamma_1 \leqslant \Gamma_2$.

Обозначим $\Gamma(A)$ n-вершинный орграф с матрицей смежности A. Пусть орграф $\Gamma(A)$ не содержит ациклических вершин, то есть состоит из k непересекающихся компонент сильной связности, $1 \leqslant k \leqslant n$.

Лемма 1. Если $\Gamma(B)$ имеет петли в каждой вершине, то $\Gamma(A) \leqslant \Gamma(AB)$.

Следствие 1. В условиях леммы множество простых контуров орграфа $\Gamma(AB)$ содержит все простые контуры орграфа $\Gamma(A)$.

Для орграфа $\Gamma(A)$, не содержащего ациклических вершин, построим k-вершинный орграф $\Gamma_A(B)$ с помощью отождествления некоторых вершин орграфа $\Gamma(B)$: вершины i и j орграфа $\Gamma(B)$ отождествляются, если и только если эти вершины принадлежат одной компоненте сильной связности орграфа $\Gamma(A)$.

Лемма 2. Если орграф $\Gamma_A(B)$ сильносвязный, то орграф $\Gamma(AB)$ тоже сильносвязный.

В соответствии с универсальным критерием примитивности [1], орграф Γ примитивный, если и только если Γ сильносвязный и длины его простых контуров взаимно просты. Используя универсальный критерий, получим достаточные условия примитивности орграфа $\Gamma(AB)$.

Теорема 1. Пусть орграф $\Gamma(A)$ содержит контуры длин $l_1, \ldots, l_k$, $(l_1, \ldots, l_k) = 1$, орграф $\Gamma(B)$ имеет петли в каждой вершине, орграф $\Gamma_A(B)$ сильносвязный. Тогда орграф $\Gamma(AB)$ примитивный и $\exp S \leqslant 2\exp(AB)$.

Пусть орграф $\Gamma(A)$ гамильтонов. Не ограничивая общности, положим, что полный цикл есть $(1, 2, \ldots, n)$. Тогда в орграфе $\Gamma(B)$ вершине i с полустепенью исхода q_i соответствует множество дуг $\{(i, b_{i,1}), \ldots, (i, b_{i,q_i})\}$, $i = 1, \ldots, n$. Обозначим

$$d_B = \text{НОД}(\rho(i, b_{i,j})\colon i = 1, \ldots, n, j = 1, \ldots, q_i),$$

где $\rho(i, j) = i - j$, если $i \geqslant j$, и $\rho(i, j) = n + i - j$, если $i < j$.

Теорема 2. Пусть орграф $\Gamma(A)$ содержит гамильтонов цикл $(1, 2, \ldots, n)$, орграф $\Gamma(B)$ имеет петли в каждой вершине и $(n, d_B) = 1$. Тогда орграф $\Gamma(AB)$ примитивный и $\exp S \leqslant 2\exp(AB)$.

Пример 1. На рис. 1 иллюстрируется теорема 1 для матриц порядка 6 (6-вершинных графов). При отождествлении вершинам $1, 2, 3$ орграфов $\Gamma(A)$ и $\Gamma(B)$ соответствует вершина α в $\Gamma_A(B)$, вершинам $4, 5$ — вершина β, вершине 6 — вершина γ.

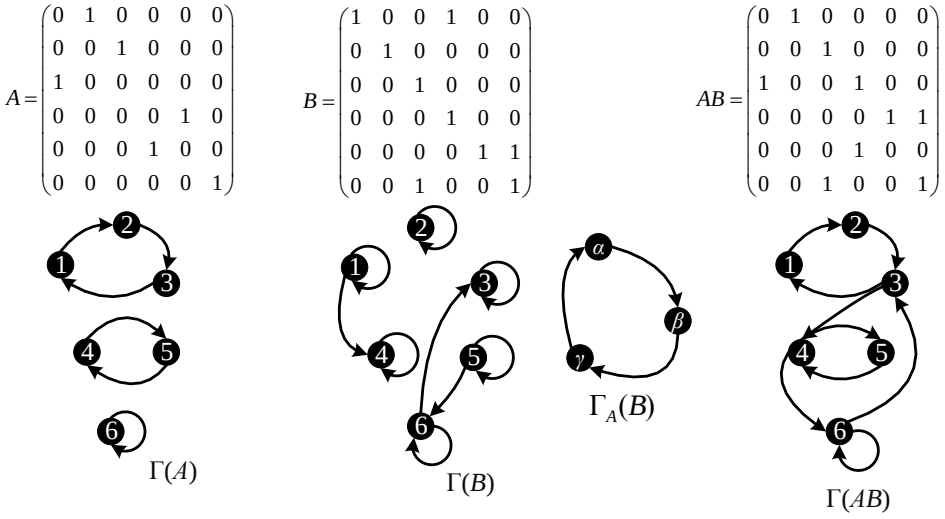

Рис. 1. Пример, иллюстрирующий теорему 1

Полученные результаты могут быть использованы для оценки перемешивающих свойств итеративных функций, построенных на основе разветвления преобразования на два заданных преобразования [2].

ЛИТЕРАТУРА

1. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 116–121.
2. *Когос К. Г., Фомичев В. М.* О разветвлениях криптографических функций на преобразования с заданным признаком // Прикладная дискретная математика. 2012. № 1(15). С. 50–54.

УДК 519.1 DOI 10.17223/2226308X/8/44

О КОЛИЧЕСТВЕ НЕДОСТИЖИМЫХ СОСТОЯНИЙ В КОНЕЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ ДВОИЧНЫХ ВЕКТОРОВ, АССОЦИИРОВАННЫХ С ОРИЕНТАЦИЯМИ ПАЛЬМ

А. В. Жаркова

Рассматриваются конечные динамические системы двоичных векторов, ассоциированных с ориентациями пальм. Данной системе изоморфна конечная динамическая система (B^{s+c}, γ), $s > 0$, $c > 1$, состояниями которой являются все возможные двоичные векторы размерности $s + c$. Приведена формула для подсчёта количества недостижимых состояний в рассматриваемых динамических системах, представлена соответствующая таблица для систем (B^{8+c}, γ), $1 < c < 9$.

Ключевые слова: *конечная динамическая система, недостижимое состояние, пальма, сверхстройное (звездообразное) дерево.*

Под *конечной динамической системой* понимается пара (S, δ), где S — конечное непустое множество, элементы которого называются *состояниями системы*; $\delta : S \to S$ — отображение множества состояний в себя, называемое *эволюционной функцией системы*. Каждой конечной динамической системе сопоставляется карта, представляющая собой орграф с множеством вершин S и дугами, проведёнными из каждой вершины $s \in S$ в вершину $\delta(s)$. Компоненты связности графа, задающего динамическую систему, называются её *бассейнами*. Каждый бассейн представляет собой контур с входящими в него деревьями. Контуры называются предельными циклами, или *аттракторами*.

Основными проблемами теории конечных динамических систем являются задачи отыскания эволюционных параметров без проведения динамики. К их числу относятся *ветвление* (количество непосредственных предшественников данного состояния) и, в частности, свойство *недостижимости* состояния (то есть когда состояние имеет нулевое ветвление). Автором составлены программы для ЭВМ, позволяющие вычислять различные параметры динамических систем двоичных векторов, ассоциированных с некоторыми типами графов [1], описаны недостижимые состояния конечных динамических систем двоичных векторов, ассоциированных с графами [2], подсчитаны количества недостижимых состояний в системах, связанных с ориентациями цепей и циклов [3].

Дерево называется *пальмой*, если оно является объединением цепей, имеющих общую концевую вершину, причём все эти цепи, за исключением, быть может, одной, имеют длину 1. Пальма является частным случаем *сверхстройного (звездообразного) дерева* (дерево, в котором в точности одна вершина имеет степень больше 2).

Пусть пальма p образована объединением цепей $p_0, p_1, \ldots, p_c$, имеющих общую концевую вершину. Будем считать, что p_0 имеет среди этих цепей максимальную длину $s \geqslant 1$. Назовём p_0 *стволом пальмы* p, цепи $p_1, p_2, \ldots, p_c$, имеющие длину 1, — её *листьями*, а их совокупность — *кроной*. Будем говорить, что p является пальмой типа (s, c). Пальма с точностью до изоморфизма определяется своим типом. При $c = 1$ пальма вырождается в цепь (см., например, [3, 4]), поэтому далее полагаем $c > 1$.

Пусть имеется пальма p типа (s, c), $s + c = n$. Зафиксируем расположение её цепей и перенумеруем рёбра пальмы p, начиная от корня (начальной вершины ствола), двигаясь к кроне (рёбра с номерами от 1 по s), а далее рёбра кроны слева направо (рёбра с номерами от $s + 1$ до $s + c$). Придадим каждому ребру пальмы произвольную ори-

ентацию и сопоставим полученному ориентированному графу p n-мерный двоичный вектор $v(p)$, полагая его i-ю компоненту равной 1, если i-е ребро пальмы p ориентировано от корня, и 0 — в противном случае. Теперь можно последовательно выписать получившуюся последовательность из нулей и единиц: $v = v_1 \dots v_s.v_{s+1} \dots v_{s+c}$, где v_i, $0 < i \leqslant s+c$, принимает значение 0 или 1 в зависимости от ориентации i-го ребра пальмы. Таким образом, каждой ориентации пальмы сопоставляется n-мерный двоичный вектор, причём $n = s+c$. В свою очередь, каждый такой вектор $v = v_1 \dots v_s.v_{s+1} \dots v_{s+c}$ однозначно определяет некоторую ориентацию пальмы $p(v)$ типа (s, c). Таким образом, между множеством P_{s+c}, $s > 0$, $c > 1$, всех возможных ориентированных пальм типа (s, c) указанного вида и множеством B^{s+c}, $s > 0$, $c > 1$, всех двоичных векторов размерности $n = s + c$ устанавливается взаимно однозначное соответствие. В дальнейшем ориентации пальмы для простоты также будем называть пальмами.

Опишем конечную динамическую систему ориентаций (s, c)-пальмы p на языке двоичных векторов. Пусть состоянием динамической системы в данный момент времени является вектор $v = v_1 \dots v_s.v_{s+1} \dots v_{s+c} \in B^{s+c}$. Тогда в следующий момент времени она окажется в состоянии $\gamma(v) = v'$, полученном путём одновременного применения следующих правил:

1) если $v_1 = 0$, то $v'_1 = 1$;
2) если $v_i = 1$ и $v_{i+1} = 0$ для некоторого i, $0 < i < s$, то $v'_i = 0$ и $v'_{i+1} = 1$;
3) если $v_i = 1$ для некоторого i, $s < i \leqslant s + c$, то $v'_i = 0$;
4) если $v_s = 1$ и $v_i = 0$ для всех i, $s < i \leqslant s + c$, то $v'_s = 0$ и $v'_i = 1$ для всех i, $s < i \leqslant s + c$;
5) других отличий между v и $\gamma(v)$ нет.

Пусть теперь имеется n-рёберная (s, c)-пальма. На языке ориентаций пальм эволюция динамической системы вводится следующим образом: если дана некоторая ориентированная пальма $p \in P_{s+c}$, то её динамическим образом $\gamma(p)$ является пальма, получаемая из p одновременным превращением всех стоков в источники. Это частный случай динамики бесконтурных связных графов, введённой в [5]. Преобразования ориентаций пальм в динамической системе (P_{s+c}, γ), $s > 0$, $c > 1$, соответствуют эволюционным преобразованиям соотносимых им двоичных векторов в динамической системе (B^{s+c}, γ), $s > 0$, $c > 1$, и обратно, а именно $v(\gamma(p)) = \gamma(v(p))$ [6]. Таким образом, динамические системы (B^{s+c}, γ) и (P_{s+c}, γ), $s > 0$, $c > 1$, изоморфны.

Теорема 1. Количество недостижимых состояний в динамической системе (B^{s+c}, γ), $s > 0$, $c > 1$, равно

$$\text{КНС}_{(s+c,\gamma)} = 2^{s+c} - 2^s - 2^{s-3} + \Omega(-1) - 2\Omega(1) + \Omega(3),$$

где

$$\Omega(x) = \sum_{i=1}^{[(s-x)/4]} (-1)^{i+1} \cdot 2^{s-x-4i} \cdot C^i_{s-x-3i},$$

причём если коэффициенты или степени принимают отрицательные значения, то соответствующие выражения принимают значение 0.

С помощью программы для ЭВМ получены данные о количестве недостижимых состояний в динамической системе (B^{s+c}, γ), представленные для $s = 8$ и $1 < c < 9$ в таблице.

c	2	3	4	5	6	7	8
$\text{КНС}_{(8+c,\gamma)}$	862	1 886	3 934	8 030	16 222	32 606	65 374

ЛИТЕРАТУРА

1. *Власова А. В.* Исследование эволюционных параметров в динамических системах двоичных векторов // Свид. о гос. регистрации программы для ЭВМ № 2009614409, выданное Роспатентом. Зарегистрировано в Реестре программ для ЭВМ 20 августа 2009 г.
2. *Жаркова А. В.* О ветвлении и непосредственных предшественниках состояний в конечной динамической системе всех возможных ориентаций графа // Прикладная дискретная математика. Приложение. 2013. № 6. С. 76–78.
3. *Жаркова А. В.* Недостижимые состояния в динамических системах, ассоциированных с цепями и циклами // Изв. Сарат. ун-та. Нов. сер. 2011. Т. 11. Сер. Математика. Механика. Информатика. Вып. 4. С. 116–123.
4. *Салий В. Н.* Об одном классе конечных динамических систем // Вестник Томского государственного университета. Приложение. 2005. № 14. С. 23–26.
5. *Barbosa V. C.* An Atlas of Edge-reversal Dynamics. Boca Raton: Chapman & Hall/CRC, 2001. 385 p.
6. *Власова А. В.* Динамические системы, определяемые пальмами // Компьютерные науки и информационные технологии: Материалы Междунар. науч. конф. Саратов: Изд-во Сарат. ун-та, 2009. С. 57–60.

УДК 519.7 DOI 10.17223/2226308X/8/45

СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ БЕСКОНЕЧНОЙ ДЛИНЫ[1]

С. А. Малюгин

Подмножество C в бесконечномерном двоичном кубе $\{0,1\}^{\mathbb{N}}$ называется совершенным двоичным кодом с расстоянием 3, если все шары единичного радиуса (в метрике Хемминга) с центрами из C попарно не пересекаются и их объединение покрывает куб $\{0,1\}^{\mathbb{N}}$. Аналогичным образом определяется совершенный двоичный код в нулевом слое $\{0,1\}_0^{\mathbb{N}}$, состоящем из всех векторов куба $\{0,1\}^{\mathbb{N}}$, имеющих конечные носители. В работе доказывается, что мощность множества всех классов эквивалентности совершенных двоичных кодов в нулевом слое $\{0,1\}_0^{\mathbb{N}}$ равна континууму, а мощность множества классов эквивалентности совершенных двоичных кодов во всём кубе — гиперконтинууму.

Ключевые слова: *совершенные двоичные коды, код Хемминга, расстояние Хемминга, коды Васильева, классы эквивалентности, континуум, гиперконтинуум.*

1. Основные определения

Пусть $\mathbb{N}$ — множество натуральных чисел. *Бесконечномерный куб* $\{0,1\}^{\mathbb{N}}$ состоит из всевозможных бесконечных последовательностей $u = (u_1, \dots, u_n, \dots)$, где $u_n \in \{0,1\}$; $n \in \mathbb{N}$. Сумма двух элементов $u, v \in \{0,1\}^{\mathbb{N}}$ определяется формулой $u + v = (u_1 \oplus v_1, \dots, u_n \oplus v_n, \dots)$, где $u = (u_1, \dots, u_n, \dots)$, $v = (v_1, \dots, v_n, \dots)$ и $u_n \oplus v_n$ — сумма элементов u_n, v_n в двухэлементном поле Галуа $\mathrm{GF}(2) = \{0,1\}$. Относительно такой операции сложения куб $\{0,1\}^{\mathbb{N}}$ является бесконечномерным векторным пространством над полем $\mathrm{GF}(2)$. Элементы куба $\{0,1\}^{\mathbb{N}}$ далее будем называть векторами. Нулевой вектор обозначаем через $\mathbf{0}$, а базисные векторы с единичной i-й координатой — через $e_i = (0, \dots, 0, \underset{i}{1}, 0, \dots)$. *Носитель* вектора $u \in \{0,1\}^{\mathbb{N}}$ (множество индексов i, для которых $u_i = 1$) обозначается через $[u]$. Число ненулевых координат вектора u называется его *весом* и обозначается через $|u|$. В отличие от конечномерного случая вес может

[1]Работа поддержана грантами РФФИ № 13-01-00463; 14-01-00507.

принимать также значение ∞. *Расстояние Хемминга* между векторами $u, v \in \{0,1\}^{\mathbb{N}}$ определяется как $|u+v|$. Расстояние Хемминга задаёт в пространстве $\{0,1\}^{\mathbb{N}}$ «обобщённую» *метрику Хемминга* со значениями в $\mathbb{N} \cup \{\infty\}$.

Определение 1. Подмножество C в бесконечномерном двоичном кубе $\{0,1\}^{\mathbb{N}}$ называется *совершенным двоичным кодом с расстоянием* 3, если все шары единичного радиуса (в метрике Хемминга) с центрами из C попарно не пересекаются и их объединение покрывает куб $\{0,1\}^{\mathbb{N}}$.

Следует отметить, что изучение кодов бесконечной длины (МДР-кодов, задаваемых квазигруппами с бесконечным числом аргументов) впервые было предпринято В. Н. Потаповым в [1]. Рассмотрим в $\{0,1\}^{\mathbb{N}}$ следующее отношение эквивалентности: $u \sim v \iff |u+v| \neq \infty$ $(u, v \in \{0,1\}^{\mathbb{N}})$. Куб $\{0,1\}^{\mathbb{N}}$ относительно этого отношения разбивается на попарно не пересекающиеся классы эквивалентности, которые далее будем называть *слоями* куба $\{0,1\}^{\mathbb{N}}$. Слой, содержащий нулевой вектор, будем обозначать символом $\{0,1\}_0^{\mathbb{N}}$ и называть его *нулевым слоем*. Он состоит из всех векторов конечного веса (такие векторы будем называть *финитными*). Очевидно, что нулевой слой является подпространством в $\{0,1\}^{\mathbb{N}}$, а любой другой слой $\mathcal{L}$ является смежным классом по этому подпространству. Пусть $\mathcal{L}$ — произвольный слой в кубе $\{0,1\}^{\mathbb{N}}$.

Определение 1′. Подмножество $C \subset \mathcal{L}$ называем совершенным двоичным кодом слоя $\mathcal{L}$, если все шары единичного радиуса с центрами из C попарно не пересекаются и их объединение покрывает слой $\mathcal{L}$.

Легко видеть, что изучение совершенных кодов в кубе $\{0,1\}^{\mathbb{N}}$ фактически сводится к изучению совершенных кодов в нулевом слое $\{0,1\}_0^{\mathbb{N}}$.

Совершенный код в $\{0,1\}_0^{\mathbb{N}}$ называется *кодом Хемминга*, если он является линейным подпространством в $\{0,1\}_0^{\mathbb{N}}$. Код Хемминга H^∞ можно определить следующим образом. Для конечных n код Хемминга H^n длины $n = 2^k - 1$ $(k > 1)$ определяется стандартным образом. Добавляя справа к векторам $u \in H^n$ бесконечное число нулевых координат, можно вложить код H^n в нулевой слой $\{0,1\}_0^{\mathbb{N}}$. Это вложение будем обозначать символом $\widetilde{H}^n$. Тогда, так как $\widetilde{H}^n \subset \widetilde{H}^{2n+1}$ $(n = 2^k - 1)$, можно положить $H^\infty = \bigcup\limits_{k=2}^{\infty} \widetilde{H}^{2^k-1}$.

2. Эквивалентность линейных совершенных кодов в нулевом слое и их группа автоморфизмов

Как и в конечномерном случае, для любой изометрии $A : \{0,1\}_0^{\mathbb{N}} \to \{0,1\}_0^{\mathbb{N}}$ существует вектор $a \in \{0,1\}_0^{\mathbb{N}}$ и перестановка $\pi : \mathbb{N} \to \mathbb{N}$, такие, что $A(u) = \widetilde{\pi}(u) + a$, где $\widetilde{\pi}((u_1, \dots, u_n, \dots)) = (u_{\pi^{-1}(1)}, \dots, u_{\pi^{-1}(n)}, \dots)$.

Определение 2. Два совершенных двоичных кода $C_1, C_2 \subset \{0,1\}_0^{\mathbb{N}}$ называются эквивалентными, если существует изометрия A нулевого слоя $\{0,1\}_0^{\mathbb{N}}$, такая, что $A(C_1) = C_2$. Два совершенных двоичных кода $C_1, C_2 \subset \{0,1\}_0^{\infty}$ называются изоморфными, если существует перестановка $\pi : \mathbb{N} \to \mathbb{N}$, такая, что $\widetilde{\pi}(C_1) = C_2$.

Лемма 1. Все коды Хемминга в слое $\{0,1\}_0^{\mathbb{N}}$ эквивалентны между собой.

3. Континуальность множества классов эквивалентности совершенных двоичных кодов бесконечной длины

В коде Хемминга H^∞ рассмотрим подпространство R_i, порождённое всеми векторами веса 3 с i-й координатой равной единице. Всевозможные смежные классы вида

$R_i^u = R_i + u$ $(u \in H^\infty)$ называются *i-компонентами* кода H^∞, $i \in \mathbb{N}$. Рассмотрим некоторое семейство $\mathcal{B} = \left\{R_{i_1}^{u_1}, R_{i_2}^{u_2}, \dots\right\}$, состоящее из конечного или бесконечного числа попарно не пересекающихся i_p-компонент, где $\mathbf{u}_p \in H^\infty$, $1 \leqslant p < m+1$ $(m \in \mathbb{N} \cup \{\infty\})$. Одна из основных конструкций нелинейных совершенных двоичных кодов состоит в том, что в коде H^n сдвигаются по координатам i_p все компоненты из семейства $\mathcal{B}$. Доказательство этого факта в точности такое же, как и в случае кодов конечной длины [2–5]. Далее будем говорить, что код $H^\infty(\mathcal{B})$ построен из кода Хемминга H^∞ *сдвигами* (или *свитчингами*) компонент из семейства $\mathcal{B}$. Если при фиксированном индексе i имеем $i_p = i$ для всех p, то код $H^\infty(\mathcal{B})$ называем *кодом Васильева* бесконечной длины. Такие коды конечной длины впервые были построены в [6]. Для нахождения мощности множества всех классов эквивалентности кодов бесконечной длины достаточно ограничиться рассмотрением кодов Васильева.

Положим $i = 1$. Компонента R_1 порождается всеми векторами v_p веса 3 с носителями $[v_p] = \{1, 2p, 2p+1\}$, $p \in \mathbb{N}$. Рассмотрим векторы $w_1 = 0$, $w_p = e_8 + e_9 + \dots + e_{2^{p+2}-2}$, $p \in \mathbb{N}$, $p \geqslant 2$. Из определения проверочной матрицы следует, что $w_p \in H^\infty$, $p \in \mathbb{N}$. Для бесконечного семейства компонент $\mathcal{B}_1 = \{R_1^{w_p}\}_{p=1}^\infty$ и любого $\varepsilon \in \{0,1\}^{\mathbb{N}}$ $(\varepsilon = (\varepsilon_1, \varepsilon_2, \dots))$ рассмотрим следующий код Васильева:

$$H^\infty(\mathcal{B}_1, \varepsilon) = \left(H^\infty \setminus \bigcup_{p=1}^{\infty} R_1^{w_p}\right) \cup \left(\bigcup_{p=1}^{\infty} \left(R_1^{w_p} + \varepsilon_p e_1\right)\right).$$

То есть код $H^\infty(\mathcal{B}_1, \varepsilon)$ получается из кода Хемминга H^∞ сдвигами только тех компонент $R_1^{u_p}$ из семейства $\mathcal{B}_1$, для которых $\varepsilon_p = 1$.

Лемма 2. Пусть L — любое линейное пространство над полем $\mathrm{GF}(2)$ и $H \subset L$ — его подпространство. Пусть $A : L \to L$ — аффинный изоморфизм пространства L и $F : L \to \{0,1\}^3$ — линейное отображение, такое, что $F(H) = \{0,1\}^3$ и $F \circ A(H) = \{0,1\}^3$. Рассмотрим два подмножества $C_1, C_2 \subset L$, удовлетворяющих условиям

$$C_1 \setminus \mathrm{Ker}F = C_2 \setminus \mathrm{Ker}F = H \setminus \mathrm{Ker}F,$$
$$C_1 \setminus H \subset \mathrm{Ker}F, \quad C_2 \setminus H \subset \mathrm{Ker}F.$$

Тогда если $A(C_1) = C_2$, то $A(H) \subseteq H$ и $a \in H$.

Эта лемма позволяет доказать следующий ключевой факт.

Теорема 1. Если $\varepsilon, \varepsilon' \in \{0,1\}^{\mathbb{N}}$, $\varepsilon \neq \varepsilon'$ $\varepsilon_1 = \varepsilon'_1 = 1$, то коды Васильева $H^\infty(\mathcal{B}_1, \varepsilon)$, $H^\infty(\mathcal{B}_1, \varepsilon')$ не эквивалентны.

Мы построили континуум попарно не эквивалентных кодов Васильева бесконечной длины. Так как в счётном множестве $\{0,1\}_0^{\mathbb{N}}$ может быть не более континуума различных кодов, то из теоремы 1 сразу получается

Следствие 1. Мощность множества всех классов эквивалентности совершенных двоичных кодов бесконечной длины равна континууму.

4. Совершенные двоичные коды в кубе $\{0,1\}^{\mathbb{N}}$

Существование совершенных двоичных кодов в кубе $\{0,1\}^{\mathbb{N}}$ сразу следует из существования таких кодов в слое $\{0,1\}_0^{\mathbb{N}}$. Для этого пронумеруем все слои числами из отрезка $[0,1]$, т. е. каждому числу $\alpha \in [0,1]$ сопоставляем слой $\mathcal{L}_\alpha \subset \{0,1\}^{\mathbb{N}}$, при этом $\{0,1\}^{\mathbb{N}} = \bigcup\limits_{\alpha \in [0,1]} \mathcal{L}_\alpha$. Выберем в каждом слое по одному элементу u_α и для любого совершенного кода $C_0 \subset \mathcal{L}_0 = \{0,1\}_0^{\mathbb{N}}$ полагаем $C = \bigcup\limits_{\alpha \in [0,1]} (C_0 + u_\alpha)$. Очевидно, множество C

является совершенным двоичным кодом в $\{0,1\}^{\mathbb{N}}$. Отметим, что при построении кода C была применена аксиома выбора.

Лемма 3. В кубе $\{0,1\}^{\mathbb{N}}$ существуют линейные совершенные двоичные коды.

Посмотрим, как устроены изометрии куба $\{0,1\}^{\mathbb{N}}$. Так как разные слои этого куба находятся на бесконечном расстоянии Хемминга друг от друга, то изометрия допускает, во-первых, произвольную перестановку (континуального) множества всех слоев. Далее, в каждом слое $\mathcal{L}_\alpha$ допускается (независимо от других слоёв) перестановка координат π_α и перенос на вектор $a_\alpha \in \{0,1\}_0^{\mathbb{N}}$. Изометрия может не быть аффинным преобразованием всего куба. На этом основании вводим два различных определения.

Определение 3. Два совершенных кода $C_1, C_2 \subset \{0,1\}^{\mathbb{N}}$ называются *изометричными* (соответственно, *эквивалентными*), если существует изометрия A пространства $\{0,1\}^{\mathbb{N}}$ (соответственно, изометрия, являющаяся аффинным преобразованием пространства $\{0,1\}^{\mathbb{N}}$), такая, что $A(C_1) = C_2$.

Лемма 4. Все линейные совершенные коды в $\{0,1\}^{\mathbb{N}}$ эквивалентны между собой.

Мощность континуума принято обозначать символом $\mathfrak{c}$. Мощность всех подмножеств континуального множества будем обозначать символом $2^{\mathfrak{c}}$. Эту мощность называют также *гиперконтинуумом*.

Пример 1. В пространстве $\{0,1\}^{\mathbb{N}}$ строится гиперконтинуальное семейство линейных совершенных двоичных кодов $\mathcal{H} = \{H_\gamma\}_{\gamma\in\Gamma}$, такое, что для любых $H_{\gamma_1}, H_{\gamma_2} \in \mathcal{H}$ $(\gamma_1 \neq \gamma_2)$ не существует ни одной перестановки $\pi : \mathbb{N} \to \mathbb{N}$, такой, что $H_{\gamma_2} = \widetilde{\pi}(H_{\gamma_1})$.

Теорема 2. Мощность множества всех классов эквивалентности совершенных двоичных кодов в пространстве $\{0,1\}^{\mathbb{N}}$ равна гиперконтинууму $2^{\mathfrak{c}}$.

ЛИТЕРАТУРА

1. *Потапов В. Н.* Бесконечномерные квазигруппы конечных порядков // Матем. заметки. 2013. Т. 93. Вып. 3. С. 457–460.
2. *Августинович С. В., Соловьева Ф. И.* Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Проблемы передачи информации. 1997. Т. 33. Вып. 3. С. 15–21.
3. *Романов А. М.* О построении совершенных нелинейных двоичных кодов инверсией символов // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4. № 1. С. 46–52.
4. *Phelps K. T. and LeVan M. J.* Kernels of nonlinear Hamming codes // Designs, Codes and Cryptogr. 1995. V. 6. No. 3. P. 247–257.
5. *Solov'eva F. I.* Switchings and perfect codes // Numbers, Information and Complexity. Dordrecht: Kluver Acad. Publ., 2000. P. 311–324.
6. *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 75–78.

УДК 512.6 DOI 10.17223/2226308X/8/46

ЭНЕРГОСБЕРЕГАЮЩЕЕ ПРОТИВОГОНОЧНОЕ КОДИРОВАНИЕ СОСТОЯНИЙ АСИНХРОННОГО АВТОМАТА

Ю. В. Поттосин

Рассматривается задача противогоночного кодирования состояний асинхронного автомата, где наряду с минимизацией длины кода состояния минимизируется

интенсивность переключений элементов памяти. Используется подход, предполагающий рассмотрение пар переходов между состояниями и установление для них условий отсутствия опасных состязаний, представляемых в виде троичной матрицы условий. Решение рассматриваемой задачи сводится к решению задачи о взвешенном минимальном покрытии строк матрицы условий множествами строк, для каждого из которых существует вектор, имплицирующий все строки из этого множества.

Ключевые слова: *асинхронный автомат, противогоночное кодирование состояний, энергосберегающее кодирование состояний.*

Моделью поведения логической схемы с памятью является конечный автомат, представляющий собой пятерку (A, B, Q, Ψ, Φ), где A, B и Q — соответственно множества входных символов, выходных символов и состояний автомата, а Ψ и Φ — функции $\Psi : A \times Q \to Q$ и $\Phi : A \times Q \to B$, называемые соответственно функцией переходов и функцией выходов. Для $q_i, q_j \in Q$ и $a \in A$ состояние $q_j = \Psi(a, q_i)$ является тем состоянием, в которое автомат переходит из состояния q_i под воздействием входного символа a. Рассматриваемая задача позволяет игнорировать функцию Φ, поэтому в дальнейшем она не будет здесь упоминаться.

Задача кодирования состояний автомата заключается в присвоении каждому состоянию определённого булева вектора $(z_1, z_2, \ldots, z_k)$, называемого кодом состояния, который соответствует набору состояний двоичных элементов памяти (триггеров) в логической схеме, где каждый переход из состояния в состояние представляется переключением одного или нескольких триггеров. Естественно, что это переключение происходит не одновременно. В реальных асинхронных схемах это явление называется *состязаниями*, или *гонками* элементов памяти. Принято называть состязания *неопасными*, если все промежуточные состояния, в которых автомат может оказаться при переходе из одного состояния в другое под воздействием некоторого входного сигнала a, являются неустойчивыми для сигнала a, т. е. при любом порядке переключений элементов памяти автомат из некоторого состояния q_i под воздействием входного сигнала a переходит всегда в состояние $q_j = \Psi(a, q_i)$. Если же при этом автомат может оказаться в некотором устойчивом состоянии q_k, отличном от q_j, то состязания называются *опасными*.

Кодирование состояний, обеспечивающее отсутствие опасных состязаний (гонок), называется *противогоночным*. Естественно, здесь возникает задача минимизации длины кода состояния, приводящая к наименьшему числу элементов памяти в реальной схеме.

Другим критерием оптимизации схемы является величина потребляемой энергии. Это обусловлено, с одной стороны, стремлением увеличить время действия источника энергии в портативных приборах и, с другой стороны, стремлением снизить остроту проблемы отвода тепла при проектировании сверхбольших интегральных схем. Как отмечено в [1], потребляемая мощность схемы, построенной на основе КМОП-технологии, пропорциональна частоте изменения сигналов. Это даёт возможность частично решать данную проблему на уровне логического проектирования. В частности, снижения энергопотребления можно добиваться при кодировании состояний автомата. Кодировать состояния при этом надо таким образом, чтобы при переходе автомата из одного состояния в другое меняли свое состояние как можно меньше элементов памяти. Проблеме энергосберегающего кодирования состояний синхронного автомата посвящено довольно много работ, одной из которых является, например, работа [2], где процесс кодирования состояний автомата представляется как размещение состояний

в булевом пространстве внутренних переменных. Проблема энергопотребления логических схем рассматривается также в [3], где решается задача определения режима максимального потребления энергии в схеме, реализующей конечный автомат. В данной работе рассматривается возможность учёта энергосбережения при противогоночном кодировании состояний асинхронного автомата. Автору не известны публикации, посвящённые данной проблеме.

Условие отсутствия опасных состязаний для пары переходов $q_i \to q_j$, $q_k \to q_l$ ($q_j \neq q_l$) при одном и том же входном сигнале a можно выразить троичным вектором [4], в котором компоненты соответствуют состояниям автомата, компоненты i и j имеют одно значение, 0 или 1, а компоненты k и l — противоположное ему значение. Остальным компонентам приписывается значение «$-$». В схеме, реализующей заданный автомат, это условие выполняется триггером, который в процессе одного перехода рассматриваемой пары хранит состояние 0, а в процессе другого — 1.

На множестве векторов, представляющих условия отсутствия опасных состязаний, имеется отношение импликации: троичный вектор $\mathbf{a}$ имплицирует троичный вектор $\mathbf{b}$, если $\mathbf{b}$ получается из $\mathbf{a}$ заменой некоторых нулей или единиц значением «$-$» и, возможно, инвертированием полученного результата. Например, вектор $(10--101)$ имплицирует векторы $(10---01)$ и $(01---1-)$. Смысл этого отношения в том, что условие, представленное вектором $\mathbf{b}$, автоматически выполняется при соблюдении условия, представленного вектором $\mathbf{a}$.

Все условия отсутствия опасных состязаний в виде описанных векторов составляют троичную матрицу, в которой отсутствуют имплицируемые строки. Эта матрица называется *матрицей условий* [4]. Говорят, что троичная матрица R *имплицирует* троичную матрицу S, если для каждой строки матрицы S в матрице R найдётся имплицирующая её строка. Задача противогоночного кодирования с минимизацией длины кода состояния сводится к нахождению матрицы с минимальным числом строк, имплицирующей матрицу условий и называемой *кратчайшей имплицирующей формой* матрицы условий. Столбцы этой матрицы будут представлять искомые коды состояний, а получаемая в результате её транспонирования матрица называется *матрицей кодирования*. Строкам матрицы кодирования соответствуют состояния автомата, а столбцам — внутренние переменные, и строки этой матрицы представляют коды соответствующих состояний.

Кратчайшая имплицирующая форма матрицы условий находится следующим образом. Множество строк матрицы условий называется *совместимым*, если существует вектор, имплицирующий каждую строку этого множества. Совместимое множество называется *максимальным*, если оно не является собственным подмножеством другого совместимого множества. Надо найти кратчайшее покрытие множества строк матрицы условий максимальными совместимыми множествами. Каждому совместимому множеству соответствует вектор, имплицирующий все строки, принадлежащие этому множеству. Векторы, соответствующие элементам полученного покрытия, в качестве строк составят кратчайшую имплицирующую форму заданной матрицы условий.

При применении описанного подхода к решению задачи противогоночного кодирования состояний автомата для снижения интенсивности переключений элементов памяти можно использовать следующие соображения.

Каждому столбцу матрицы кодирования можно поставить в соответствие множество переходов. Это множество для i-го столбца составляют те переходы, которыми связаны состояния автомата, в кодах которых переменная z_i имеет различные значения, т. е. при таких переходах i-й триггер в реальной схеме, реализующей автомат,

меняет своё состояние. Следовательно, для снижения интенсивности переключений элементов памяти надо выбрать такой вариант противогоночного кодирования состояний, который соответствует наименьшему множеству переходов между состояниями.

Если удаётся вычислить вероятности переходов, то столбцу матрицы кодирования состояний ставится в соответствие вероятность события, которое заключается в том, что происходит некоторый переход из множества переходов, связанных с данным столбцом. Поскольку переходы между состояниями автомата являются несовместимыми событиями, эта вероятность равна сумме вероятностей отдельных переходов из данного множества. Для подсчёта вероятностей переходов между состояниями в [2] используется метод Чэпмена — Колмогорова, где данные вероятности получаются в результате решения системы линейных уравнений с этими вероятностями в качестве неизвестных. Однако этот метод можно применять только тогда, когда автомат является полностью определённым, а его граф поведения является сильносвязным ориентированным графом. В противном случае столбцу матрицы кодирования состояний автомата приписывается мощность связанного с ним множества переходов.

Таким образом, каждому совместимому множеству строк матрицы условий и соответственно вектору, имплицирующему все строки из этого множества, приписывается вес в виде числа переходов или суммы вероятностей переходов, связанных с этим вектором. Искомое решение получается в виде покрытия множества строк матрицы условий максимальными совместимыми множествами, обладающего минимальным весом. Весом покрытия является сумма весов принадлежащих ему элементов.

Кодирование состояний автомата можно представить как размещение состояний в пространстве внутренних переменных z_1, z_2, …, z_k [2], т. е. по вершинам булева гиперкуба, представляющего это пространство. В [2] введён критерий качества такого размещения с точки зрения интенсивности переключений элементов памяти. Этот критерий выражается формулой $D = \sum w_{ij}(d_{ij} - 1)$, где d_{ij} — расстояние по Хэммингу между кодами состояний q_i и q_j; w_{ij} — число переходов или вероятность перехода между состояниями q_i и q_j, и суммирование берётся по всем парам состояний, соответствующим парам вершин в гиперкубе. Очевидно, чем меньше значение D, тем лучше результат размещения, и $D = 0$, если всем парам состояний, связанным переходами, соответствуют рёбра гиперкуба. Тогда при любом переходе из состояния в состояние переключается ровно один элемент памяти. Сравнение по критерию D результатов решения примеров показало целесообразность использования предлагаемого метода.

ЛИТЕРАТУРА

1. *Мурога С.* Системное проектирование сверхбольших интегральных схем. В 2-х кн. Кн. 1. М.: Мир, 1985.
2. *Закревский А. Д.* Алгоритмы энергосберегающего кодирования состояний автомата // Информатика. 2011. № 1(29). С. 68–78.
3. *Закревский А. Д.* Нахождение режима максимального энергопотребления логической схемы // Прикладная дискретная математика. 2012. № 2. С. 100–104.
4. *Закревский А. Д.* Логический синтез каскадных схем. М.: Наука, 1981.

УДК 519.17 DOI 10.17223/2226308X/8/47

ШПЕРНЕРОВЫ ДЕРЕВЬЯ

В. Н. Салий

В бесконтурном орграфе отношение достижимости на множестве вершин является отношением порядка. Одним из интересных свойств для упорядоченного множества является его шпернеровость — наличие в нём антицепи максимальной длины, все элементы которой имеют одинаковую высоту. В графах с отношением достижимости это свойство обсуждается для выходящих и входящих деревьев, модифицируется и рассматривается для связанных с ними функциональных и контрафункциональных орграфов, для неориентированных деревьев.

Ключевые слова: *упорядоченное множество, бесконтурный орграф, шпернерово свойство, дерево, входящее дерево, выходящее дерево, функциональный орграф, контрафункциональный орграф.*

1. Под высотой элемента в конечном упорядоченном множестве $(A, \leqslant)$ понимается наибольшая из длин убывающих цепей, начинающихся с этого элемента (длина убывающей цепи — уменьшенное на единицу количество элементов в ней). Например, все минимальные элементы в $(A, \leqslant)$ имеют высоту 0.

Антицепь — это некоторый набор попарно не сравнимых элементов из $(A, \leqslant)$. Считая длиной антицепи количество элементов в ней, назовём антицепь главной, если она имеет максимально возможную для антицепей в $(A, \leqslant)$ длину, и назовем правильной, если все её элементы имеют одинаковую высоту.

Конечное упорядоченное множество по определению обладает шпернеровым свойством, или является шпернеровым, если среди его главных антицепей есть хотя бы одна правильная. Это свойство впервые рассмотрел Шпернер [1], доказавший, в частности, что оно выполняется для совокупности $P(S)$ всех подмножеств конечного множества S, упорядоченной теоретико-множественным включением.

2. Ориентированный граф (орграф), не содержащий контуров, называется бесконтурным орграфом. Говорят, что в данном орграфе G вершина v достижима из вершины u, если в G существует путь с началом u и концом v. В этом случае пишут $(u, v) \in \delta$, определяя тем самым отношение достижимости в G.

Известно, что отношение достижимости δ в бесконтурных орграфах является отношением порядка (о бесконтурных орграфах см. в [2]). Так что если $G = (V, \alpha)$ — бесконтурный орграф с множеством вершин V и отношением смежности α, то можно рассматривать ассоциированное с ним упорядоченное множество (V, δ). Бесконтурный орграф $G = (V, \alpha)$ назовём шпернеровым, если (V, δ) — шпернерово упорядоченное множество. В общем случае эффективного способа проверки свойства шпернеровости для бесконтурных орграфов пока нет. В [3] найден критерий шпернеровости для многоугольных орграфов, т. е. бесконтурных орграфов, получающихся из циклов путём ориентации рёбер. В [4] предложена полиномиальная по сложности процедура, позволяющая выяснить наличие или отсутствие шпернерова свойства для линейных орграфов, т. е. орграфов, получающихся путём ориентации рёбер из цепей.

Далее рассмотрим некоторые вопросы, связанные со свойством шпернеровости для деревьев.

3. Для заданного дерева, т. е. связного графа без циклов, при наличии у него n рёбер возможны 2^n ориентаций. Свойства ассоциированных с ними упорядоченных множеств исследовались различными авторами. Так, в [5] установлено, что наименьшая из длин

главных антицепей среди всех таких порядков равняется $[\lambda/2]$ или $[\lambda/2]+1$, где λ — количество висячих вершин дерева.

Наибольший интерес для деревьев представляют два типа ориентации рёбер: выходящее дерево — когда в полученном орграфе имеется единственный источник (вершина, не достижимая из других вершин), и входящее дерево — когда в полученном орграфе имеется единственный сток (вершина, из которой не достижимы другие вершины).

Нетрудно понять, что всякое выходящее дерево является шпернеровым. Действительно, в множестве его вершин, упорядоченном достижимостью, единственный источник — наибольший элемент, а стоки (висячие вершины) — минимальные элементы, причём эти минимальные элементы образуют главную антицепь, которая является правильной (у всех её элементов высота 0).

4. Пусть $G=(V,\alpha)$ — некоторый орграф. Его расконтуриванием называется всякая совокупность дуг, удаление которых превращает G в бесконтурный орграф. Расконтуривание, по определению, является минимальным, если никакое его собственное подмножество не является расконтуриванием. Заметим, что минимальное расконтуривание не нарушает свойства связности орграфа G. Орграф G назовем шпернеровым, если у него есть минимальное расконтуривание, приводящее к шпернеровому бесконтурному орграфу.

Орграф называется контрафункциональным, если каждая его вершина имеет степень захода 1, т. е. в неё входит единственная дуга. Известно [6], что связный орграф является контрафункциональным тогда и только тогда, когда в нём есть точно один контур и удаление из этого контура любой дуги (минимальное расконтуривание) приводит к образованию выходящего дерева. Поскольку, как было отмечено, все выходящие деревья — шпернеровы, любой связный контрафункциональный орграф также шпернеров.

5. Менее очевидны построения, связанные с входящими деревьями. Если (T,α) — входящее дерево, то очевидно, что соответствующее ему упорядоченное множество (T,δ) является нижней полурешёткой (у любых двух элементов есть точная нижняя грань), наименьший элемент которой — корень (единственный сток) дерева, и при этом у каждого элемента v имеется единственный нижний сосед (т. е. элемент u, такой, что $u<v$ и не существует $x\in T$ со свойством $u<x<v$).

Нижнюю полурешётку с наименьшим элементом (нулём), в которой у каждого ненулевого элемента имеется единственный нижний сосед, по ассоциации будем называть древесной полурешёткой. Элемент a конечного упорядоченного множества $(A,\leqslant)$ называется разложимым (в пересечение), если он является точной нижней гранью некоторых двух отличных от него элементов.

Теорема 1. Конечная древесная полурешётка есть шпернерово упорядоченное множество тогда и только тогда, когда в ней высота каждого максимального элемента больше высоты любого разложимого элемента.

Пусть (T,α) — входящее дерево. В упорядоченном множестве (T,δ) высота вершины — это расстояние от неё до корня, максимальными элементами являются висячие вершины, а разложимыми элементами — точки ветвления (в каждую такую вершину входят как минимум две дуги). Так что в терминах деревьев теорема 1 выглядит как

Теорема 2. Входящее дерево является шпернеровым тогда и только тогда, когда расстояние от каждой висячей вершины до корня больше, чем расстояние до него от любой точки ветвления.

6. Следующая полиномиальная процедура позволяет проверить наличие или отсутствие свойства шпернеровости для входящих деревьев.

Пусть A — матрица смежности, а D — (стандартно вычисляемая из A) матрица достижимости дерева (T, α). Тогда:

1) в матрице A выделяются нулевые столбцы, они соответствуют висячим вершинам, образующим подмножество $H \subset T$;
2) в матрице A выделяются столбцы, содержащие не менее двух единиц, они соответствуют точкам ветвления, образующим подмножество $B \subset T$;
3) в матрице D в каждой строке, соответствующей вершине $u \in H$, подсчитывается количество единиц $d(u)$. Выбирается число $d_H = \min\limits_{u \in H} d(u)$;
4) в матрице D в каждой строке, соответствующей вершине $v \in B$, подсчитывается количество единиц $d(v)$. Выбирается число $d_B = \max\limits_{v \in B} d(v)$;
5) дерево шпернерово тогда и только тогда, когда $d_H > d_B$.

Орграф называется функциональным, если каждая его вершина имеет степень исхода 1, т. е. из неё выходит единственная дуга. Известно [6], что связный орграф является функциональным тогда и только тогда, когда в нём есть точно один контур и удаление из этого контура любой дуги (минимальное расконтуривание) приводит к образованию входящего дерева. Проведя описанную выше процедуру для каждого минимального расконтуривания функционального орграфа, можно ответить на вопрос, является ли этот орграфа шпернеровым.

7. Неориентированное дерево назовём шпернеровым, если шпернеровым свойством обладает хотя бы одно из ассоциированных с ним входящих деревьев.

Дерево называется радиальным, если в нём есть вершина (центр), равноудалённая от всех висячих вершин.

Следствие 1. Радиальное дерево является шпернеровым.

Дерево называется сверхстройным, если в нём имеется единственная вершина со степенью не меньше 3. Сверхстройное дерево является объединением не менее чем трёх цепей, имеющих общую вершину (корень). Частные случаи: пальма (все цепи, кроме одной, имеют длину 1), звезда (у всех цепей длина 1).

Следствие 2. Сверхстройное дерево является шпернеровым.

Для того чтобы определить, является ли предъявленное дерево шпернеровым, нужно протестировать на шпернеровость связанные с ним входящие деревья — с помощью процедуры из п. 6. Для её запуска матрица смежности исходного дерева следующим образом преобразуется в матрицу смежности входящего дерева, получающегося при конкретном выборе корня.

Пусть в качестве корня выбрана вершина v. Тогда:

1) в начальной строке, соответствующей вершине v, матрицы смежности дерева каждая единица заменяется на ноль, а единица, симметричная ей относительно главной диагонали, помечается;
2) в строке, содержащей помеченную единицу, каждая непомеченная единица заменяется на ноль, а симметричная ей относительно главной диагонали единица помечается;
3) процесс заканчивается, когда в каждой строке, кроме начальной, останется только одна (помеченная) единица. Полученная матрица будет матрицей смежности для входящего дерева с корнем v.

ЛИТЕРАТУРА

1. *Sperner E.* Ein Satz uber Untermengen einer endlichen Menge // Math. Zeitschrift. 1928. B. 27. No. 1. S. 544–548.
2. *Богомолов А. Д., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997.
3. *Салий В. Н.* Шпернерово свойство для многоугольных графов // Прикладная дискретная математика. Приложение. 2014. № 7. С. 135–137.
4. *Новокшонова Е. Н.* Шпернерово свойство для линейных графов // Компьютерные науки и информационные технологии: Материалы Междунар. науч. конф. Саратов: Издат. Центр «Наука», 2014. С. 230–231.
5. *Atkinson M. D. and Ng D. T. N.* On the width of an orientation of a tree // Order. 1988. V. 5. No. 1. P. 33–43.
6. *Харари Ф.* Теория графов. М.: Мир, 1973.

УДК 519.1+519.173 DOI 10.17223/2226308X/8/48

О РАЗНООБРАЗИИ ШАРОВ ГРАФА ЗАДАННОГО ДИАМЕТРА[1]

Т. И. Федоряева

Изучаются векторы разнообразия шаров (i-я компонента вектора равна числу различных шаров радиуса i) для обыкновенных связных графов в асимптотике. Исследовано асимптотическое поведение числа графов с разнообразием шаров специального вида, в частности с локальным (полным) разнообразием шаров. Для типичного графа заданного диаметра получено описание строения разнообразия шаров больших радиусов.

Ключевые слова: *граф, шар, радиус шара, вектор разнообразия шаров.*

В работе изучается разнообразие шаров обыкновенного связного графа в асимптотике. Пусть $\tau_i(G)$ — число всех различных шаров радиуса i в метрическом пространстве графа G с обычным расстоянием между вершинами, т. е. длиной кратчайшей цепи, соединяющей эти вершины.

Определение 1 [1]. Вектор $\tau(G) = (\tau_0(G), \tau_1(G), \ldots, \tau_d(G))$, где $d = d(G)$ — диаметр графа G, называется *вектором разнообразия шаров* графа G.

Например, вектор разнообразия шаров простой цепи длины d, как показано в [1], равен $\Delta_d = (\Delta_0^d, \Delta_1^d, \ldots, \Delta_d^d)$, где

$$\Delta_i^d = \begin{cases} d+1, & \text{если } 0 \leqslant i \leqslant \lfloor d/2 \rfloor, \\ 2(d-i)+1, & \text{если } \lfloor d/2 \rfloor < i < d, \\ 1, & \text{если } i \geqslant d. \end{cases}$$

Определение 2 [2]. Граф G обладает *локальным t-разнообразием шаров*, если $|V(G)| = \tau_0(G) = \tau_1(G) = \ldots = \tau_t(G)$, $0 \leqslant t < d(G)$. Граф G с локальным t-разнообразием шаров при $t = d(G) - 1$ называется графом *полного разнообразия шаров*.

Таким образом, вектор разнообразия шаров графа G с полным разнообразием шаров имеет вид $(|V(G)|, \ldots, |V(G)|, 1)$. В [1] показано, что класс деревьев с полным разнообразием шаров является бедным, так как состоит лишь из звезды $K_{1,n}$, и получена

[1]Работа поддержана грантом РФФИ, проект № 14-01-00507.

характеризация деревьев с локальным разнообразием шаров. Наименьший порядок графов диаметра d с локальным t-разнообразием шаров (полным разнообразием шаров) найден в [3], а в [4] все такие графы наименьшего порядка явно описаны с точностью до изоморфизма и вычислены их векторы разнообразия шаров. В [3] установлены все возможные значения параметров n, d и t, при которых существует n-вершинный граф диаметра d с полным разнообразием шаров (локальным t-разнообразием шаров). В [5] изучен вопрос единственности n-вершинного графа диаметра d с полным разнообразием шаров. Только при $n = 2d > 6$ или $d \leqslant 1$ существует единственный такой граф — $2d$-вершинный цикл при $d > 3$ и полный граф K_n при $d \leqslant 1$.

В настоящей работе исследуется асимптотическое поведение числа графов с локальным (полным) разнообразием шаров и строение вектора разнообразия шаров графа заданного диаметра. Хорошо известен следующий результат.

Теорема 1 [6]. Почти все графы являются графами диаметра 2.

Более того, справедлива следующая

Теорема 2 [2]. Почти все графы являются графами диаметра 2 с полным разнообразием шаров.

Непосредственно из теорем 1 и 2 вытекает

Теорема 3. Граф диаметра 2 является графом полного разнообразия шаров.

Основным результатом работы является следующая

Теорема 4. Пусть $d \geqslant 3$. Тогда в графе диаметра d число различных шаров радиуса i равно Δ_i^d для всех $i \geqslant d/2$.

Следствие 1. Пусть $d \geqslant 3$ и $t \geqslant d/2$. Тогда граф диаметра d не обладает локальным t-разнообразием шаров и, в частности, не является графом полного разнообразия шаров.

ЛИТЕРАТУРА

1. *Федоряева Т. И.* Разнообразие шаров в метрических пространствах деревьев // Дискрет. анализ и исслед. операций. Сер. 1. 2005. Т. 12. № 3. С. 74–84.
2. *Евдокимов А. А.* Локально изометрические вложения графов и свойство продолжения метрики // Сиб. журн. исслед. операций. 1994. Т. 1. № 1. С. 5–12.
3. *Федоряева Т. И.* Векторы разнообразия шаров для графов и оценки их компонент // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14. № 2. С. 47–67.
4. *Федоряева Т. И.* О графах с заданными диаметром, числом вершин и локальным разнообразием шаров // Дискрет. анализ и исслед. операций. 2010. Т. 17. № 1. С. 65–74.
5. *Федоряева Т. И.* Мажоранты и миноранты класса графов с фиксированными диаметром и числом вершин // Дискрет. анализ и исслед. операций. 2013. Т. 20. № 1. С. 58–76.
6. *Bollobas B.* Graph Theory. Springer Verlag, 1979.

Секция 7

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 004.431, 004.4'42, 004.451 DOI 10.17223/2226308X/8/49

МОДИФИКАЦИЯ ЛЯПАСА ДЛЯ РАЗРАБОТКИ ОС

С. Ю. Гречнев, Д. А. Стефанцов

Описывается модификация транслятора ЛЯПАС для возможности разработки операционной системы. Изменены инициализирующий и завершающий ассемблерные коды, скорректирована работа с комплексами, оптимизировано использование памяти программой, добавлены новые возможности: доступ к произвольной ячейке оперативной памяти и получение адреса процедур.

Ключевые слова: *ЛЯПАС, операционная система, Русский язык программирования.*

Разработка операционной системы (ОС) предъявляет к языку программирования и компилятору с него ряд специфических требований, например необходимость хранения служебных структур данных на протяжении всего времени работы ОС, возможность записи адресов подпрограмм в переменные языка, возможность генерирования ассемблерного кода без привязки к существующей ОС, в которой ведётся разработка, и к её формату исполняемого файла. В данной работе сообщается о модификации Логического Языка для Представления Алгоритмов Синтеза (ЛЯПАСа) [1] и соответствующего транслятора для разработки ОС [2]. Кроме упомянутых изменений, в язык добавлены возможности, повышающие удобство разработки программ на нём, а в компилятор — повышающие надёжность генерируемой ассемблерной программы.

Для работы операционной системы необходимо хранить некоторые структуры данных от запуска компьютера до его выключения. Примерами таких структур являются глобальная таблица дескрипторов (GDT), таблица дескрипторов прерываний (IDT) [3], таблица планировщика процессов. Однако в ЛЯПАСе отсутствуют глобальные переменные, обычно применяемые для данных целей, поэтому в язык добавлен доступ к произвольной ячейке оперативной памяти. Такой доступ осуществляется через специальный комплекс K, i-й элемент которого представляет собой ячейку оперативной памяти по адресу i. Дополнительно это позволяет выводить сообщения на экран, производя их запись в участок памяти с фиксированным адресом — видеобуфер.

Для построения IDT введена возможность получения адресов подпрограмм. Во внутреннюю переменную τ помещается адрес ассемблерной метки, с которой начинается подпрограмма.

Перечисленные возможности считаются потенциально небезопасными для разработки пользовательских программ и включаются при трансляции флагом `-os`.

Для компиляции файла, запускаемого в ОС GNU/Linux, транслятор добавляет инициализирующий и завершающий коды. Инициализирующий код запрашивает у ОС память под комплексы в куче, переходит на первую подпрограмму, после завершения выполняет системный вызов `sys_exit`; завершающий код содержит подпрограмму

`_addmem`, которая запрашивает дополнительную память в куче. Изменение инициализирующего и завершающего кодов включается флагом `-os`.

Дополнительно к описанным в ЛЯПАС внесены изменения, делающие язык более удобным. Во-первых, в работе с комплексами добавлена проверка по ёмкости. При обращении к i-му элементу комплекса ёмкостью S проверяется условие $i < S$. Если оно не выполняется, программа переходит на метку `_errend`.

Во-вторых, оптимизировано использование памяти программой. Ранее в ЛЯПАСе для каждой вызываемой подпрограммы в стеке выделялось 1420 байт под все возможные локальные переменные, параметры всех возможных комплексов (тип комплекса, адрес комплекса в куче, ёмкость, мощность), адрес начала свободной памяти в куче. Адреса локальных переменных фиксировались в стеке в соответствии с их именами: вызывающая подпрограмма выделяла память в стеке для вызываемой, помещала туда входные параметры, копировала значения выходных параметров после завершения подпрограммы. Данный способ прост в реализации, однако неэффективно использует память и создаёт много вспомогательных конструкций в коде.

Предлагаются следующие изменения. Память выделяется только под используемые локальные переменные; переменные и комплексы размещаются в стеке в порядке их упоминания, что позволяет намного эффективнее использовать память. Вызывающая подпрограмма выделяет память в стеке для входных и выходных параметров вызываемой подпрограммы, заполняет входные параметры и отдаёт управление вызываемой. Последняя самостоятельно выделяет память в стеке под локальные переменные, а после завершения работы удаляет их. После этого вызывающая подпрограмма копирует значения выходных параметров в свои локальные переменные и возвращает стек к исходному состоянию.

Новая организация памяти программы позволяет также реализовать эффективную композицию подпрограмм. Обозначим множество значений переменных V, множества значений символьных и логических комплексов F и L соответственно. Тогда каждая подпрограмма соответствует функции из декартова произведения, составленного из V, F, L, в другое декартово произведение, составленное аналогичным образом. Например, подпрограмма с заголовком $f(c, a, \mathrm{L1}, \mathrm{F3}/b, \mathrm{L2})$ соответствует функции $f : V \times V \times L \times F \to V \times L$. Будем говорить, что существует композиция подпрограмм f и g, если существует композиция соответствующих функций. Значения входных и выходных параметров подпрограммы будем называть входными и выходными значениями подпрограммы соответственно.

Ранее в языке для получения значения $(gf)(a)$ композиции подпрограмм f и g необходимо было вызвать подпрограмму f на a, скопировать её выходные значения в локальные переменные, подать их на вход функции g и получить её выходные значения. При новой организации памяти можно реализовать более эффективную композицию подпрограмм. Для этого после завершения работы одной подпрограммы стек не возвращается к исходному состоянию, выходные значения завершённой подпрограммы становятся входными значениями следующей в композиции подпрограммы, в стеке выделяется память под выходные значения последней, после чего происходит её вызов. Это позволяет избежать лишнего копирования данных и использования локальных переменных для передачи значений с выхода одной подпрограммы на вход другой.

В ЛЯПАСе вызов функции обозначается следующим образом: $*f(in/out)$, где f — имя подпрограммы; in — список входных значений; out — список выходных значений. Для удобства чтения и понимания программ на ЛЯПАСе композиция обозначена схожим образом: $*f_n*f_{n-1}\ldots*f_1(in_1/out_n)$, где f_1, …, f_n — названия подпрограмм;

in_1 — входные значения первой подпрограммы; out_n — выходные значения последней. При этом компилятор проверяет существование композиции подпрограмм. Для увеличения числа возможных композиций подпрограмм предлагается зафиксировать порядок перечисления входных и выходных параметров: сначала описываются параметры-переменные, затем — параметры-логические комплексы, затем — параметры-символьные комплексы. Эта особенность языка будет полезна при создании крупных библиотек на ЛЯПАСе.

ЛИТЕРАТУРА

1. *Агибалов Г. П., Липский В. Б., Панкратова И. А.* О криптографическом расширении и его реализации для русского языка программирования // Прикладная дискретная математика. 2013. № 3. С. 93–104.
2. *Стефанцов Д. А., Томских П. А.* Разработка операционной системы на языке ЛЯПАС // Прикладная дискретная математика. Приложение. 2015. № 8. С. 134–135.
3. Intel 64 and IA-32 Architectures Software Developer Manuals `http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html`

УДК 519.681.2 DOI 10.17223/2226308X/8/50

ОПЕРАЦИОННАЯ СЕМАНТИКА ЛЯПАСА

А. О. Жуковская, Д. А. Стефанцов

Сообщается о разработке операционной семантики ЛЯПАСа. Описываются её возможные применения: доказательство методом абстрактной интерпретации корректности обращения к элементам комплекса и создание верифицирующего транслятора.

Ключевые слова: *операционная семантика, ЛЯПАС, абстрактная интерпретация, верифицирующий транслятор.*

Язык программирования ЛЯПАС разработан в 1960-х годах в Томском государственном университете, использовался в СССР и других странах, в настоящее время возрождается на кафедре защиты информации и криптографии ТГУ с целью разработки доверенного программного обеспечения [1]. В данной работе сообщается об операционной семантике ЛЯПАСа, которая может применяться как минимум для двух целей: для доказательства формальных свойств программ на ЛЯПАСе и для создания верифицирующего транслятора.

Семантика языка программирования — формализация значений конструкций языка построением их математических моделей. Существует несколько вариантов семантик, самые распространённые — операционные и денотационные семантики. Денотационные семантики основаны на абстракции функций и ориентированы на функциональные языки. Операционные семантики основаны на определении состояний абстрактной машины и переходов между ними. Семантические правила представляют собой переход из одного состояния в другое при соблюдении условий. Для ЛЯПАСа и метода абстрактной интерпретации наиболее подходящий вариантом является операционная семантика.

Под программой понимается синтаксически правильная последовательность команд, представленная нумерованным списком. Состоянием программы на ЛЯПАСе является шестёрка объектов (c, var, τ, EL, Q, S), где c — номер текущей команды; var — массив значений переменных; τ — значение внутренней переменной; EL — массив спис-

ков элементов комплексов; Q и S — массивы мощностей и ёмкостей комплексов соответственно. Операции в ЛЯПАСе можно разделить на четыре группы: операции присваивания, логические и арифметические операции, операции перехода, операции над комплексами. Формулы (1) представляют примеры правил для операций из каждой группы. Это операции занесения значения в переменную, дизъюнкции, перехода по нулю и добавления элемента в комплекс:

$$\begin{gathered}
\frac{p[c] =\Rightarrow \alpha}{(c, var, \tau, EL, Q, S) \longrightarrow (c+1, var[\alpha/\tau], \tau, EL, Q, S)}, \\
\frac{p[c] = \vee\gamma,\ \tau_1 = \tau \vee \gamma}{(c, var, \tau, EL, Q, S) \longrightarrow (c+1, var, \gamma, EL, Q, S)}, \\
\frac{p[c] = 0 \to \delta,\ \tau = 0}{(c, var, \tau, EL, Q, S) \longrightarrow (\delta, var, \tau, EL, Q, S)}, \\
\frac{p[c] = @{>}\phi\xi,\ Q(\phi) < S(\phi),\ \xi \leqslant Q(\phi)}{(c, var, \tau, EL, Q, S) \longrightarrow (c+1, var, \tau, EL[\phi/EL(\phi){:}\mathrm{insert}(\xi, \tau)], Q[\phi/Q(\phi)+1], S)}.
\end{gathered} \tag{1}$$

В используемом на данный момент компиляторе имеется недостаток при работе с комплексами: каждый раз при обращении к элементу производится проверка, не выходит ли индекс за границы комплекса. Это значительно замедляет работу программ, но убирать проверку можно только в тех местах, где есть полная уверенность, что выход за границы комплекса не произойдёт. Для того чтобы получить возможность не тратить время на проверку там, где в этом нет необходимости, нужен способ автоматического доказательства корректности обращения к элементам комплекса. Для построения такого способа может быть применён метод абстрактной интерпретации [2]. Суть метода заключается в том, что семантическим правилам в конкретном домене ставятся в соответствие правила некоторого абстрактного домена, который по структуре проще конкретного. Домены и соответствие между ними должны удовлетворять некоторым правилам. Доказательство производится в абстрактном домене, а затем результат интерпретируется в конкретном.

Опираясь на семантические правила, можно не только доказать отдельные утверждения о программах, но и создать верифицирующий транслятор, что важно для написания доверенного программного обеспечения. Для языка C существует верифицирующий транслятор CompCert [3], основанный на применении средства доказательства теорем Coq [4]. Аналогичный транслятор может быть создан в будущем для ЛЯПАСа.

В дальнейшем для реализации поставленных целей следует представить семантические правила в Coq. Для доказательства корректности обращения к элементам комплекса необходимо задать абстрактный домен и соответствие между семантическими правилами и правилами в абстрактном домене. Для создания верифицирующего транслятора следует задать в Coq семантику машинного языка и построить доказательства корректности переходов, используемых транслятором.

ЛИТЕРАТУРА

1. *Агибалов Г. П., Липский В. Б., Панкратова И. А.* О криптографическом расширении и его реализации для Русского языка программирования. // Прикладная дискретная математика. 2013. № 3. С. 93–105.
2. *Besson F., Cachera D., Jensen T., and Pichardie D.* Certified static analysis by abstract interpretation // Foundations of Security Analysis and Design. 2009. No. 5705. P. 223–257.
3. The CompCert page. `http://compcert.inria.fr/`
4. The Coq Proof Assistant page. `https://coq.inria.fr/`

УДК 004.4'2, 004.4'4 DOI 10.17223/2226308X/8/51

СИСТЕМА УПРАВЛЕНИЯ БИБЛИОТЕКАМИ ДЛЯ ЛЯПАСА

В. О. Сафонов

Предлагается реализация системы управления библиотеками для языка программирования ЛЯПАС. Эта система состоит из трёх основных частей: первая является серверной и отвечает за хранение библиотек, вторая является утилитой для создания библиотек, третья — утилитой, которая позволяет управлять набором библиотек, установленных на компьютере. Описывается формат библиотеки для ЛЯПАСа и система модульной компиляции.

Ключевые слова: *ЛЯПАС, модульная компиляция, библиотека подпрограмм.*

Система управления библиотеками — набор программного обеспечения, позволяющего управлять процессом создания, установки, удаления и обновления библиотек. Такая система является важным инструментом создания программ, так как позволяет находить нужные для решения задачи библиотеки и тем самым существенно сократить время разработки. В настоящий момент транслятор с ЛЯПАСа [1] не поддерживает компиляцию программы из отдельных модулей, в частности не определён формат файла, содержащего библиотеку функций.

Для модульной компиляции выделены три основных требования: 1) компактность исполняемого файла; 2) простота использования; 3) проверка корректности аргументов функции на этапе компиляции. В данный момент предполагается использование статических библиотек ввиду простоты реализации, в будущем планируется использование динамических библиотек.

Компиляция библиотеки разбита на три этапа: 1) трансляция исходного кода на языке ЛЯПАС в набор подпрограмм на языке ассемблера NASM [2]; 2) преобразование набора подпрограмм на языке ассемблера в набор объектных файлов в формате ELF [3]; 3) сборка статической библиотеки из набора объектных файлов. Выходная статическая библиотека содержит отдельный объектный файл для каждой из подпрограмм компилируемой библиотеки.

Можно выделить следующие особенности описанного подхода:

1) Утилита компоновки ld [4] добавляет из статической библиотеки только те объектные файлы, в которых содержится нужная для компоновки функция. В исполняемый файл будут добавлены только используемые функции.
2) Для каждой функции при трансляции в язык ассемблера создается специальная секция [3] с её сигнатурой. Если при компиляции в библиотеках не содержится функции с нужной сигнатурой, то компилятор сообщает об ошибке.
3) Для использования библиотеки необходимо указать её имя при помощи специальной директивы, а при запуске — путь к папке с этой библиотекой.

Система управления библиотеками состоит из трёх подсистем. При помощи утилиты LBuilder можно создавать и редактировать библиотеки. Сервис LServer позволяет создать репозиторий, управлять библиотеками в нём, распространять с его помощью библиотеки. Конечный пользователь при помощи утилиты LManager выбирает репозитории других пользователей и загружает нужные библиотеки.

На данном этапе ведётся разработка функциональности модульной компиляции для существующего компилятора ЛЯПАСа. В будущем планируется описать архитектуру для трёх утилит системы управления библиотеками, а затем разработать их на языке ЛЯПАС, что позволит использовать их в ОС ЛЯПАС.

ЛИТЕРАТУРА

1. *Агибалов Г. П., Липский В. Б., Панкратова И. А.* О криптографическом расширении и его реализации для Русского языка программирования // Прикладная дискретная математика. 2013. №3. С. 93–105.
2. Netwide Assembler. `http://www.nasm.us/`
3. *TIS Committee.* Tool Interface Standard (TIS) Executable and Linking Format (ELF) Specification Version 1.2. 1995.
4. The GNU linker ld (GNU Binutils) version 2.25. `https://sourceware.org/binutils/docs-2.25/ld/index.html`

УДК 004.451.9 DOI 10.17223/2226308X/8/52

РАЗРАБОТКА ОПЕРАЦИОННОЙ СИСТЕМЫ НА ЯЗЫКЕ ЛЯПАС

Д. А. Стефанцов, П. А. Томских

Сообщается о результатах исследований по созданию ОС ЛЯПАС, предназначенной для разработки и запуска программ на ЛЯПАСе. Реализованы следующие функции её ядра: вывод сообщений на экран, инициализация контроллеров устройств, обработка прерываний, взаимодействие с таймером и клавиатурой, многозадачность. Многозадачность демонстрируется несколькими параллельно работающими процессами, которые можно приостанавливать и возобновлять нажатием определённой клавиши. Планируется реализация файловой подсистемы и подсистемы виртуальной памяти.

Ключевые слова: *ЛЯПАС, операционная система.*

ОС ЛЯПАС предназначена для разработки и запуска программ, написанных на языке ЛЯПАС [1]. Предполагается специализация данной ОС для выполнения требовательных к вычислительным ресурсам криптографических алгоритмов. Планируется работа ОС ЛЯПАС на процессорах архитектуры x86-64 с возможностью использовать аппаратные средства для ускорения работы алгоритмов, например выделить одно или несколько ядер процессора полностью под один процесс или использовать графические процессоры для параллельных вычислений. В настоящий момент ОС ЛЯПАС компилируется для 32-битных процессоров архитектуры x86.

В разработке этой ОС можно выделить следующие этапы:

1) Создание транслятора T1 с ЛЯПАСа в язык ассемблера, работающего под управлением GNU/Linux. ЛЯПАС, с которого производится трансляция, обладает дополнительными возможностями по сравнению с ЛЯПАС-Т [1]: доступ к любой ячейке памяти с помощью специального комплекса, возможность использовать адреса процедур в качестве операндов [2].
2) Создание базовых компонент ОС ЛЯПАС — загрузчика и ядра — с помощью T1. После компиляции в машинные коды и расположения этих компонент на диске ОС ЛЯПАС может выполнять некоторые действия, например вывод на экран данных о своей работе.
3) Определение формата исполняемого файла для ОС ЛЯПАС. Возможно, таким форматом станет ELF [3].
4) В ОС ЛЯПАС добавляется возможность запуска программ. Эти программы пишутся в GNU/Linux на языке ЛЯПАС и транслируются в машинный код, представленный в формате исполняемого файла ОС ЛЯПАС, с помощью транслятора T2. Транслятор T2 получается изменением T1.

5) Под управлением GNU/Linux пишется транслятор Т3, который транслирует программы на ЛЯПАСе в машинный код в формате исполняемого файла для ОС ЛЯПАС. Сам Т3 пишется на ЛЯПАСе и транслируется с помощью Т2. После этого шага становится возможным создание программ для ОС ЛЯПАС в самой ОС ЛЯПАС.
6) Исходный текст ОС ЛЯПАС и транслятор Т3 изменяются так, чтобы Т3 мог скомпилировать ОС ЛЯПАС. После этого шага ОС ЛЯПАС можно разрабатывать в самой ОС ЛЯПАС.

На данном этапе разрабатываются загрузчик и ядро ОС ЛЯПАС. В функции загрузчика входят только очистка экрана и загрузка ядра с диска.

Ядро разделено на два модуля. В первом модуле производится переход в защищённый режим и вызов второго модуля. В этом модуле определена также глобальная таблица дескрипторов (GDT) и выделяется память под таблицу дескрипторов прерываний (IDT) [4].

Основные функции ядра находятся во втором модуле. К таким функциям относятся: вывод строк на экран (функция `print(F1/)`, комплекс `F1` — выводимая строка); инициализация контроллеров (функция `init_controllers(/)`); обработка прерываний (функция `timer_interrupt(/)` обрабатывает прерывания от таймера, функция `keyboard_interrupt(/)` — от клавиатуры); заполнение IDT (функция `construct_idt(/)`); переключение процессов (при нажатии клавиши 1, 2 или 3 происходит остановка или возобновление соответствующего процесса, выполняется это функцией `handle_scancode(/)`, которая вызывается функцией `keyboard_interrupt(/)`); многозадачность (функция `timer_interrupt(/)` вызывает планировщик — функцию `scheduler(/)`, который переходит на выполнение следующего процесса). В этом же модуле находится код процессов, демонстрирующих многозадачность (функции `proc_1(/)`, `proc_2(/)`, `proc_3(/)` — бесконечный цикл с выводом названия соответствующей функции, и `proc_0(/)` — бесконечный цикл без действий). Подготовка к переходу к первому процессу осуществляется функцией `kernel(/)`.

На данный момент ОС ЛЯПАС после загрузки переходит к демонстрации многозадачности — поочерёдному выполнению трёх процессов (функции `proc_1(/)`, `proc_2(/)` и `proc_3(/)`). Эти процессы можно приостанавливать и возобновлять нажатием клавишей 1, 2 или 3 соответственно. Если эти три процесса приостановлены, то выполняется процесс `proc_0(/)`.

В ближайшее время планируется добавить некоторые системные вызовы, настроить страничную адресацию, реализовать работу с файлами.

ЛИТЕРАТУРА

1. *Агибалов Г. П., Липский В. Б., Панкратова И. А.* О криптографическом расширении и его реализации для Русского языка программирования // Прикладная дискретная математика. 2013. № 3. С. 93–105.
2. *Гречнев С. Ю., Стефанцов Д. А.* Модификация ЛЯПАС для разработки ОС // Прикладная дискретная математика. Приложение. 2015. № 8. С. 129–131
3. *TIS Committee.* Tool Interface Standard (TIS) Executable and Linking Format (ELF) Specification Version 1.2. 1995.
4. Intel 64 and IA-32 Architectures Software Developer Manuals `http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html`

Секция 8

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 512.55 DOI 10.17223/2226308X/8/53

ПРИМЕНЕНИЕ АЛГОРИТМОВ ЛОКАЛЬНОГО ПОИСКА К РЕШЕНИЮ СИСТЕМ ПСЕВДОБУЛЕВЫХ ЛИНЕЙНЫХ НЕРАВЕНСТВ

Н. В. Анашкина, А. Н. Шурупов

Предложен эвристический алгоритм решения систем псевдобулевых линейных неравенств, являющийся модификацией алгоритма Балаша. Выход из тупиковой точки производится с помощью техники выбора очередного состояния, как в алгоритме имитации отжига. Приводятся результаты экспериментального сравнения предложенного алгоритма и упомянутых эвристик для решения случайных систем линейных неравенств с использованием двух типов целевых функций — суммы и максимума невязок неравенств решаемой системы. Экспериментально установлена бóльшая эффективность предложенного алгоритма. Этот же алгоритм был применён к решению систем линейных неравенств, описывающих линейный регистр сдвига с булевой пороговой функцией выхода. Описывающая линейный регистр сдвига система линейных неравенств характеризуется экспоненциальным числом неравенств по отношению к длине выходной последовательности линейного регистра сдвига. Описываются способы сокращения объёма указанной системы линейных неравенств без сокращения длины выхода. Во всех исследованных случаях предложенный алгоритм находит решения системы линейных неравенств, не всегда совпадающие с оригинальным решением.

Ключевые слова: *алгоритм имитации отжига, алгоритм Балаша, псевдобулевые линейные неравенства.*

Рассмотрим следующую задачу (0-1)-целочисленного линейного программирования:

$$\sum_{i=1}^{n} w_{i,j} x_i \leqslant t_j, \tag{1}$$

где $w_{i,j}, t_j \in \mathbb{Z}$; $x_i \in \{0,1\}$; $j = 1, \ldots, m$.

Известно, что эта задача NP-полна и часто называется задачей решения целочисленной системы линейных неравенств (СЛН) с булевыми неизвестными (такие неравенства также называют псевдобулевыми). В [1] приведены результаты экспериментального сравнения алгоритма Балаша [2] и имитации отжига [3] для решения случайных СЛН вида (1). Рассмотрим модификацию алгоритма Балаша, использующую технику алгоритма имитации отжига для выхода из тупиковых точек. Для краткости будем называть эту модификацию алгоритмом БИО и приведём ниже его псевдокод.

Алгоритм БИО

1) Выбрать случайно начальную точку $\mathbf{x}_0 \in \{0,1\}^n$. Положить $i = 0$.
2) Применить прямой проход алгоритма Балаша к $\mathbf{x}_i$ и получить результат — тупиковую точку $\mathbf{y}$.

3) Если $\mathbf{y}$ — решение (1), то закончить работу. В противном случае выбрать $\mathbf{z}$ из окрестности $S_2(\mathbf{x}_i)$ в соответствии с правилами алгоритма отжига. Положить $i = i + 1$, $\mathbf{x}_i = \mathbf{z}$.
4) Проверить критерии остановки и в случае невыполнения перейти на шаг 2.

Окрестность $S_2(\mathbf{x}_i)$ представляет собой шар радиуса 2 в смысле метрики Хемминга с центром в точке $\mathbf{x}_i$. По сути шаг 3 является попыткой рандомизированного выбора новой точки для повторного применения алгоритма Балаша, сочетающей свойства случайного и направленного поиска, характерные для алгоритма имитации отжига.

В соответствии с методикой, изложенной в [1], проведено экспериментальное исследование эффективности алгоритма БИО в случаях использования разных целевых функций: суммы невязок неравенств и максимума из невязок неравенств. Обе целевые функции часто используются в эвристических алгоритмах (например, вторая — в оригинальном алгоритме Хачияна [4]). Усреднённые результаты исследования для задачи решения заведомо совместной случайной СЛН приведены в таблице. Для сравнения указаны результаты применения к тем же СЛН обычных алгоритмов Балаша и имитации отжига с целевой функцией первого типа. Легко видеть, что алгоритм БИО независимо от используемой целевой функции работает эффективнее алгоритма Балаша или имитации отжига. Однако целевая функция «сумма» позволяет достичь лучших средних результатов (в итоге на 6 %, а в пике — на 14 %) при решении переопределённых СЛН. Для СЛН с числом неравенств равным числу переменных выигрыш принадлежит второй целевой функции. Среднее число шагов алгоритма БИО (число повторений п. 2–4) для первой целевой функции равно 25, а для второй — 124. Тем не менее только на 4 из 12 серий экспериментов алгоритм БИО с первой целевой функцией превосходил по эффективности использование второй целевой функции, хотя более существенно — в среднем 35 % против 8 %.

Сравнение эффективности алгоритма БИО (с использованием разных целевых функций) и классических эвристик

Отношение числа неравенств к числу переменных								Итого	
1		2		3		10			
MAX SA	SUM Balas	MAX SA	SUM Balas	MAX SA	SUM Balas	MAX SA	SUM Balas	MAX SA	SUM Balas
60 %	49 %	84 %	93 %	84 %	99 %	86 %	100 %	79 %	85 %
40 %	15 %	84 %	56 %	85 %	79 %	100 %	99 %	77 %	62 %

Для алгоритма БИО (в варианте с первой целевой функцией) проведены экспериментальные исследования эффективности для решения неслучайных СЛН, в частности, описывающих функционирование фильтрующего генератора на основе линейного регистра сдвига со случайно и равновероятно выбранным начальным заполнением. Более точно, рассматривается автономный линейный регистр сдвига с булевой пороговой функцией в качестве функции выхода, функционирование которого описывается соотношениями $y_i = f(\mathbf{x}_i) = f(\mathbf{x}_{i-1}A) = f(\mathbf{x}_0 A^i)$, где y_i — i-й знак выходной последовательности; $\mathbf{x}_i = (x_1^{(i)}, \ldots, x_m^{(i)})$ — i-е состояние автомата, $i = 0, \ldots, m-1$; A — сопровождающая матрица многочлена $x^n + x^\mu + 1$; f — булева пороговая функция от n переменных с целочисленной структурой $(\mathbf{w}, t)$, $\mathbf{w} = (w_1, \ldots, w_n)$, $w_i, t \in \mathbb{Z}$. Определение булевой пороговой функции, её структуры и других используемых ниже понятий можно найти в [1]. Везде далее будем рассматривать только псевдобулевы целочисленные неравенства.

Для составления СЛН, связывающих выходную последовательность $\mathbf{y} = (y_1, \ldots, y_m)$ с начальным состоянием $\mathbf{x}_0$, необходимо знать пороговое представление булевой функции, задаваемой псевдобулевым неравенством $a_1(v_1 \oplus v_2) + a_2x_2 + \ldots + a_nx_n \leqslant t$. Известно [5], что это неравенство (при $a_1 \neq 0$) равносильно системе из двух линейных псевдобулевых неравенств

$$\begin{cases} a_1v_1 + a_2x_2 + \ldots + a_nx_n - (M - t)v_2 \leqslant t, \\ -a_1v_1 + a_2x_2 + \ldots + a_nx_n + (M - t)v_2 \leqslant M - a_1, \end{cases}$$

где $M = \max\{a_1x_1 + \ldots + a_nx_n : x_i \in \{0, 1\}\}$.

Таким образом, при добавлении очередного знака выходной последовательности размер СЛН может увеличиться вдвое. Для выходной последовательности длины m верхняя оценка числа неравенств равна $2^m - 1$. Существуют приёмы сокращения числа неравенств в системе. Например, с сохранением равносильности можно отбросить неинформативные неравенства [1], т. е. те, которые задают гиперплоскость, не имеющую пересечений с единичным гиперкубом. Условие неинформативности задается неравенством $\rho(\mathbf{w}, t) > \|\mathbf{w}\|\sqrt{n}$, где $\rho(\mathbf{w}, t) = |\sum_{i=1}^{n} w_i - 2t|$. Точно информативными являются неравенства, для которых задаваемая ими гиперплоскость удалена от центра гиперкуба на расстояние не больше $1/2$, или, что то же самое, $\rho(\mathbf{w}, t) \leqslant \|\mathbf{w}\|$. Проведённые экспериментальные исследования выявили отсутствие неинформативных или не точно информативных неравенств в СЛН, порождаемых описанным выше автоматом. Ещё один приём сокращения числа неравенств в СЛН связан с выбором начального состояния $\mathbf{x}_0$. Выбрав начальное состояние равным $\mathbf{x}_{\lfloor m/2 \rfloor}$, можно построить две СЛН, одну — как было описано раньше для выходной последовательности $\mathbf{y}\prime = (y_{\lfloor m/2 \rfloor}, \ldots, y_m)$, а другую — для выходной последовательности $\mathbf{y}\prime\prime = (y_{\lfloor m/2 \rfloor}, y_{\lfloor m/2 \rfloor - 1}, \ldots, y_0)$ обратного регистра сдвига. Размер полученной системы оценивается сверху числом $2^{\lfloor m/2 \rfloor} - 1$.

Так, в одном эксперименте для регистра длины 30, функции от 25 существенных переменных и длины выхода $m = 32$ СЛН с использованием сокращения состоит из 132984 неравенств, а без сокращения — более чем из 3 млн. Алгоритм БИО решил сокращённую систему за 8 шагов, потребовавших 18 с. Найденное решение не совпало с исходным, что свидетельствует о сильной избыточности полученной СЛН.

Авторы приносят благодарность А. А. Фролову за идею выбора начального состояния для сокращения числа неравенств.

ЛИТЕРАТУРА

1. *Анашкина Н. В., Шурупов А. Н.* Экспериментальное сравнение алгоритмов Балаша и имитации отжига в задаче решения систем линейных неравенств // Прикладная дискретная математика. Приложение. 2014. № 7. С. 151–153.
2. *Анашкина Н. В.* Обзор методов решения систем линейных неравенств // Вестник Московского университета леса. Лесной вестник. 2004. № 1(32). С. 144–148.
3. *Кочетов Ю. А.* Вероятностные методы локального поиска для задач дискретной оптимизации // Дискретная математика и ее приложения: Сб. лекций молодежных и научных школ по дискретной математике и ее приложениям. М.: Изд-во центра прикл. исслед. при мех.-мат. фак. МГУ, 2001. С. 84–117.
4. *Хачиян Л. Г.* Полиномиальный алгоритм в линейном программировании // Докл. АН СССР. 1979. Т. 244. № 5. С. 1033–1096.
5. *Балакин Г. В., Никонов В. Г.* Методы сведения булевых уравнений к системам пороговых соотношений // Обозрение прикладной и промышленной математики. 1994. Т. 1. Вып. 3. С. 389–401.

УДК 519.7, 004.832.25 DOI 10.17223/2226308X/8/54

ПРИМЕНЕНИЕ АЛГОРИТМОВ РЕШЕНИЯ ПРОБЛЕМЫ БУЛЕВОЙ ВЫПОЛНИМОСТИ К КРИПТОАНАЛИЗУ ХЭШ-ФУНКЦИЙ СЕМЕЙСТВА MD[1]

И. А. Богачкова, О. С. Заикин, С. Е. Кочемазов, И. В. Отпущенников, А. А. Семёнов

Задачи поиска коллизий криптографических хэш-функций семейства MD рассматриваются как варианты задачи о булевой выполнимости (SAT). Для построения SAT-кодировок алгоритмов MD4 и MD5 использована система Transalg автоматической трансляции алгоритмических описаний дискретных функций в булевы уравнения. Полученные кодировки оказались существенно экономнее известных аналогов. В построенные SAT-кодировки хэш-функций добавлены дополнительные условия, кодирующие известные разностные атаки на данные функции. Время решения SAT-задач, кодирующих поиск одноблоковых коллизий для функции MD4, составило в среднем менее 1 с на ПК средней производительности. Для решения SAT-задач, кодирующих поиск двухблоковых коллизий для функции MD5, использованы параллельные SAT-решатели и вычислительный кластер. В результате был выделен класс двухблоковых коллизий для MD5 с 10 первыми нулевыми байтами. Построено несколько десятков коллизий такого типа. Рассмотрена также задача обращения хэш-функции MD4 (поиск прообраза для фиксированного хэша). В процессе решения данной задачи разработана техника, использующая так называемые «переменные переключения». Использование переменных переключения позволило найти новые дополнительные условия (типа «условий Доббертина»), учёт которых ускорил решение проблемы обращения 39-шагового варианта MD4 в сотни раз.

Ключевые слова: *криптографические хэш-функции, коллизии для хэш-функций, алгоритмы MD4, MD5, задача о булевой выполнимости, SAT.*

Хэш-функциями называются отображения вида $\chi : \{0,1\}^* \to \{0,1\}^c$, где c — некоторая натуральная константа. Хэш-функции используются в целом ряде разделов Computer Science для ускорения работы с данными. В криптографии хэш-функции являются основой большого числа различных криптосистем и протоколов. В отличие от «обычных» хэш-функций, к криптографическим хэш-функциям предъявляются дополнительные условия, требующие, чтобы задачи, связанные с обращением этих функций, были вычислительно трудными. Более точно, трудной должна быть собственно задача обращения: по известному значению хэша y найти вход x (обычно некоторой фиксированной длины), такой, что $\chi(x) = y$. Стандартным является также требование сложности задачи поиска коллизий. Поскольку константа c фиксирована, то для произвольного $n > c$ отображение $\chi : \{0,1\}^n \to \{0,1\}^c$ не может быть биективным. Если при этом χ определена всюду на $\{0,1\}^n$, то существуют такие различные $x_1, x_2 \in \{0,1\}^n$, что $\chi(x_1) = \chi(x_2)$. В этом случае говорят, что пара сообщений x_1, x_2 образует коллизию. Итак, еще одно требование к криптографическим хэш-функциям состоит в том, что задача поиска коллизий должна быть вычислительно трудной.

Одной из наиболее распространённых основ для криптографических хэш-функций является конструкция Меркля — Дамгарда [1, 2]. В соответствии с данной конструкцией двоичный вход x разбивается на блоки фиксированной длины n (этот параметр за-

[1]Работа выполнена при частичной поддержке грантов РФФИ (№ 14-07-31172 мол-а, 14-07-00403 а и 15-07-07891 а); стипендий Президента РФ СП-3667.2013.5, СП-1184.2015.5; Совета по грантам Президента РФ для гос. поддержки ведущих научных школ (НШ-5007.2014.9).

даётся в спецификации алгоритма). При необходимости исходное сообщение дополняется незначащей информацией для получения слова, длина которого кратна n. Пусть x — входное слово, разбитое на N блоков, каждый из которых имеет длину n:

$$x = M_1|\dots|M_N$$

(подразумевается конкатенация блоков). Процесс построения хэша $y = \chi(x)$ — это итеративная процедура вычисления «функции сжатия» (compression function):

$$\chi_i = f(\chi_{i-1}, M_i), \quad i \in \{1, \dots, N\}, \quad \chi_N = y.$$

Для произвольного $i \in \{1, \dots, N\}$ слово χ_i имеет длину c, которая задаётся в спецификации алгоритма; там же задаётся начальное значение (Initial Value) χ_0. Функция сжатия f — это обычно сложная функция, представляемая в виде суперпозиции «раундовых» функций.

Наиболее известными криптографическими хэш-функции, базирующимися на конструкции Меркля — Дамгарда, являются представители семейств MD [3] и SHA. В хэш-функциях MD4 и MD5 $c = 128$, а длина одного блока входного сообщения равна 512 битам. На сегодняшний день, насколько можно судить из открытых источников, даже задача обращения MD4 не имеет эффективного решения для случайных 512-битных входов. Мы не рассматриваем здесь ситуации, связанные с подбором паролей, когда относительно короткий пароль или его «дубликат» можно восстановить по хэшу полным перебором или с использованием различных стратегий пространственно-временного компромисса, таких, например, как Rainbow-метод.

С другой стороны, хорошо известны примеры успешного построения коллизий для функций MD4 и MD5. Первыми работами, в которых продемонстрирован метод, позволяющий устойчиво порождать коллизии для этих функций, являются X. Wang с соавторами [4, 5]. В дальнейшем «метод Wang» неоднократно совершенствовался и модифицировался. К сожалению, мы не можем здесь перечислить все соответствующие ссылки, так как это займёт слишком много места. Метод Wang представляет собой разновидность разностной атаки и может рассматриваться как развитие идей дифференциального криптоанализа [6] (по крайней мере, именно так его позиционирует сама X. Wang). Суть метода Wang заключается в случайном выборе некоторого сообщения с последующей его модификацией, цель которой состоит в «подгонке» получаемой пары сообщений под дифференциальный путь. В [7] предложено использовать алгоритмы решения проблемы булевой выполнимости (SAT) для автоматизации этапа подгонки. С использованием SAT-решателя minisat в [7] довольно эффективно удавалось находить одноблоковые коллизии для хэш-функции MD4. Задача поиска двухблоковых коллизий для MD5 оказалась тем не менее весьма сложной (текст работы [7] не позволяет точно определить ни время, за которое удавалось находить коллизии для MD5, ни число найденных коллизий). Как это ни странно, но результаты работы [7] не получили дальнейшего развития. Это особенно удивительно в свете интенсивного развития технологий решения SAT-задач, наблюдаемого в последние годы [8].

Следующий шаг в использовании SAT-подхода для поиска коллизий хэш-функций семейства MD был сделан, по всей видимости, только в 2014 г. авторами настоящей работы. Полученные в этом направлении результаты опубликованы в [9]. Дадим краткое их описание. Во-первых, отметим основной недостаток работы [7], который состоит в том, что для построения SAT-кодировок использовались узкоспециальные средства кодирования схемных представлений булевых функций. В [9] для этой цели использована система Transalg [10] автоматической трансляции в SAT алгоритмов вычисления

дискретных функций. Полученные кодировки оказались существенно экономнее кодировок, построенных в [7]. Время поиска одноблоковых коллизий для MD4 составило менее 1 с в среднем в сравнении с 10 мин в [7]. При помощи параллельных SAT-решателей в [9] построены семейства двухблоковых коллизий для хэш-функции MD5. Более того, были выделены коллизии специального вида, а именно начинающиеся с 10 нулевых байт (10 примеров таких коллизий приведены в приложении к [9]).

Помимо перечисленного, рассмотрена задача обращения хэш-функции MD4. Ранее к этой задаче также применялся SAT-подход [11]. Однако, как уже отмечалось, до сих пор никому не удалось осуществить успешное обращение полнораундовой версии MD4. В этом смысле рекордное значение равно 39 шагам алгоритма (число шагов в неослабленной версии MD4 равно 48). Атака на версию MD4 с 39 шагами, описанная в [11], требовала около 8 часов работы решателя minisat. При этом в SAT-кодировку добавлялись дополнительные ограничения на некоторые переменные сцепления. Эти ограничения выбирались похожими на ограничения, описанные в [12]. Мы разработали новую технику генерации дополнительных ограничений такого рода. Основная идея состоит в следующем. Пусть C — КНФ, кодирующая задачу обращения некоторой функции χ, и X — множество переменных, фигурирующих в C. Предположим, что к C требуется добавить ограничения, задающие некоторый предикат над переменными из множества $\tilde{X}$, $\tilde{X} \subseteq X$. Пусть $R(\tilde{X})$ — формула, задающая данный предикат. Введём в рассмотрение новую переменную $u \notin X$. Рассмотрим формулу $C \wedge (\overline{u} \vee R(\tilde{X})$. Очевидно, что ограничение $R(\tilde{X})$ учитывается, когда переменная u принимает значение 1. При $u = 0$ ограничение $R(\tilde{X})$ не активно. Переменные типа u называются переменными переключения. В результате варьирования различных значений переменных переключения можно найти набор дополнительных ограничений, учёт которых позволит существенно повысить скорость решения SAT-задачи, кодирующей обращение рассматриваемой функции. При этом для работы с переменными переключения можно использовать различные техники «обучения», встроенные в современные SAT-решатели. В частности, можно рассматривать значения переменных переключения как «assumptions» [13]. На данном этапе мы применили довольно простой механизм перебора значений переменных переключения. В результате найдены ограничения, отличающиеся от приведённых в [11]. Использование новых ограничений сократило время обращения 39-шаговой версии MD4 с нескольких часов до нескольких секунд. В ближайшем будущем мы планируем развивать технику работы с переменными переключения в направлении перебора существенно более широких (чем на текущий момент) множеств дополнительных ограничений.

ЛИТЕРАТУРА

1. *Merkle R. A.* Certified digital signature // LNCS. 1990. V. 435. P. 218–238.
2. *Damgard I. A.* A design principle for hash functions // LNCS. 1990. V. 435. P. 416–427.
3. *Rivest R. L.* The MD4 Message Digest Algorithm // LNCS. 1991. V. 537. P. 303–311.
4. *Wang X., Lai X., Feng D., et.al.* Cryptanalysis of the hash functions MD4 and RIPEMD // LNCS. 2005. V. 3494. P. 1–18.
5. *Wang X. and Yu H.* How to break MD5 and other hash functions // LNCS. 2005. V. 3494. P. 19–35.
6. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. No. 1. P. 3–72.
7. *Mironov I. and Zhang L.* Applications of SAT solvers to cryptanalysis of hash functions // LNCS. 2006. V. 4121. P. 102–115.

8. *Biere A., Heule V., van Maaren H, and Walsh T.* Handbook of Satisfiability. Amsterdam: IOS Press, 2009.
9. *Богачкова И. А., Заикин О. С., Кочемазов С. Е., Отпущенников И. В., Семёнов А. А.* Задачи поиска коллизий для криптографических хеш-функций семейства MD как варианты задачи о булевой выполнимости // Вычислительные методы и программирование. 2015. Т. 16. С. 61–77.
10. *Отпущенников И. В., Семёнов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
11. *De D., Kumarasubramanian A., and Venkatesan R.* Inversion attacks on secure hash functions using SAT solvers // LNCS. 2007. V. 4501. P. 377–382.
12. *Dobbertin H.* The first two rounds of MD4 are not One-Way // Proc. 5th Intern. Workshop Fast Software Encryption. London, UK: Springer Verlag, 1998. P. 284–292.
13. *Nadel A. and Ryvchin V.* Efficient SAT solving under assumptions // LNCS. 2012. V. 7317. P. 242–255.

УДК 519.178 DOI 10.17223/2226308X/8/55

ВЫЧИСЛЕНИЕ ВЕРХНЕЙ ОЦЕНКИ ВЕРШИННОЙ ЦЕЛОСТНОСТИ ГРАФА НА ОСНОВЕ МИНИМАЛЬНЫХ СЕПАРАТОРОВ

В. В. Быкова, Ю. И. Кириллов

Рассматривается трудно вычисляемый числовой параметр графа, называемый вершинной целостностью и используемый в анализе и синтезе отказоустойчивых сложных технических систем. Для нахождения данного параметра необходимо знание всех сепараторов исходного графа. Предлагается алгоритм, который ограничивается построением и анализом только всех минимальных сепараторов. Поэтому алгоритм даёт верхнюю оценку вершинной целостности графа. Вычислительная сложность предлагаемого алгоритма полиномиально зависит от числа вершин и числа минимальных сепараторов графа. Результаты экспериментов показали, что вычисленные оценки являются хорошими и часто достижимыми.

Ключевые слова: *алгоритмы на графах, вершинная целостность графа, минимальные сепараторы.*

Все последние десятилетия проблеме исследования мер целостности графов уделяется особое внимание, поскольку она тесно связана с вопросами анализа и синтеза сложных технических систем, для которых отказоустойчивость является важнейшим показателем качества функционирования. Вершинная целостность — одна из детерминированных мер целостности графа [1].

Пусть $G = (V, E)$ — простой связный граф с множеством вершин V и множеством рёбер E, при этом $n = |V| \geqslant 1$ — порядок графа G. Под вершинной целостностью (*Vertex Integrity*) графа G понимается числовой параметр $I(G)$, вычисляемый по формуле

$$I(G) = \min_{S \subseteq V} \{|S| + w(G - S)\}, \tag{1}$$

где $w(G - S)$ — порядок наибольшей компоненты связности графа $G - S$, который получается из G удалением всех вершин, входящих в $S \subseteq V$. Множество S, для которого достигается равенство в (1), принято называть I-множеством. В неполном связном графе G всякое I-множество является сепаратором этого графа [2]. Доказано [3], что задача вычисления вершинной целостности графа NP-трудная. Ввиду высокой вы-

числительной сложности нахождения точных значений вершинной целостности произвольного графа актуальны нижние и верхние оценки для $I(G)$.

Множество всех вершин графа $G = (V, E)$, смежных с некоторой вершиной $v \in V$, образует в G окрестность вершины v, которая обозначается через $N(v)$. Под замкнутой окрестностью вершины v понимается множество $N[v] = N(v) \cup \{v\}$. Множество вершин $N(S) = \left(\bigcup\limits_{v \in S} N(v) \right) \setminus S$ называется окрестностью для $S \subseteq V$ в G. Множество вершин $S \subseteq V$ разделяет несмежные вершины u и v графа G, если в графе $G - S$ вершины u и v принадлежат различным компонентам связности. Множество S при этом называют (u, v)-сепаратором; (u, v)-сепаратор называют минимальным, если в нём нет собственного подмножества, являющегося (u, v)-сепаратором. Сепаратор S минимальный, если в G существует такая пара вершин u и v, что S является минимальным (u, v)-сепаратором, то есть минимальным относительно, по крайней мере, двух вершин этого графа. Известно, что S — минимальный сепаратор графа G, если и только если существуют две различные области связности C_1 и C_2 графа $G - S$, такие, что $N(C_1) = N(C_2) = S$ [4]. Если S является минимальным (u, v)-сепаратором и $S \subseteq N(v)$, то S называется минимальным сепаратором, близким к v. Обозначим через M множество всех минимальных сепараторов графа $G = (V, E)$. В общем случае множество M может содержать экспоненциальное число сепараторов.

В настоящей работе предлагается алгоритм, позволяющий с помощью минимальных сепараторов вычислять верхнюю оценку меры вершинной целостности и находить соответствующие приближения к I-множествам заданного графа за время $\mathrm{O}(n^3|M|)$. Поиск всех минимальных сепараторов осуществляется по следующему алгоритму.

Алгоритм. Поиск минимальных сепараторов

Вход: Граф $G(V, E)$
Выход: M — множество всех минимальных сепараторов графа G
1. $M := \varnothing$
2. Для каждого $v \in V$
3. $\quad H := G - N[v]$
4. $\quad$ Для каждой области связности C графа H
5. $\quad\quad S := N(v) \cap N(C)$
6. $\quad\quad$ Если $S \neq \varnothing$, то $M := M \cup \{S\}$
7. Для каждого $S \in M$
8. $\quad$ Для каждого $x \in S$
9. $\quad\quad X := S \cup N(x)$
10. $\quad\quad H := G - X$
11. $\quad\quad$ Для каждой области связности C графа H
12. $\quad\quad\quad S := N(C) \cap X$
13. $\quad\quad\quad$ Если $S \neq \varnothing$, то $M := M \cup \{S\}$

Каждый из найденных минимальных сепараторов подставляется в выражение $|S| + w(G - S)$. Минимальное полученное значение I^* является верхней оценкой $I(G)$.

Программный код алгоритма написан на языке C++ в среде разработки Code::Blocks. Вычисленное значение верхней оценки I^* и время работы t_a предложенного алгоритма сравнивались с точным значением вершинной целостности графа, полученным методом полного перебора за время t. Вычислительный эксперимент был проведён на случайных связных графах различных порядков; результаты эксперимента для $n = 20$ представлены в таблице.

№ графа	t	I	t_a	I^*	$I^* - I$	t/t_a
1	31,922	15	0,066	16	1	483,6667
2	27,653	16	0,638	16	0	43,34326
3	27,634	15	3,636	15	0	7,60011
4	25,34	16	16,881	16	0	1,501096
5	25,95	15	0,05	16	1	519
6	26,487	15	0,624	15	0	42,44712
7	26,717	15	5,793	15	0	4,611945
8	26,04	15	0,05	15	0	520,8
9	24,56	15	0,03	16	1	818,6667
10	23,096	14	0,587	14	0	39,34583

Алгоритм был также опробован на графах с известным типом структур (на двумерных решётках, на графах Гретша, Хватала, Хивуда и др.). Результаты экспериментов позволяют говорить о том, что вычисленные значения оценок являются хорошими и часто достижимыми. При этом время нахождения оценки существенно меньше, чем при использовании метода полного перебора. Однако было замечено, что алгоритм даёт бóльшую ошибку на графах с регулярной структурой (например, на двумерной решётке).

ЛИТЕРАТУРА

1. *Быкова В. В.* О мерах целостности графа // Прикладная дискретная математика. 2014. № 4(26). С. 96–111.
2. *Barefoot C. A., Entringer R., and Swart H. C.* Vulnerability in graphs — a comparative survey // J. Combin. Math. Combin. Comput. 1987. No. 1. P. 13–22.
3. *Clark L. H., Entringer R. C., and Fellows M. R.* Computational complexity of integrity // J. Combin. Math. Combin. Comput. 1987. No. 2. P. 179–191.
4. *Berry A. and Bordat J.-P.* Structuring the minimal separators of an undirected graphs. Technical Report 152, LIM, Marseille, 1996.

УДК 681.5.015 DOI 10.17223/2226308X/8/56

ПОСТРОЕНИЕ ФУНКЦИИ ОШИБКИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ИДЕНТИФИКАЦИИ АЛГОРИТМА РАНЖИРОВАНИЯ

О. А. Кожушко

Предлагается функция ошибки для постановки задачи идентификации алгоритма ранжирования результатов текстового поиска. Приводится обоснование некорректности применения функций ошибки, используемых в задачах, где выходные значения принимают действительные значения. В качестве альтернативы предлагается функция ошибки, которая учитывает не абсолютное, а относительное изменение результатов ранжирования. Приводится частный случай постановки задачи идентификации, в которой результат ранжирования рассматривается как класс релевантности.

Ключевые слова: *алгоритм ранжирования, идентификация системы, функция ошибки.*

Задача идентификации системы подразумевает построение модели, устанавливающей взаимосвязь между входными и выходными значениями данной системы, и в общем виде ставится следующим образом [1].

Пусть исходная система реализует неизвестное отображение $F : DX \to DY$. Необходимо построить отображение $M_F : DX \to DY$ таким образом, что $M_F(x) = F(x)$

для всех $x \in DX$. В этом случае исходная система рассматривается как «чёрный ящик», для которого определены входы и выходы, однако неизвестны принципы его функционирования.

Задача идентификации системы в терминах машинного обучения ставится следующим образом. Пусть исходная модель F реализует функцию вида $F : DX \to DY \subset \mathbb{R}^m$. Необходимо построить модель $M_F : DX \to DY \subset \mathbb{R}^m$, такую, что на заданном множестве примеров $X = \{x_i : x_i \in DX, i = 1, \ldots, N\}$

$$E(F, M_F, X) < \varepsilon,$$

где E — функция ошибки; ε — заданная константа.

В данной работе в качестве исследуемой системы рассматривается алгоритм ранжирования. В общем виде алгоритм ранжирования осуществляет отображение вида

$$F_D(q, d) = \mathrm{rank}_D(f(q, d)),$$

где D — рассматриваемая коллекция документов, а функция rank сопоставляет документу порядковый номер в списке документов коллекции, отсортированном по убыванию значения функции релевантности. Функция релевантности f получает на вход пару векторов $\langle q, d\rangle$, описывающих текстовый запрос и документ соответственно, и вычисляет числовую оценку релевантности $r = f(q, d) \in \mathbb{R}$.

Ключевым отличием данной задачи идентификации алгоритма ранжирования от задачи построения ранжирующей функции является то, что выходные значения системы принимают ранговые значения. В настоящее время известно несколько работ, посвящённых решению задачи идентификации алгоритма ранжирования [2], однако в них нет чёткой постановки задачи.

При постановке задачи идентификации необходимо решить две следующих подзадачи. Первая состоит в определении множества входных факторов. Задача подбора факторов, задающих значения компонент входных векторов q и d, обычно решается с помощью экспертной оценки, исходя из эмпирических соображений и априори известной информации. Итоговый набор значимых факторов может быть получен следующими методами:

1) Подбором всех возможных факторов и дальнейшим исключение малозначимых. Значимость фактора может быть определена с помощью корреляционного анализа зависимости между значениями фактора и результатами ранжирования.
2) Методом AdDel [3], суть которого состоит в последовательном добавлении факторов, улучшающих качество идентификации, и удалении факторов, негативно влияющих на качество идентификации.

Вторая подзадача, решению которой посвящена данная работа, вытекает из свойств функции F_D, задающей частичный порядок на множестве пар векторов $\langle q, d\rangle$. Опишем эти свойства в виде леммы.

Лемма 1. Если $F_D(q, d_1) - F_D(q, d_2) = F_D(q, d_3) - F_D(q, d_4)$, то в общем случае $f_D(q, d_1) - f_D(q, d_2) \neq f_D(q, d_3) - f_D(q, d_4)$. То есть если разность рангов документов одинакова для двух пар документов, из этого в общем случае не следует равенство разности значений функции релевантности. Верно и обратное утверждение: если $f_D(q, d_1) - f_D(q, d_2) = f_D(q, d_3) - f_D(q, d_4)$, то в общем случае $F_D(q, d_1) - F_D(q, d_2) \neq$ $\neq F_D(q, d_3) - F_D(q, d_4)$.

Следует отметить, что значение ранга по конкретному запросу напрямую зависит от коллекции документов. Добавление в коллекцию одного документа, релевантного определённому запросу, изменит на 1 ранги множества документов по этому запросу.

Эти свойства функции F_D делают невозможным использование стандартных функций ошибки (таких, как среднеквадратичная функция ошибки MSE), применяемых для неранговых величин. В данной задаче применима следующая функция ошибки:

$$E(F, M_F, Q, D) = \frac{1}{N_D^2 N_Q} \sum_{q \in Q} \sum_{d_i, d_j \in D} |(F_D(q, d_j) - F_D(q, d_j)) - (M_F(q, d_j) - M_F(q, d_j))|,$$

где N_Q — количество запросов в множестве Q; N_D — количество документов в множестве D. С помощью данной функции оценивается разница в последовательностях ранжирования. Попарно сравниваются ранги документов, используемых в ранжировании по тестовым запросам. В случае, когда последовательные в исходном ранжировании документы следуют в модели M_F через k рангов друг от друга, значение функции ошибки увеличивается на $\dfrac{|k-1|}{N_D^2 N_Q}$. Следует отметить, что резкое изменение ранга одного документа в последовательности слабо влияет на значение функции ошибки. Значимые значения функция ошибки принимает в том случае, когда пары документов получают существенно различные ранги.

Задача идентификации может быть сведена к задаче классификации документов по степени релевантности. В этом случае определяется несколько степеней релевантности, например высоко-релевантные и низко-релевантные документы. Выход алгоритма ранжирования определяется не как ранг, а как степень релевантности. Такой подход обоснован тем, что при конструировании исходной системы ранжирования также используются оценки релевантности. Различие состоит в том, что при решении задачи идентификации степень релевантности задается тем, в какой промежуток значений рангов по данному запросу попадает данный документ, а в случае задачи конструирования алгоритма ранжирования — асессорами [4].

Задача классификации имеет следующий вид. Пусть определено M классов релевантности, а функция $\mathrm{class}(\mathrm{rank}(q, d))$ задаёт номер класса релевантности по рангу, присвоенному алгоритмом ранжирования. Необходимо построить идентифицирующую модель M_F, такую, что на заданном множестве примеров $X = \{\langle q, d\rangle_i \in \mathbb{R}^{n+m}, i = 1, \ldots, N\}$

$$E(F, M_F, X) = \frac{1}{N} \sum_{\langle q,d\rangle} I(\mathrm{class}(F_D(q, d), \mathrm{class}(M_F(q, d)) < \varepsilon,$$

где E — функция ошибки; ε — заданная константа;

$$I(x_1, x_2) = \begin{cases} 1, & \text{если } x_1 = x_2, \\ 0 & \text{иначе.} \end{cases}$$

В этом случае используется классическая функция ошибки для задачи классификации. Такой подход был успешно использован в работе [5]. Данная функция позволяет также избежать резких скачков при смене ранга одного документа за счёт интерпретации ранга как степени релевантности. Однако её использование влечёт за собой потерю части информации о разнице в последовательностях документов внутри классов релевантности.

В дальнейшем приведённые подходы могут быть использованы исследователями при построении идентифицирующих моделей как для алгоритмов ранжирования, так и для других функций, задающих частичный порядок на множестве векторов.

ЛИТЕРАТУРА

1. *Семенов А. Д., Артамонов Д. В., Брюхачев А. В.* Идентификация систем управления. Учеб. пособие. Пенза: Изд-во Пенз. ун-та, 2003. 211 с.
2. Материалы компании AlterTrader Research [Электронный ресурс]. `http://www.altertrader.com/` — 21.04.2015.
3. *Загоруйко Н. Г., Кутненко О. А.* Методы распознавания, основанные на алгоритме AdDel // Сиб. журн. индустр. матем. 2004. Т. 7. № 1. С. 39–47.
4. *Воронцов К. В.* Методы обучения ранжированию (Learning to rank). Курс лекций. [Электронный ресурс]. 2013. `http://www.machinelearning.ru/wiki/images/8/89/Voron-ML-Ranking-slides.pdf`
5. *Кожушко О. А., Тарков М. С.* Использование иерархической временной памяти для идентификации системы ранжирования документов // Проблемы информатики. 2015. №1(26). С. 47–54.

УДК 519.688 DOI 10.17223/2226308X/8/57

ПОЛИНОМЫ ХОЛЛА БЕРНСАЙДОВЫХ ГРУПП ПЕРИОДА 3[1]

А. А. Кузнецов, К. В. Сафонов

Пусть $B_k = (k, 3)$ — бернсайдова k-порождённая группа периода 3. В работе вычислены полиномы Холла для B_k при $k \leqslant 4$.

Ключевые слова: *периодическая группа, собирательный процесс, полиномы Холла.*

Пусть $B_k = (k, 3)$ — бернсайдова k-порождённая группа периода 3. Ф. Леви и ван дер Варден доказали [1], что $|B_k| = 3^{k+\binom{k}{2}+\binom{k}{3}}$ и ступень нильпотентности B_k не превышает 3.

Для каждой B_k несложно получить pc-представление (*power commutator presentation*), используя систему компьютерной алгебры GAP или MAGMA.

Пусть $a_1^{x_1} \dots a_n^{x_n}$ и $a_1^{y_1} \dots a_n^{y_n}$ — два произвольных элемента в группе B_k, записанные в коммутаторном виде. Тогда их произведение равно

$$a_1^{x_1} \dots a_n^{x_n} \cdot a_1^{y_1} \dots a_n^{y_n} = a_1^{z_1} \dots a_n^{z_n}.$$

Основой для нахождения степеней z_i является собирательный процесс [2, 3], который реализован в указанных системах компьютерной алгебры. Кроме того, существует альтернативный способ для вычисления произведений элементов группы, предложенный Ф. Холлом [4]. Холл показал, что z_i представляют собой полиномиальные функции (в нашем случае над полем $\mathbb{Z}_3$), зависящие от переменных $x_1, \dots, x_i, y_1, \dots, y_i$, которые принято сейчас называть *полиномами Холла*. Согласно [4],

$$z_i = x_i + y_i + p_i(x_1, \dots, x_{i-1}, y_1, \dots, y_{i-1}).$$

Необходимость применения полиномов Холла возникает при решении задач, требующих многократного умножения элементов группы. Исследование структуры графа Кэли некоторой группы является одной из таких задач. Вычислительные эксперименты на ЭВМ в группах периода пять и семь [5, 6] выявили, что метод полиномов Холла

[1]Работа выполнена при поддержке Министерства образования и науки РФ (проект Б 112/14) и гранта Президента РФ (проект МД-3952.2015.9).

имеет преимущество перед традиционным собирательным процессом. Следует также отметить, что данный метод легко программно реализуем, в том числе на многопроцессорных вычислительных системах.

В настоящей работе вычислены ранее неизвестные полиномы Холла для групп B_k при $k \leqslant 4$. Для $k > 4$ полиномы вычисляются аналогично, однако их вывод занимает значительно больше места. Заметим, что, вычислив полиномы для некоторого k, нетрудно получить полиномы Холла для меньших значений k.

Получим в GAP pc-представление группы B_4.

Коммутаторы веса 1:

$$a_1, a_2, a_3, a_4 \text{ — образующие группы.}$$

Коммутаторы веса 2:

$$a_5 = [a_2, a_1],\ a_6 = [a_3, a_1],\ a_7 = [a_3, a_2],\ a_8 = [a_4, a_1],\ a_9 = [a_4, a_2],\ a_{10} = [a_4, a_3].$$

Коммутаторы веса 3:

$$a_{11} = [a_5, a_3] = [a_2, a_1, a_3],\ a_{12} = [a_5, a_4] = [a_2, a_1, a_4],$$
$$a_{13} = [a_6, a_4] = [a_3, a_1, a_4],\ a_{14} = [a_7, a_4] = [a_3, a_2, a_4].$$

Список определяющих соотношений R для базисных коммутаторов (тривиальные соотношения вида $a_i^3 = 1$ и $[a_j, a_i] = 1$ для краткости не приводятся):

$$[a_2, a_1] = a_5,\ [a_3, a_1] = a_6, [a_3, a_2] = a_7, [a_4, a_1] = a_8,\ [a_4, a_2] = a_9,\ [a_4, a_3] = a_{10},$$
$$[a_5, a_3] = a_{11},\ [a_5, a_4] = a_{12},\ [a_6, a_2] = a_{11}^2,\ [a_6, a_4] = a_{13},\ [a_7, a_1] = a_{11},\ [a_7, a_4] = a_{14},$$
$$[a_8, a_2] = a_{12}^2,\ [a_8, a_3] = a_{13}^2,\ [a_9, a_1] = a_{12},\ [a_9, a_3] = a_{14}^2,\ [a_{10}, a_1] = a_{13},\ [a_{10}, a_2] = a_{14}.$$

Таким образом, $B_4 = \langle\, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14} \mid R \,\rangle$.

Каждый элемент группы выражается единственным образом в виде нормального коммутаторного слова:

$$\forall g \in B_4 \quad (g = a_1^{x_1} a_2^{x_2} a_3^{x_3} a_4^{x_4} a_5^{x_5} a_6^{x_6} a_7^{x_7} a_8^{x_8} a_9^{x_9} a_{10}^{x_{10}}, a_{11}^{x_{11}}, a_{12}^{x_{12}}, a_{13}^{x_{13}}, a_{14}^{x_{14}}), \quad x_i \in \mathbb{Z}_3.$$

Основным результатом настоящей работы является

Теорема 1. Пусть $a_1^{x_1} \dots a_{14}^{x_{14}}$ и $a_1^{y_1} \dots a_{14}^{y_{14}}$ — два произвольных элемента в группе B_4, записанные в коммутаторном виде. Тогда их произведение равно $a_1^{x_1} \dots a_{14}^{x_{14}} \times$ $\times\, a_1^{y_1} \dots a_{14}^{y_{14}} = a_1^{z_1} \dots a_{14}^{z_{14}}$, где $z_i \in \mathbb{Z}_3$ — полиномы Холла, задаваемые следующими формулами:

$$z_1 = x_1 + y_1,$$
$$z_2 = x_2 + y_2,$$
$$z_3 = x_3 + y_3,$$
$$z_4 = x_4 + y_4,$$
$$z_5 = x_5 + y_5 + x_2 y_1,$$
$$z_6 = x_6 + y_6 + x_3 y_1,$$
$$z_7 = x_7 + y_7 + x_3 y_2,$$
$$z_8 = x_8 + y_8 + x_4 y_1,$$
$$z_9 = x_9 + y_9 + x_4 y_2,$$
$$z_{10} = x_{10} + y_{10} + x_4 y_3,$$

$$z_{11} = x_{11} + y_{11} + x_5y_3 + 2x_6y_2 + x_7y_1 + x_2x_3y_1 + x_2y_1y_3 + 2x_3y_1y_2,$$
$$z_{12} = x_{12} + y_{12} + x_5y_4 + 2x_8y_2 + x_9y_1 + x_2x_4y_1 + x_2y_1y_4 + 2x_4y_1y_2,$$
$$z_{13} = x_{13} + y_{13} + x_{10}y_1 + x_6y_4 + 2x_8y_3 + x_3x_4y_1 + x_3y_1y_4 + 2x_4y_1y_3,$$
$$z_{14} = x_{14} + y_{14} + x_{10}y_2 + x_7y_4 + 2x_9y_3 + x_3x_4y_2 + x_3y_2y_4 + 2x_4y_2y_3.$$

ЛИТЕРАТУРА

1. *Levi F. and van der Waerden B.* Uber eine besondere Klasse von Gruppen // Abh. Math. Sem. Univ. Hamburg. 1933. No. 9. S. 154–158.
2. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.
3. *Holt D., Eick B., and O'Brien E.* Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.
4. *Hall P.* Nilpotent groups, Notes of lectures given at the Canadian Mathematical Congress 1957 Summer Seminar, in The collected works of Philip Hall. Oxford: Clarendon Press, 1988. P. 415–462.
5. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. №1. С. 110–116.
6. *Кузнецов А. А. Сафонов К. В.* Hall's polynomials of finite two-generator groups of exponent seven // Журнал СФУ. Сер. математика и физика. 2014. №2. С. 186–190.

УДК 512.54.05+519.712.4 DOI 10.17223/2226308X/8/58

О СЛОЖНОСТИ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В ИНТЕРВАЛЕ В ГРУППЕ С ЭФФЕКТИВНЫМ ИНВЕРТИРОВАНИЕМ

М. В. Николаев

Задача дискретного логарифмирования в интервале заключается в поиске для заданной конечной группы G (с аддитивной записью операции), заданных $P, Q \in G$, $N < |G| - 1$ такого значения n, что $Q = nP$, $0 \leqslant n \leqslant N$. Одним из наиболее эффективных методов решения данной задачи является алгоритм Годри — Шоста. В 2010 г. С. Гэлбрейт и К. Руправи представили усовершенствованную версию алгоритма для групп с эффективным инвертированием. Оценка средней трудоёмкости решения задачи составила $(1{,}36 + o(1))\sqrt{N}$ групповых операций в G при $N \to \infty$. В настоящей работе приводится новая модификация алгоритма Годри — Шоста для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием и получена оценка средней трудоёмкости, составляющая $(1 + \varepsilon)\sqrt{\pi N/2}$ групповых операций в G.

Ключевые слова: *задача дискретного логарифмирования в интервале, алгоритм Годри — Шоста.*

Приведём постановки задач.

Определение 1. Задача дискретного логарифмирования.
Дано: группа $G = \langle P \rangle$, $Q \in G$.
Найти: $n \in \{0, \ldots, |G| - 1\}$, такое, что $Q = nP$.

Определение 2. Задача дискретного логарифмирования в интервале.
Дано: группа $G = \langle P \rangle$, $Q \in G$, $N \in \mathbb{N}$, $2|N$, $N < |G| - 1$, $Q = nP$ для некоторого (неизвестного) $n \in \{-N/2, \ldots, N/2\}$.
Найти: n.

В настоящее время в общем случае одним из наиболее эффективным алгоритмом решения задачи дискретного логарифмирования в интервале является алгоритм Годри — Шоста [1]. Основная его идея может быть сформулирована следующим образом. Сначала выбираются так называемые «домашнее» (tame) и «дикое» (wild) множества:

$$T = \{-N/2, \ldots, N/2\}, \quad W = \{-N/2 + n, \ldots, N/2 + n\}.$$

Затем параллельно вычисляются псевдослучайные последовательности

$$x_i P, \quad x_i \in T, \quad i = 1, 2, \ldots; \tag{1}$$

$$Q + z_j P, \quad (n + z_j) \in W, \quad j = 1, 2, \ldots \tag{2}$$

до тех пор, пока в них не найдутся два одинаковых элемента

$$x_k P = Q + z_l P, \tag{3}$$

откуда находим $n = x_k - z_l$.

Средняя трудоёмкость алгоритма Годри — Шоста и его различных модификаций, измеряемая количеством групповых операций в G, равна по порядку величины среднему значению количества элементов последовательностей, вычисляемых до появления совпадающих элементов, в предположении, что значения n, x_i и z_j выбираются случайно равновероятно и независимо из соответствующих множеств. Это среднее значение может быть получено с использованием результата [2], являющегося обобщением парадокса дней рождения.

Предположим теперь, что группа G обладает эффективно вычислимой операцией φ взятия обратного элемента, т. е. время, необходимое для вычисления обратного элемента, существенно меньше времени, необходимого для выполнения одной групповой операции. Тогда группа G распадается на непересекающиеся классы эквивалентности (орбиты) относительно действия φ, и подобно тому, как это делается в работе [3] для классической задачи дискретного логарифмирования, можно ускорить алгоритм, если искать не совпадающие элементы последовательностей (1) и (2), а совпадающие классы эквивалентности этих элементов. Действительно, в этом случае вместо равенства (3) имеем равенство

$$\varphi^s(x_k P) = Q + z_l P$$

для некоторого s, откуда

$$Q = ((-1)^s x_k - z_l)P,$$

т. е. $n = (-1)^s x_k - z_l$.

Примером такой группы *с эффективным инвертированием* является группа точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов. Действительно, $\varphi(x, y) = (x, -y)$, т. е. $\varphi(aP) = -aP$ и класс эквивалентности точки aP относительно действия группы $\langle\varphi\rangle$ состоит из aP и $\varphi(aP)$. Каждому такому классу эквивалентности соответствует множество $\{a, -a\}$.

В [4] для этого случая предложена соответствующая модификация алгоритма Годри — Шоста, имеющая при $N \to \infty$ трудоёмкость $(1{,}36 + \mathrm{o}(1))\sqrt{N}$ групповых операций.

В настоящей работе конструктивно доказывается возможность дальнейшего улучшения оценки средней трудоёмкости решения задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием. Основной результат может быть сформулирован в виде следующей теоремы.

Теорема 1. Пусть G — циклическая группа с эффективным инвертированием, пусть также $2|N$. Тогда для любого $\varepsilon > 0$ существует такой алгоритм решения задачи дискретного логарифмирования в интервале в группе G, что при случайном равновероятном выборе n его средняя трудоёмкость не превосходит $(1+\varepsilon)\sqrt{\pi N/2} + \mathrm{O}_\varepsilon(N^{1/4})$ групповых операций, где $N \to \infty$.

Здесь запись O_ε означает, что константа под символом O зависит от ε. Подробное изложение представленных результатов можно найти в [5].

ЛИТЕРАТУРА

1. *Gaudry P. and Schost E.* A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm // LNCS. 2004. V. 3076. P. 208–222.
2. *Galbraith S. D. and Holmes M.* A non-uniform birthday problem with applications to discrete logarithms // Discr. Appl. Math. 2012. V. 160. No. 10–11. P. 1547–1560. `eprint.iacr.org/2010/616`.
3. *Wiener M. J. and Zuccherato R. J.* Faster attacks on elliptic curve cryptosystems // LNCS. 1999. V. 1556. P. 190–200.
4. *Galbraith S. D. and Ruprai R. S.* Using equivalence classes to accelerate solving the Discrete Logarithm Problem in a short interval // LNCS. 2010. V. 6056. P. 368–383. `eprint.iacr.org/2010/615`.
5. *Николаев М. Н.* О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием // Прикладная дискретная математика. 2015. № 2(28). С. 97–102.

УДК 621.396:621.372 DOI 10.17223/2226308X/8/59

РЕАЛИЗАЦИЯ НЕЙРОННОЙ WTA-СЕТИ НА МЕМРИСТОРНОМ КРОССБАРЕ

М. С. Тарков

Предложен алгоритм отображения матрицы весовых коэффициентов нейронной WTA-сети на мемристорный кроссбар. Выполнено моделирование нейронной WTA-сети, построенной на основе мемристорного кроссбара, с использованием программы LTSPICE. Полученные результаты могут быть использованы как при математическом моделировании, так и при физической реализации нейронных сетей с межнейронными связями на мемристорах.

Ключевые слова: *мемристор, сопротивление мемристора, кроссбар, нейронная сеть, матрица весовых коэффициентов, WTA.*

Искусственная нейронная сеть обычно использует матрицу весовых коэффициентов для представления множества синапсов слоя нейронов. Соответственно вычисление активации слоя нейронов можно рассматривать как умножение этой матрицы весов на вектор входных сигналов слоя. Аппаратная реализация нейронной сети требует много памяти для хранения матрицы весов слоя нейронов и является дорогостоящей.

Решение этой проблемы упрощается при использовании в качестве ячейки памяти устройства, называемого мемристором. Мемристор был предсказан теоретически в 1971 г. Леоном Чуа [1]. Первую физическую реализацию мемристора продемонстрировала в 2008 г. лаборатория фирмы «Hewlett Packard» в виде тонкоплёночной структуры TiO_2 [2]. В России первый мемристор на основе TiO_2 получен в 2012 г. в Тюменском государственном университете.

Мемристор имеет много достоинств, таких, как энергонезависимость хранения информации, малое потребление энергии, высокая плотность интеграции и замечательная масштабируемость. Уникальная способность сохранять следы возбуждения устройства делает его идеальным кандидатом для реализации синапсов в электронных нейронных сетях. Мемристор ведет себя подобно синапсу: он «запоминает» полный электрический заряд, прошедший через него. Память, основанная на мемристорах, может достигать очень высокой степени интеграции 100 Гбит/см^2, в несколько раз более высокой, чем на основе технологии флэш-памяти. Эти уникальные свойства делают мемристор многообещающим устройством для создания массово-параллельных нейроморфных систем.

Мемристорный кроссбар содержит мемристор на каждом пересечении горизонтальных и вертикальных проводников. Он интересен для реализации матриц соединений в нейронных сетях, поскольку может обеспечить большое число сигнальных связей и вычислить взвешенную комбинацию входных сигналов.

Слой WTA-нейронов (Winner Takes All) может быть описан выражением

$$y_i = f(a_i), \quad a_i = \sum_{j=0}^{N} w_{ij} x_j, \tag{1}$$

где w_i — вектор весов i-го нейрона, $i = 1, \ldots, p$; f — функция активации нейрона; x — вектор входных сигналов слоя нейронов; y_i — выходной сигнал i-го нейрона. Предполагается, что x_j, $j = 1, \ldots, N$ — сигналы, образованные входным объектом сети, $x_0 \equiv 1$, w_{i0} — порог i-го нейрона.

Входной вектор x относится слоем нейронов к классу i при выполнении неравенства

$$a_i > a_j, \ j \in \{1, \ldots, p\}, \ j \neq i.$$

Положим

$$f(a) = \begin{cases} 1, & a > 0, \\ 0, & a \leqslant 0. \end{cases} \tag{2}$$

Пусть на вход слоя поступает множество попарно различимых объектов $\{x^i = (x^i_1, \ldots, x^i_N)\}$, т. е. $x^i \neq x^j$ при $i \neq j$, причём $x^i_k = \pm 1$. Такими объектами могут быть бинарные изображения. Пусть каждый из объектов x^i содержит m компонентов, равных 1 («белый цвет»), и n компонентов, равных -1 («чёрный цвет»), $m + n = N$, то есть объекты отличаются друг от друга цветами пикселей (рис. 1).

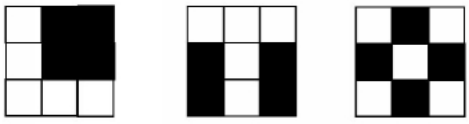

Рис. 1. Изображения символов L, T и X

Поставим в соответствие белому пикселю вес $w_{ij} = W_{\max}$, а чёрному — $w_{ij} = W_{\min}$, где $W_{\max} > W_{\min}$ — заданные значения. Положим порог $w_{i0} = 0$, $i = 1, \ldots, p$. Тогда i-й нейрон выигрывает соревнование при входном векторе x^i, поскольку

$$a_i = (x^i, w_i) = mW_{\max} - nW_{\min}; \tag{3}$$

$$a_j = (x^i, w_j) \leqslant (m-1)W_{\max} - (n+1)W_{\min}, \tag{4}$$

что соответствует принципу WTA.

Полагая порог $w_{i0} = (m-1)W_{\max} - (n+1)W_{\min}$, из (1)–(4) получаем

$$a_i = W_{\max} - W_{\min} > 0,\ f(a_i) = 1;$$
$$a_j < 0,\ f(a_j) = 0,\ j \neq i.$$

Отображение данного варианта WTA-сети на мемристорный кроссбар сводится к заданию весов сети посредством проводимостей мемристоров кроссбара.

На рис. 2 представлена реализация в симуляторе LTspice IV [3] WTA-сети из трёх нейронов на базе мемристорного кроссбара для распознавания изображений символов L, T и X (рис. 1). На вертикальные шины кроссбара подаются компоненты вектора входных сигналов. Каждый горизонтальный ряд мемристоров образует адаптивный сумматор, вычисляющий активацию нейрона, транзистор NMOS реализует функцию активации (2). Например, нейрон, распознающий символ L, образован мемристорами M10–M19, транзистором T1 и резистором R1. В качестве выходных сигналов нейронов соответственно рассматриваются напряжения на резисторах R1, R2 и R3. Входные сигналы задаются источниками напряжения V0–V9, V10 — источник питания транзисторов T1–T3. Сопротивления мемристоров, соответствующих входным сигналам, равны $R_{\min} = 3 \cdot 10^3$ Ом, $R_{\max} = 6 \cdot 10^3$ Ом, $W_{\min} = 1/R_{\max}$, $W_{\max} = 1/R_{\min}$. Проводимость пороговых мемристоров M10–M30 равна $W_0 = (m-1)W_{\max} - (n+1)W_{\min} = 4W_{\max} - 5W_{\min} = 1/R_0$, где сопротивление $R_0 = 2 \cdot 10^3$ Ом. В экспериментах использовалась SPICE-модель мемристора из [4, 5]. Эксперименты показали, что предложенная реализация нейронной WTA-сети может быть успешно использована для распознавания изображений.

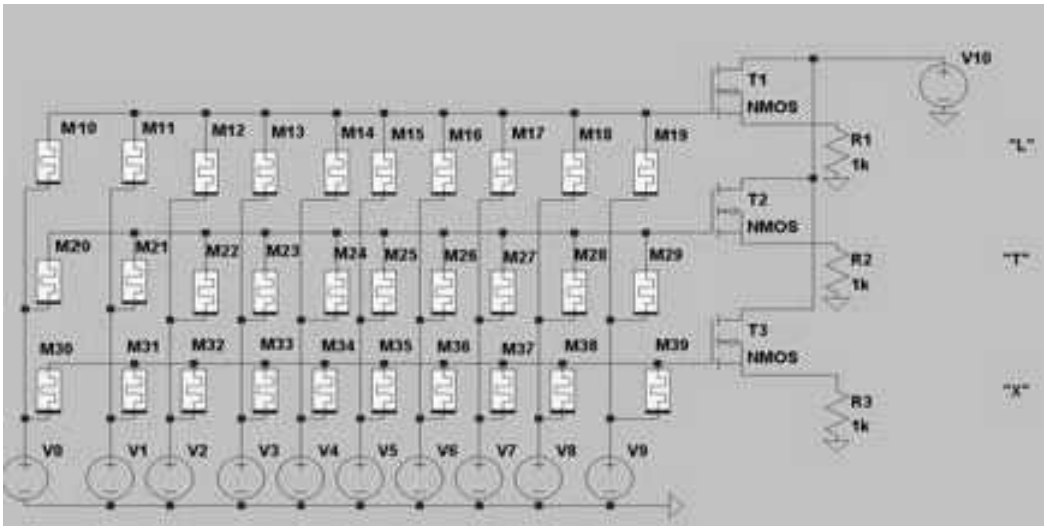

Рис. 2. WTA-сеть

ЛИТЕРАТУРА

1. *Chua L.* Memristor — the missing circuit element // IEEE Trans. Circuit Theory. 1971. V. 18. P. 507–519.
2. *Strukov D. B., Snider G. S., Stewart D. R., and Williams R. S.* The missing memristor found // Nature. 2008. V. 453. P. 80–83.
3. *Володин В. Я.* Компьютерное моделирование электронных схем. СПб.: БХВ-Петербург, 2010. 400 с.

4. *Biolek Z., Biolek D., and Biolkova V.* SPICE model of memristor with nonlinear dopant drift // Radioengineering. 2009. V. 18. No. 2. P. 210–214.
5. `http://www.falatic.com/index.php/69` — Memristor simulation with LTspice — a practical example! 2015.

СВЕДЕНИЯ ОБ АВТОРАХ

АБРОСИМОВ Михаил Борисович — доктор физико-математических наук, профессор Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **mic@rambler.ru**

АВЕЗОВА Яна Эдуардовна — аспирантка Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: **avezovayana@gmail.com**

АГИБАЛОВ Геннадий Петрович — доктор технических наук, профессор, заведующий кафедрой защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **agibalov@isc.tsu.ru**

АЛЕХИНА Марина Анатольевна — доктор физико-математических наук, профессор, заведующая кафедрой Пензенского государственного университета, г. Пенза. E-mail: **ama@sura.ru**

АНАШКИНА Наталия Викторовна — кандидат технических наук, доцент, Лаборатория ТВП, г. Москва. E-mail: **6237030@mail.ru**

АНИСЕНЯ Николай Ильич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **anisenya@gmail.com**

БАРСУКОВА Оксана Юрьевна — старший преподаватель Пензенского государственного университета, г. Пенза. E-mail: **kuzya_7@mail.ru**

БОГАЧКОВА Ирина Александровна — студентка Института математики, экономики и информатики, г. Иркутск. E-mail: **the42dimension@gmail.com**

БОНДАРЕНКО Леонид Николаевич — кандидат технических наук, доцент, доцент кафедры дискретной математики Пензенского государственного университета, г. Пенза.
E-mail: **leobond5@mail.ru**

БРОСЛАВСКИЙ Олег Викторович — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **o.v.broslavsky@gmail.com**

БЫКОВА Валентина Владимировна — доктор физико-математических наук, профессор Сибирского федерального университета, г. Красноярск. E-mail: **bykvalen@mail.ru**

ВИТКУП Валерия Александровна — студентка механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **vvitkup@yandex.ru**

ГОРОДИЛОВА Анастасия Александровна — аспирантка Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **gorodilova@math.nsc.ru**

ГРАБОВСКАЯ Светлана Михайловна — кандидат физико-математических наук, старший преподаватель Пензенского государственного университета, г. Пенза. E-mail: **swetazin@mail.ru**

ГРЕЧНЕВ Сергей Юрьевич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета.
E-mail: **sgrechnev@gmail.com**

ДЕВЯНИН Петр Николаевич — доктор технических наук, доцент, председатель УМС УМО по ИБ, г. Москва. E-mail: **peter_devyanin@hotmail.com**

ДОРОХОВА Алиса Михайловна — аспирантка кафедры криптологии и дискретной математики НИЯУ МИФИ, аналитик ООО «Код Безопасности», г. Москва. E-mail: **a.dorokhova@kaf42.ru**

ЕГОРОВА Вера Владимировна — магистрантка Новосибирского государственного университета, программист Лаборатории современных компьютерных технологий НИЧ НГУ, г. Новосибирск.
E-mail: **vvegorova@gmail.com**

ЕПИШКИНА Анна Васильевна — кандидат технических наук, доцент кафедры криптологии и дискретной математики Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: **avepishkina@mephi.ru**

ЖАРКОВА Анастасия Владимировна — кандидат физико-математических наук, доцент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **VAnastasiyaV@gmail.com**

ЖУКОВСКАЯ Александра Олеговна — студентка кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **zhuka157@yandex.ru**

ЗАИКИН Олег Сергеевич — кандидат технических наук, научный сотрудник Института динамики систем и теории управления им. В. М. Матросова, г. Иркутск. E-mail: **zaikin.icc@gmail.com**

ИВАЧЕВ Артем Сергеевич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **ivachyou@gmail.com**

КАРГИН Степан Павлович — аспирант Пензенского государственного университета, г. Пенза. E-mail: **dm@pnzgu.ru**

КАРОНДЕЕВ Андрей Михайлович — студент кафедры информационной безопасности МГТУ им. Н. Э. Баумана, г. Москва. E-mail: **karondeev@yandex.ru**

КАРПОВ Артем Валерьевич — аспирант кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **karpov@isc.tsu.ru**

КИРИЛЛОВ Юрий Игоревич — аспирант Сибирского федерального университета, г. Красноярск. E-mail: **yurikirillov1991@gmail.com**

КОГОС Константин Григорьевич — аспирант Национального исследовательского ядерного университета «МИФИ», г. Москва. E-mail: **kgkogos@mephi.ru**

КОЖУШКО Оюна Алексеевна — аспирантка Новосибирского государственного университета, г. Новосибирск. E-mail: **oyuna@mail.ru**

КОЛЕГОВ Денис Николаевич — кандидат технических наук, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **d.n.kolegov@gmail.com**

КОЛОМЕЕЦ Николай Александрович — кандидат физико-математических наук, научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск.
E-mail: **nkolomeec@gmail.com**

КОЧЕМАЗОВ Степан Евгеньевич — программист Института динамики систем и теории управления им. В. М. Матросова, г. Иркутск. E-mail: **veinamond@gmail.com**

КУЗНЕЦОВ Александр Алексеевич — доктор физико-математических наук, профессор, директор института Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнёва, г. Красноярск. E-mail: **alex_kuznetsov80@mail.ru**

КУЦЕНКО Александр Владимирович — студент механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **AlexandrKutsenko@bk.ru**

КЯЖИН Сергей Николаевич — аспирант кафедры криптологии и дискретной математики Национального исследовательского ядерного университета «МИФИ», математик Центра специальных разработок МО РФ, г. Москва. E-mail: **s.kyazhin@kaf42.ru**

МАЛЮГИН Сергей Артемьевич — доктор физико-математических наук, ведущий научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск.
E-mail: **mal@math.nsc.ru**

МЕДВЕДЕВА Наталья Валерьевна — кандидат физико-математических наук, доцент, доцент Уральского государственного университета путей сообщения, г. Екатеринбург.
E-mail: **medvedeva_n_v@mail.ru**

МИЛОВАНОВ Тимофей Игоревич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **timcess@gmail.com**

МОДЕНОВА Ольга Владимировна — аспирантка Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **oginiel@rambler.ru**

НИКОЛАЕВ Максим Владимирович — аспирант кафедры информационной безопасности Московского государственного университета им. М. В. Ломоносова, г. Москва.
E-mail: **max.abstract@gmail.com**

ОБЛАУХОВ Алексей Константинович — студент Новосибирского государственного университета, г. Новосибирск. E-mail: **oblaukhov@gmail.com**

ОВСЯННИКОВ Станислав Владимирович — аспирант кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **naphaso@gmail.com**

ОЛЕКСОВ Никита Евгеньевич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **n.e.oleksov@gmail.com**

ОТПУЩЕННИКОВ Илья Владимирович — кандидат технических наук, научный сотрудник Института динамики систем и теории управления им. В. М. Матросова, г. Иркутск.
E-mail: **otilya@yandex.ru**

ПАНКРАТОВА Ирина Анатольевна — кандидат физико-математических наук, доцент, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **pank@isc.tsu.ru**

ПЕСТУНОВ Андрей Игоревич — кандидат физико-математических наук, доцент кафедры информационной безопасности Новосибирского государственного университета экономики и управления, г. Новосибирск. E-mail: **pestunov@gmail.com**

ПОГОРЕЛОВ Борис Александрович — доктор физико-математических наук, профессор, действительный член Академии криптографии Российской Федерации, г. Москва.

ПОКРАСЕНКО Денис Павлович — студент механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **L_P_D@mail.ru**

ПОТАПОВ Владимир Николаевич — кандидат физико-математических наук, старший научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск.
E-mail: **vpotapov@math.nsc.ru**

ПОТТОСИН Юрий Васильевич — кандидат физико-математических наук, доцент, ведущий научный сотрудник Объединенного института проблем информатики НАН Беларуси, г. Минск.
E-mail: **pott@newman.bas-net.by**

ПУДОВКИНА Марина Александровна — кандидат физико-математических наук, доцент Национального исследовательского ядерного университета «МИФИ», г. Москва.
E-mail: **maricap@rambler.ru**

РЫБАКОВ Андрей Валентинович — аспирант кафедры дискретной математики Пензенского государственного университета, г. Пенза. E-mail: **anajrov@gmail.com**

РЫБАЛОВ Александр Николаевич — кандидат физико-математических наук, доцент кафедры математической логики и логического программирования Омского государственного университета им. Ф. М. Достоевского, г. Омск, старший научный сотрудник Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **alexander.rybalov@gmail.com**

САЛИЙ Вячеслав Николаевич — кандидат физико-математических наук, профессор, заведующий кафедрой теоретических основ компьютерной безопасности и криптографии Саратовского государственного университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **SaliiVN@info.sgu.ru**

САФОНОВ Вадим Олегович — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **vsaffonov.1115@gmail.com**

САФОНОВ Константин Владимирович — доктор физико-математических наук, профессор, заведующий кафедрой Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнёва, г. Красноярск. E-mail: **safonovkv@rambler.ru**

СЕМЕНОВ Александр Анатольевич — кандидат технических наук, заведующий лабораторией дискретного анализа и прикладной логики Института динамики систем и теории управления им. В. М. Матросова, г. Иркутск. E-mail: **biclop.rambler@yandex.ru**

СТЕФАНЦОВ Дмитрий Александрович — старший преподаватель кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета. E-mail: **d.a.stefantsov@isc.tsu.ru**

ТАРКОВ Михаил Сергеевич — кандидат технических наук, доцент, старший научный сотрудник Института физики полупроводников СО РАН, г. Новосибирск. E-mail: **tarkov@isp.nsc.ru**

ТИТОВ Сергей Сергеевич — доктор физико-математических наук, профессор, профессор Уральского государственного университета путей сообщения, г. Екатеринбург. E-mail: **stitov@usaaa.ru**

ТКАЧЕНКО Николай Олегович — аспирант Национального исследовательского Томского государственного университета, г. Томск. E-mail: **n.o.tkachenko@gmail.com**

ТОКАРЕВА Наталья Николаевна — кандидат физико-математических наук, старший научный сотрудник Института математики им. С. Л. Соболева, г. Новосибирск.
E-mail: **tokareva@math.nsc.ru**

ТОМСКИХ Павел Александрович — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета.
E-mail: **pavlic148@gmail.com**

ТРЕНЬКАЕВ Вадим Николаевич — кандидат технических наук, доцент, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **tvnik@sibmail.com**

ТРЕПАЧЕВА Алина Викторовна — аспирантка Южного федерального университета, г. Ростов-на-Дону. E-mail: **alina1989malina@ya.ru**

ФЕДОРЯЕВА Татьяна Ивановна — кандидат физико-математических наук, доцент, старший научный сотрудник Института математики им. С. Л. Соболева, г. Новосибирск.
E-mail: **fti@math.nsc.ru**

ФОМИЧЕВ Владимир Михайлович — доктор физико-математических наук, профессор, профессор Финансового университета при Правительстве Российской Федерации, заместитель по науке технического директора ООО «Код Безопасности», г. Москва. E-mail: **fomichev@nm.ru**

ЧЕРЕМУШКИН Александр Васильевич — доктор физико-математических наук, член-корреспондент Академии криптографии РФ, г. Москва. E-mail: **avc238@mail.ru**

ЧЕЧУЛИНА Дарья Константиновна — магистрантка Новосибирского государственного университета, программист Лаборатории современных компьютерных технологий НИЧ НГУ, г. Новосибирск. E-mail: **dashachechulina@gmail.com**

ШАРАПОВА Марина Леонидовна — старший преподаватель кафедры математического анализа механико-математического факультета Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **msharapova@list.ru**

ШУРУПОВ Андрей Николаевич — кандидат технических наук, доцент, МИРЭА, г. Москва. E-mail: **ashurupov@mail.ru**

ШУШУЕВ Георгий Иннокентьевич — аспирант Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **g.shushuev@gmail.com**

АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ

SECTION 1

Bondarenko L. N., Sharapova M. L. **MACMAHON'S STATISTICS PROPERTIES ON SETS OF WORDS.** Properties of MacMahon's statistics of maj and inv are considered on three sets of words over $\{1, \ldots, n\}$: 1) permutations of degree n; 2) all words of length n; 3) concave permutations of degree n. New recursive descriptions of the generating polynomials of couples $(\mathrm{des}, \mathrm{maj})$ and $(\mathrm{des}, \mathrm{inv})$ are obtained on sets 1 and 3; the corresponding recursive descriptions on the set 2 are only obtained for $(\mathrm{des}, \mathrm{maj})$ and for statistics inv. On the sets 1 and 2, these recursive descriptions are used for another proof of the known MacMahon's theorem about the coincidence of distributions of maj and inv. On the set 2, the statistics of fas and cas are defined as special average values of a symbol in a word, fas and des are equally distributed, and the theorem of coincidence of distributions of couples $(\mathrm{fas}, \mathrm{maj})$ and $(\mathrm{fas}, \mathrm{inv})$, and also of couples $(\mathrm{cas}, \mathrm{maj})$ and $(\mathrm{cas}, \mathrm{inv})$ is proved.
Keywords: *MacMahon's statistics, generating polynomial, recursive description, Euler's statistics.*

Dorokhova A. M. **MIXING DIGRAPHS OF TRANSFORMATIONS BASED ON SHIFT REGISTERS WITH TWO FEEDBACKS.** Some substitutions are described among the transformations of binary shift registers with two feedbacks. A primitiveness criterion and some exponent estimates are given for the corresponding mixing digraphs.
Keywords: *binary shift registers, exponent of graph, mixing digraph of transformation.*

Kyazhin S. N., Fomichev V. M. **ON LOCAL EXPONENTS OF THE MIXING GRAPHS FOR THE FUNCTIONS REALIZED BY A5/1 TYPE ALGORITHMS.** It is shown that the mixing graphs for the functions realized by A5/1 type algorithms based on linear feedback shift registers of lengths n, m, p with characteristic polynomials of weights ν, μ, π are primitive. The following lower and upper bounds for the mixing graph exponent and local exponent depending on these parameters take place: $1 + \max\{\lceil n/\nu \rceil, \lceil m/\mu \rceil, \lceil p/\pi \rceil\} \leqslant \exp \Gamma \leqslant \max\{n, m, p\}$. It is obtained that, for A5/1 algorithm, exponent $\exp \Gamma$ and local exponent $*J\text{-}\exp \Gamma$, $J = \{1, 20, 42\}$, are equal to 21. This matches the idle running length of A5/1 generator.
Keywords: *A5/1 generator, primitive graph, exponent, local exponent.*

Oblaukhov A. K. **ON SOME METRICAL PROPERTIES OF LINEAR SUBSPACES IN BOOLEAN CUBE.** Metric complements of Boolean cube subsets are studied. General characteristics of linear subspaces' metric complements are given. Subspaces with special bases are studied. It is proven that completely regular (and therefore perfect and uniformly packed) codes are metrically regular.
Keywords: *subspace, metrically regular set, metric complement, completely regular code.*

Pogorelov B. A., Pudovkina M. A. **PROPERTIES OF THE GROUP GENERATED BY TRANSLATION GROUPS OF THE VECTOR SPACE AND THE RESIDUE RING.** In this paper, we consider the additive group $\mathbb{Z}_{2^n}^+$ of the residue ring $\mathbb{Z}_{2^n}$, the additive group V_n^+ of the vector space V_n over the field GF(2), and subgroups of the group G_n generated by $\mathbb{Z}_{2^n}^+$, V_n^+. These groups are subgroups of the Sylow 2-subgroup of the symmetrical group $S(\mathbb{Z}_{2^n})$ and have common systems of imprimitivity. In cryptography, $\mathbb{Z}_{2^n}^+$, V_n^+ are connected with groups generated by all key additions. We

describe a permutation structure of subgroups of G_n. We prove that the group of lower triangular $(n \times n)$-matrices over GF(2) and the full affine group over $\mathbb{Z}_{2^n}$ are subgroups of G_n. We also describe properties of imprimitive subgroups of G_n.
Keywords: *wreath product, imprimitive group, Sylow 2-subgroup, additive group of the residue ring, additive group of the vector space, ARX block cipher.*

Pogorelov B. A., Pudovkina M. A. **$\otimes_{\mathbf{W},\mathrm{CH}}$-MARKOVIAN TRANSFORMATIONS.** Let X be an alphabet of plaintexts (ciphertexts) of iterated block ciphers and $(X, \otimes)$ be a regular abelian group. The group operation $\otimes$ defines the difference of a text pair. $\otimes$-Markov ciphers are defined as iterated ciphers of which round functions satisfy the condition that the differential probability is independent of the choice of plaintexts from X. For $\otimes$-Markov ciphers with independent round keys, the sequence of round differences forms a Markov chain. In this paper, we consider $\otimes$-Markov ciphers and a partition $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ with blocks being lumped states of the Markov chain. An l-round $\otimes$-Markov cipher is called $\otimes_{\mathbf{W},\mathrm{ch}}$-markovian if the cipher and $\mathbf{W}$ satisfy the following condition: the block numbers sequence $j_0, \ldots, j_l$ such that, for all $i \in \{0, \ldots, l\}$, the i^{th}-round difference belongs to W_{j_i} is a Markov chain. This definition can be also extended for permutations on X. For a partition $\mathbf{W}$ and differential probabilities of a round function of an l-round $\otimes$-Markov cipher, we get conditions that the cipher is $\otimes_{\mathbf{W},\mathrm{ch}}$-markovian. We describe $\otimes_{\mathbf{W},\mathrm{ch}}$-markovian permutations on $\mathbb{Z}_n$ based on an exponential operation and a logarithmic operation, which are defined on $\mathbb{Z}_n$ and GF$(n+1)$.
Keywords: *Markov block cipher, Markov chain, truncated differential technique, exponential transformation*

Fomichev V. M. **ON DEGREE STRUCTURE OF GRAPHS.** The paper presents some properties of degree structure for different classes of digraphs and describes degree structure for primitive digraphs with n vertices and $n+1$ and $n+2$ arcs. For any integer $n \geqslant 5$ and $k \in \{2, \ldots, n-3\}$, the existence of a minimal primitive digraph with n vertices, $n+k$ arcs and degree structure $\{(1,1)^{n-1}, (k+1, k+1)^1\}$ is shown.
Keywords: *minimal primitive graph, graph degree structure.*

SECTION 2

Vitkup V. A. **ON THE NUMBER OF SYMMETRIC COORDINATE FUNCTIONS OF APN FUNCTION.** In the paper, symmetric properties of APN functions are considered. For any APN function F, it is proved that F can not be a symmetric vector function and there is no permutation of its coordinates such that F keeps its value. Theorems about strict upper bounds for the number of its symmetric and rotation symmetric coordinate Boolean functions are proved. The lower bound for the number of distinct values of F is obtained. It is shown that there exists an upper bound for the maximal number of coinciding values of F.
Keywords: *vector Boolean function, APN function, symmetric function.*

Gorodilova A. A. **ON INTERSECTION OF DERIVATIVES IMAGES FOR APN FUNCTIONS.** The class of APN functions is considered in the paper. A vector Boolean function F in n variables from the set of all binary vectors of length n to itself is called an APN function if the equation $F(x) \oplus F(x \oplus a) = b$ has at most 2 solutions for any vectors a, b, where a is a nonzero vector. A derivative of the function F in the direction of a is a Boolean function $D_a F(x) = F(x) \oplus F(x \oplus a)$. Two questions about intersections of the value sets for derivatives of two APN functions are proposed. The first one is about

the minimal cardinality of such intersections. The second question is what a relationship these two APN functions have if the value sets of all directional derivatives of them pairwise coincide. Some partial results about both questions are obtained.
Keywords: *vector Boolean functions, directional derivatives, APN functions.*

Ivachev A. S. **RESEARCH OF THE GROUP OF BIJECTIVE DIFFERENTIABLE MODULO p^n FUNCTIONS.** The group of bijective differentiable modulo p^n functions is researched up to isomorphism. A method of searching for conjugation element in this group is proposed. The method consists in solving a system of linear equations over $\mathbb{Z}_p$. A technique for generating transitive functions via conjugating the function $f(x) = x + 1$ by the bijective differentiable modulo p^n functions is described.
Keywords: *differentiable modulo p^n functions, transitive functions, bijective functions, conjugation.*

Karpov A. V. **THE INVERSE OF DIFFERENTIABLE PERMUTATIONS OVER GROUPS.** The concept of a differentiable function over a group with a normal series generalizing the concept of a polynomial function is introduced. In the case of abelian, nilpotent and solvable groups, a recurrent formula for constructing the inverse of differentiable permutation with respect to composition is proved.
Keywords: *permutation, polynomial over group, differentiable function.*

Kolomeec N. A. **ON THE MINIMAL DISTANCE GRAPH CONNECTIVITY FOR BENT FUNCTIONS.** For the set $\mathcal{B}_{2k}$ of all bent functions in $2k$ variables, the graph GB_{2k} is defined. The vertices in GB_{2k} are all functions in $\mathcal{B}_{2k}$ and two of them are adjacent if and only if the Hamming distance between them is equal to 2^k. It is proved that, for $k = 1, 2, 3$, the graph GB_{2k} is connected and, for any k, the subgraph of GB_{2k} induced by the subset of all vertices being affine equivalent to Maiorana — McFarland bent functions is also connected.
Keywords: *Boolean functions, bent functions, the minimal distance.*

Kutsenko A. V. **ON SELF DUAL BENT FUNCTIONS.** Here, it is proved that a Boolean function f in n variables is self-dual bent if and only if the Hamming weight of the function $F_y(x) = f(x) \oplus f(y) \oplus x \cdot y$ is equal to $2^{n-1} - 2^{n/2-1}$ for any $y \in \mathbb{F}_2^n$.
Keywords: *Boolean function, bent function, self-dual bent.*

Pankratova I. A. **ON THE INVERTIBILITY OF VECTOR BOOLEAN FUNCTIONS.** The class $\mathcal{F}_{n,m,k}$ of invertible vector Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with coordinate functions depending on the given number k variables is considered. It is proved that 1) these functions do not exist for any $n = m$ and $k = 2$; 2) the functions of the class $\mathcal{F}_{n,n,n-1}$ can (can not) be built from affine coordinate functions for even (odd) n; 3) if $\mathcal{F}_{n,m,k} \neq \varnothing$ then $\mathcal{F}_{n+1,m+1,k} \neq \varnothing$.
Keywords: *vector Boolean functions, invertible function.*

Pokrasenko D. P. **ON ALGEBRAIC IMMUNITY OF VECTOR BOOLEAN FUNCTIONS.** In the paper, the component algebraic immunity of vector Boolean functions is studied. A theorem on a correspondence between the maximum component algebraic immunity of a function and its balancedness is proven. A relationship between the maximum component algebraic immunity and matrices of a special form is obtained. For a small number of variables, some functions with maximum component algebraic immunity are constructed.
Keywords: *component algebraic immunity, vector Boolean function, balancedness.*

Potapov V. N. **PROPERTIES OF p-ARY BENT FUNCTIONS THAT ARE AT MINIMAL DISTANCE FROM EACH OTHER.** It is proved that, in the case of prime p, the minimal Hamming distance between distinct p-ary bent functions in $2n$ variables is equal to p^n. It is shown that for $p > 2$ the number of p-ary bent functions being on the minimal distance from a quadratic bent function is equal to $p^n(p^{n-1}+1)\cdots(p+1)(p-1)$.
Keywords: *bent function, Hamming distance, quadratic form.*

Cheremushkin A. V. **ENUMERATION OF BOOLEAN FUNCTIONS WITH A FIXED NUMBER OF AFFINE PRODUCTS.** A recursive enumeration method for determining the number of Boolean functions with a fixed number of affine products and fixed function weights or nonlinearity degree is proposed.
Keywords: *Boolean function, affine classification, Möbius inversion.*

Shurupov A. N. **SOME STRUCTURAL PROPERTIES OF QUADRATIC BOOLEAN THRESHOLD FUNCTIONS.** With the help of a binary partial order relation on the set of quadratic forms with Boolean variables, some classes of simultaneously decomposed (or not having any decompositions) quadratic Boolean threshold functions are described. Simple representatives of these classes are pointed out. In some cases, we can prove whether a variable is essential or not for a quadratic Boolean threshold functions.
Keywords: *quadratic Boolean threshold function, decomposition, essential variable.*

Shushuev G. I. **ON PROPERTIES OF THE SET OF VALUES OF AN ARBITRARY VECTOR BOOLEAN FUNCTION.** For an arbitrary vector Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, some sufficient conditions that $\{F(x) \oplus F(x \oplus a) : x, a \in \mathbb{F}_2^n\} = \mathbb{F}_2^n$ are stated. This result is applied to researching metrical properties of APN functions.
Keywords: *vector Boolean function, differentially δ-uniform function, APN function.*

SECTION 3

Agibalov G. P. **WATERMARKING CIPHERS.** In order to protect both the data confidentiality and legality, a concept of a watermarking cipher (also called a w-cipher) is defined. The main idea of this is as follows: the transformation of a plaintext x by the composition of the encryption and decryption operations using some encryption and decryption keys yields a proper text x' containing a unique watermark w. The encryption and decryption keys in the w-cipher are connected in some way with each other and with the given watermark w. In contrast with the ciphers usually studied in cryptography, the encryption function in a w-cipher is not compulsorily invertible. Thus in fact w-ciphers are not ciphers in the known sense of the word but the ciphers are w-ciphers of a certain partial type, and all terms, notions and notations related to ciphers are quite applicable to w-ciphers. It is shown how a data watermarking can be performed by applying a w-cipher in such a way that the concealment of a watermark into a plaintext is accomplished by this w-cipher either in the encryption or in the decryption processes. Some examples of w-ciphers constructed on the basis of symmetric stream ciphers are presented in the paper.
Keywords: *data protection, encryption, watermarks, watermarking ciphers, stream ciphers.*

Egorova V. V., Chechulina D. K. **PUBLIC-KEY CRYPTOSYSTEM BASED ON FULLY HOMOMORPHIC ENCRYPTION.** In this paper, we discuss the practical usage of fully homomorphic encryption. The application of this encryption to constructing a public-key cryptosystem based on the RSA algorithm is shown. An implementation of this cryptosystem demonstrates that all arithmetical calculations over the encrypted data

are correct. Also, it proves that the multiplication of ciphertexts doesn't lead to increasing the dimension of the multiplication result.
Keywords: *homomorphic encryption, public-key cryptosystem, RSA algorithm.*

Karondeev A. M. **ADDITION MODULO 2^n IN BLOCK CIPHERS.** Cryptographic properties of the addition modulo 2^n and bitwise addition modulo 2 are analysed in this article. For the first operation, the author proposes some linear and non-linear approximations and their usage in cryptanalysis. Also, a modification of the linear cryptanalysis method is proposed. In some cases, this modification allows a more efficient way for attack. For example, an attack on eight rounds GOST 28147-89 can be carried out with this modification and cannot be done without it. The author gives examples how the approximations are used for known plaintext attack on ciphers using the addition modulo 2^n for key mixing. The author shows that the usage of the addition modulo 2^n instead of XOR increases the resistance of block ciphers to linear cryptanalysis and its non-linear modification.
Keywords: *addition modulo 2^n, block ciphers, cryptanalysis.*

Medvedeva N. V., Titov S. S. **NON-ENDOMORPHIC PERFECT CIPHERS WITH TWO ELEMENTS IN PLAINTEXT ALPHABET.** This paper deals with the non-endomorphic perfect ciphers in the case when the plaintext alphabet consists of two elements. According to Shannon, these ciphers are absolutely immune against the attack on ciphertext. In terms of linear algebra on the basis of Birkhoff's theorem (about the classiffcation of doubly stochastic matrices), the matrices of cipher keys probabilities are described. The set of possible values of apriori probabilities for elements of ciphertext alphabet is constructed.
Keywords: *perfect ciphers, non-endomorphic ciphers, maximum ciphers, doubly stochastic matrices.*

Pestunov A. I. **PRELIMINARY EVALUATION OF A MINIMAL NUMBER OF ROUNDS IN LIGHTWEIGHT BLOCK CIPHERS FOR PROVIDING THEIR SATISFACTORY STATISTICAL PROPERTIES.** We experimentally evaluate a minimal number of rounds, which provide satisfactory statistical properties of some well-known and new lightweight block ciphers. The experiments employed the "Book Stack" test. The testing scheme was as follows. We increased the number of rounds until the test detected deviations from randomness. Depending on the cipher, the blocks were represented by two, three or four 32-bit words. The testing sample consisted of the first words in blocks. The size of the sample was 2^{26} bytes.
Keywords: *block cipher, lightweight cipher, statistical analysis, statistical test, number of rounds, pseudo-random numbers.*

Pogorelov B. A., Pudovkina M. A. **$\otimes_{\mathbf{W},\mathrm{CH}}$-MARKOVIAN AND IMPRIMITIVE PROPERTIES OF BLOCK CIPHERS.** In this paper, we describe relations between $\otimes_{\mathbf{W},\mathrm{ch}}$-markovian block ciphers and a wreath product. Let X be an alphabet of plaintexts (ciphertexts) in iterated block ciphers, $(X, \otimes)$ be a regular abelian group, and $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ be a partition of X. In the case when $\mathbf{W}$ is the set of cosets of a subgroup of $(X, \otimes)$, we prove that $\otimes$-Markov block cipher is $\otimes_{\mathbf{W},\mathrm{ch}}$-markovian iff $\mathbf{W}$ is an imprimitivity system of the group generated by round functions of the cipher. We show that there are $\otimes_{\mathbf{W},\mathrm{ch}}$-markovian block ciphers where $\mathbf{W}$ is not a set of cosets. So, for the additive group $(V_n^+, \oplus)$ of the vector space V_n, we describe $\oplus_{\mathbf{W},\mathrm{ch}}$-markovian classes of non-linear and affine transformations for $\mathbf{W}$ being not a set of cosets. We show that the set of

all affine $\oplus_{\mathbf{W},\mathrm{ch}}$-markovian transformations on V_n is a group and give examples of it.
Keywords: *imprimitive group, homomorphism method, XSL-block cipher, wreath product.*

Rybalov A. N. **ON GENERIC COMPLEXITY OF THE QUADRATIC RESIDUOSITY PROBLEM.** Generic-case approach to algorithmic problems was suggested by A. Miasnikov, I. Kapovich, P. Schupp and V. Shpilrain in 2003. This approach studies behavior of an algorithm on typical (almost all) inputs and ignores the rest of inputs. Many classical undecidable or hard algorithmic problems become feasible in the generic case. But there are generically hard problems. For example, this is the classical discrete logarithm problem. In this talk, we consider generic complexity of the quadratic residuosity problem. We fit this problem in the frameworks of generic complexity and prove that its natural subproblem is generically hard provided that the quadratic residuosity problem is hard in the worst case.
Keywords: *generic complexity, quadratic residue, probabilistic algorithm.*

Tokareva N. N. **NSUCRYPTO — A STUDENT'S OLYMPIAD IN CRYPTOGRAPHY: AN IDEA, REALIZATION AND RESULTS.** We briefly discuss the experience of the first international student's olympiad in cryptography NSUCRYPTO. Principles of its organization and mathematical problems given to participants are considered.
Keywords: *NSUCRYPTO, olympiad, cryptography, Boolean functions.*

Trepacheva A. V. **CIPHERTEXTS-ONLY ATTACK ON A LINEAR FULLY HOMOMORPHIC CRYPTOSYSTEM.** The paper proposes a new ciphertexts-only attack on a linear fully homomorphic cryptosystem based on the problem of big numbers factorization. Theoretical and practical estimations of probability to find a key using this attack are given. Also, a link between factorization problem and cryptosystem security is analysed. It is shown how to increase the efficiency by replacing modulo n without loss of cipher strength.
Keywords: *fully homomorphic encryption, factorization problem, ciphertexts-only attack.*

SECTION 4

Anisenya N. I. **A SECURE DISTRIBUTED PROTOCOL IN A COMPETITIVE ENVIRONMENT OF A CTF CONTESTS KIND.** The possibility of using distributed protocol in a competitive environment is demonstrated. A mathematical method of holding task-based CTF contests under threat of DDoS attack against organizers' servers is used as an example. For the purpose, a decentralized protocol distributing some organizers' functions among participants is proposed. The protocol meets the main security requirements due to the competitive nature of CTF contests. Its stability against the possible attacks are researched.
Keywords: *distributed protocols, protected computing, fault-tolerant systems.*

Devyanin P. N. **SECURITY VIOLATION NECESSARY CONDITIONS FOR TIME INFORMATION FLOWS IN MROSL DP-MODEL.** This article presents a theorem about the security violation necessary conditions for time information flows in Linux family operating systems. The conditions are easily to implement. According to these conditions, to prevent prohibited time information flows it is necessary: 1) to eliminate containers where both the Boolean mandatory attribute CCR (Container Clearance Required) and the integrity attribute CCRI (CCR for integrity) are `true`; 2) to eliminate containers which include entities with less level of confidentiality; 3) to completely prohibit

using entities-"holes" not saving data or use their implementation not creating time information flows. After this, for the access control security in OS Astra Linux Special Edition, it is sufficient to ensure the memory information flows security in the sense of Bell — La-Padula model and the mandatory integrity control.
Keywords: *computer security, formal model, information flow.*

Kolegov D. N., Broslavsky O. V., Oleksov N. E. **IMPLEMENTATION OF COVERT TIMING CHANNELS BASED ON HTTP CACHE HEADERS IN CLOUD FILE STORAGE SERVICES.** It is shown how covert timing channels based on HTTP cache headers can be implemented in cloud file storage services. Most of the cloud file storages like Google Drive allow users to operate with cache-control headers, particularly with files' ETags. So it is possible to implement covert timing channel based on ETag cache header. Consider two man-in-the-browser attackers, s_1 and s_3, located on different hosts, and fully trusted web server, accessible via `https://drive.google.com/drive/`, with some file hosted on it. The only requirement for covert channel is that the file should be accessible for writing to s_1 and for reading to s_3. The attacker s_1 sends a request to Google Drive API (POST request to `https://www.googleapis.com/drive/v2/files/fileId/touch`) to modify the file's last access time (and hence ETag). Then the attacker s_3 sends a request to Google Drive API (GET request to `https://www.googleapis.com/drive/v2/files/fileId`) to get the file's metadata including ETag. If the recieved header value is the same as before, s_3 considers that he get bit 1, otherwise (when file has been changed and header values do not match) s_3 considers that he get bit 0. This method allows to increase channel's throughput (in comparison with some other methods) and provides the anonymity for communications between attackers s_1 and s_3.
Keywords: *HTTP, covert channels, web-application security, botnets.*

Kolegov D. N., Broslavsky O. V., Oleksov N. E. **NON-INVASIVE INTEGRITY CONTROL METHOD FOR COOKIE IN WEB APPLICATIONS.** A non-invasive integrity control method for cookies in web applications is suggested. The method is based on cryptographic protocols and keying hash functions. It involves the creation and usage of a set of auxiliary cookies. So for every controlled cookie C, there is a cookie containing *hmac* from cookie C and its expiration date as well as the value of the expiration date itself. This allows to control the value integrity for C and to ensure the impossibility of its deletion. Besides, there is an auxiliary cookie allowing to control integrity of path, domain and other attributes for all controlled cookies. The value integrity for this auxiliary cookie is also provided with the help of *hmac*. Generally speaking, the proposed method solves the following problems in web applications: providing the integrity value for cookies; protecting cookies from deletion and prolongation, that is, from changing the attribute "expires" and setting the flag *session*; providing the value integrity for attributes "path" and "domain"; controlling the transmission of cookie with the attribute "secure" over a secure connection. All these functions of the method are quite capable of being implemented in web applications in non-invasive way. Thus, the method can be used in non-invasive protection mechanisms against web application attacks employing cookies as an attack vector.
Keywords: *cryptographic protocols, hash functions, web application, HTTP cookie.*

Kolegov D. N., Tkachenko N. O. **NON-INVASIVE METHOD OF MANDATORY ACCESS CONTROL IMPLEMENTAION ON DBMS LAYER IN WEB APPLICATIONS.** We propose non-invasive method of mandatory access control implementation on DBMS MySQL layer in web applications. This method is based on formal DP-

models for DBMS MySQL and proxy-based reference monitor for SQL queries. The main idea of the method is identification of users in account-based web applications and SQL query rewriting. Users' identities are added by applicaion's module (Django middleware) and transmitted in comments of SQL queries to MySQL-proxy. After identification of users has been completed, we simulate DBMS's entities identification and row level security by SQL rewriting.
Keywords: *access control, web applications, DBMS security.*

Milovanov T. I. **IMPLEMENTATION OF DNS REBINDING.** The possibility of DNS Rebindng attack realization in modern browsers is researched. This attack is directed at bypassing Same Origin Policy. The conditions for successful attack realization when the target host is located in a local network are studied. A list of the most vulnerable browsers is produced. The attack is implemented in the BeEF (Browser Exploitation Framework) being a tool for penetration testing. Some advices for protection against this attack are given.
Keywords: *HTTP, pentesting, Web application security.*

Ovsyannikov S., Trenkaev V. **ATTRIBUTE BASED ACCESS CONTROL FOR KEY-VALUE STORES.** A way of restricting access to key-value store based on query parameters (key, operation, password) is proposed. The query parameters are used as subjects (objects) attributes to make access control decisions. Thus this type of control can be related to the attribute based access control model. An access control function with arguments of query parameters is defined. The function has the values from $\{Allow, Deny, Pass\}$ and can be changed by store user.
Keywords: *attribute based access control, key-value store, NoSQL database.*

Epishkina A. V., Kogos K. G. **THE CAPACITY OF A PACKET LENGTH COVERT CHANNEL.** Covert channels are used for information hiding and realize one of the most serious security threat. Widespread IP networks allow for designing such channels using special properties of packet data transfer. Packet length covert channels are resistant to traffic encryption, but some difficulties to detect them are known. It makes significant an investigation of capacity limitation methods. This work presents a technique to estimate and limit the capacity of covert channels based on the packet length modulation by traffic padding.
Keywords: *covert channel, packet length, dummy packet, capacity limitation.*

SECTION 5

Alekhina M. A. **UNRELIABILITY OF CIRCUITS IN CASE OF CONSTANT FAILURES ON INPUTS AND OUTPUTS OF GATES.** We consider the implementation of Boolean functions by circuits of unreliable functional elements in the basis containing only Sheffer stroke. It is assumed that each of the circuit elements is exposed to type 0 or type 1 failures in its inputs and outputs with probabilities γ_0 or γ_1 and ε_0 or ε_1 respectively. It is shown that any Boolean function can be so implemented by a such circuit that the asymptotic estimate of its unreliability is no more than $2\varepsilon_0 + 2\gamma_0 + \varepsilon_1 + 2\gamma_1^2$ for $\gamma_0, \gamma_1, \varepsilon_0, \varepsilon_1 \to 0$. This estimation is achieved for functions $f \notin \bigcup_{n=1}^{\infty} K(n)$ where $K(n)$ is the set of all Boolean functions $\bar{x}_i \vee h$ and $x_i \wedge \bar{h}$ for $i \in \{1, \ldots, n\}$ and h — an arbitrary Boolean function of variables $x_1, \ldots, x_n$.
Keywords: *unreliable functional gates, unreliability of circuits, constant failures.*

Alekhina M. A., Barsukova O. U. **A LOWER BOUND FOR UNRELIABILITY OF CIRCUITS IN THE WEBB BASIS.** A realization of ternary logic functions by circuits of unreliable functional gates in the basis consisting of Webb function is described. It is assumed that any basic gate, for any input values, gives the correct output value with a probability $1-2p$ and can give any of two incorrect values with the probability p. It is also assumed that all gates in a circuit get such a faulty independently of each other. In the paper, a lower bound for unreliability of circuits realizing functions of a certain class is obtained.

Keywords: *ternary logic functions, circuit of unreliable functional gates, reliability and unreliability of circuit.*

Alekhina M. A., Kargin S. P. **LOWER BOUNDS FOR UNRELIABILITY OF CIRCUITS IN THE ROSSER — TOURKETT BASIS.** We consider the implementation of four-valued logic functions by circuits consisting of unreliable functional gates in the Rosser — Tourkett basis. It is assumed that all elements of the circuit independently with probability p are subject to inverse failures on the outputs, i. e. each basic element can give each of incorrect values with the probability p and correct value with the probability $1-3p$. In this paper, a class K of four-valued functions is introduced in such a way that almost all four-valued functions are contained in K and any circuit realizing a function from K operates with an unreliability that is asymptotically (for small p) not less than $9p$.

Keywords: *four-valued logic functions, unreliable functional gates, unreliability of circuits, inverse failures on outputs of gates.*

Grabovskaya S. M. **AN UPPER BOUND FOR RELIABILITY OF NON-BRANCHING PROGRAMS WITH AN UNRELIABLE STOP-OPERATOR.** A realization of Boolean functions by non-branching programs with a conditional stop-operator is considered in an arbitrary complete finite basis. All computational operators are supposed to be subject to output one-type constant faults with a probability $\varepsilon \in (0, 1/2)$. Conditional stop-operators are subject to faults of two types: the first and the second kinds with probabilities $\delta \in (0, 1/2)$ and $\eta \in (0, 1/2)$ respectively. Three bases are considered: with a special function, with the generalized disjunction, and with the generalized conjunction. Some upper bounds for the reliability of non-branching programs in these bases are given. For an arbitrary complete finite basis, such a bound is equal to $\max\{\varepsilon, \eta\} + 78\mu^2$ for each $\varepsilon \in (0, 1/960]$ and $\mu = \max\{\varepsilon, \delta, \eta\}$.

Keywords: *Boolean function, non-branching program, conditional stop operator, reliability, constant faults on the outputs.*

Rybakov A. V. **ON LENGTH, HEIGHT AND RELIABILITY OF CIRCUITS REALIZING SELECTION FUNCTION.** We consider planar (flat) circuits realizing the selection function $v_n = \bigvee\limits_{\sigma} x_1^{\sigma_1} x_2^{\sigma_2} \dots x_n^{\sigma_n} y_{|\widetilde{\sigma}|}$, where n is an even integer; $\sigma_i \in \{0, 1\}$, $x_i^{\sigma_i} = x_i$ if $\sigma_i = 1$ and $x_i^{\sigma_i} = \bar{x}_i$ if $\sigma_i = 0$, $i = 1, 2, \dots, n$; $|\widetilde{\sigma}| \in \{0, 1, \dots, 2^n - 1\}$ and $|\widetilde{\sigma}| = \sum\limits_{i=1}^{n} \sigma_i 2^{n-i}$. It is assumed that the switching elements are absolutely reliable, functional elements are subject to inversion failures on its outputs and independently pass into defective states. Some relations for the length and height, as well as an estimate of the unreliability of such circuits are found.

Keywords: *Boolean functions, planar circuits, inversion failures, unreliability of circuit, function of selection.*

SECTION 6

Abrosimov M. B., Modenova O. V. **NUMBER ESTIMATION FOR ADDITIONAL ARCS IN A MINIMAL 1-VERTEX EXTENSION OF TOURNAMENT.** We obtain lower and upper bounds for the number of additional arcs in minimal vertex 1-extension of arbitrary tournament. It is shown that the estimates are sharp. We describe tournaments, for which estimates are attained.
Keywords: *tournament, minimal vertex extension, fault-tolerance.*

Avezova Y. E., Fomichev V. M. **PRIMITIVENESS CONDITIONS FOR SYSTEMS OF TWO GRAPHS.** Some sufficient conditions for primitiveness of two n-vertex digraphs system are obtained in the case when there are no acyclic vertices in one of this two graphs, particularly when it contains a Hamiltonian cycle. Also, an exponent estimate for the two digraphs system is obtained in terms of the exponent of their product. The results can be used for evaluation of the mixing properties of iterative functions based on the transformation branching into two given transformations.
Keywords: *primitive graph, exponent of graph, Hamiltonian cycle.*

Zharkova A. V. **ON NUMBER OF INACCESSIBLE STATES IN FINITE DYNAMIC SYSTEMS OF BINARY VECTORS ASSOCIATED WITH PALMS ORIENTATIONS.** Finite dynamic systems of binary vectors associated with palms orientations are considered. A palm is a tree which is a union of paths having a common end vertex and all these paths, except perhaps one, have the length 1. States of a dynamic system (P_{s+c}, γ), $s > 0$, $c > 1$, are all possible orientations of a palm with trunk length s and leafs number c, and evolutionary function transforms a given palm orientation by reversing all arcs that enter into sinks. This dynamic system is isomorphic to finite dynamic system (B^{s+c}, γ), $s > 0$, $c > 1$, where states of this system are all possible binary vectors of dimension $s + c$. Let $v = v_1 \dots v_s.v_{s+1} \dots v_{s+c} \in B^{s+c}$, then $\gamma(v) = v'$ where v' is obtained by simultaneous application of the following rules: 1) if $v_1 = 0$, then $v'_1 = 1$; 2) if $v_i = 1$ and $v_{i+1} = 0$ for some i where $0 < i < s$, then $v'_i = 0$ and $v'_{i+1} = 1$; 3) if $v_i = 1$ for some i where $s < i \leqslant s + c$, then $v'_i = 0$; 4) if $v_s = 1$ and $v_i = 0$ for all i where $s < i \leqslant s + c$, then $v'_s = 0$ and $v'_i = 1$ for all i, $s < i \leqslant s + c$; 5) there are no other differences between v and $\gamma(v)$. A formula for counting the number of inaccessible states in the considered dynamic systems is proposed. The table with the number of inaccessible states in systems (B^{8+c}, γ) for $1 < c < 9$ is given.
Keywords: *finite dynamic system, inaccessible state, palm, starlike tree.*

Malyugin S. A. **PERFECT BINARY CODES OF INFINITE LENGTH.** A subset C of the infinite-dimensional Boolean cube $\{0,1\}^{\mathbb{N}}$ is called a perfect binary code with distance 3 if all balls of radius 1 (in the Hamming metric) with centres in C are pairwise disjoint and their union covers the cube $\{0,1\}^{\mathbb{N}}$. A perfect binary code in the zero layer $\{0,1\}_0^{\mathbb{N}}$, consisting of all vectors of the cube $\{0,1\}^{\mathbb{N}}$ having finite supports, is defined similarly. It is proved that the cardinality of the set of all equivalence classes of perfect binary codes in the zero layer $\{0,1\}_0^{\mathbb{N}}$ is continuum. At the same time, the cardinality of the set of all equivalence classes of perfect binary codes in the whole cube $\{0,1\}^{\mathbb{N}}$ is hypercontinuum.
Keywords: *perfect binary codes, Hamming code, Hamming distance, Vasil'ev codes, equivalence classes, continuum, hypercontinuum.*

Pottosin Yu. V. **LOW POWER RACE-FREE STATE ASSIGNMENT OF AN ASYNCHRONOUS AUTOMATON.** The problem of race-free state assignment in an asynchronous automaton is considered in a formulation where both the length of state code

and the switching activity of memory elements should be minimized. To solve this problem the author uses the approach that involves consideration of the pairs of transitions between states for establishing the absence conditions for critical races. This conditions are represented as rows of a ternary matrix called the condition matrix. The state codes of a given automaton are obtained as a result of covering the condition matrix rows by compatible sets of columns. To take into account the low switching activity of memory elements, the compatible sets and correspondingly the vectors related to them are supplied with weights. So, the problem of low power race-free state assignment of an asynchronous automaton is reduced to the weighted cover problem.
Keywords: *asynchronous automaton, race-free state assignment, low power state assignment.*

Salii V. N. **THE SPERNER PROPERTY FOR TREES.** The reachability relation of a directed acyclic graph is a partial order on the set of its vertices. One of the interesting properties of a partially ordered set is its Sperner property that means that at least one of maximum antichains is formed from elements of the same height. In graphs with the reachability relation, this property is discussed for out-trees and in-trees, it is modified and studied for functional and contrafunctional digraphs closely related to these trees, and for unoriented trees also.
Keywords: *partially ordered set, Sperner property, tree, acyclic digraph, out-tree, in-tree, functional digraph, contrafunctional digraph.*

Fedoryaeva T. I. **ON THE DIVERSITY OF BALLS IN A GRAPH OF A GIVEN DIAMETER.** The diversity vectors for balls in connected graphs are asymptotically studied. Here for a graph, the ith component of the vector is equal to the number of different balls of radius i in the graph. The asymptotic behavior of the number of graphs with a special (in particular with the local) diversity of balls is researched. The diversity of balls of large radii in a graph of a given diameter is described.
Keywords: *graph, balls, radius of ball, the diversity vector for balls.*

SECTION 7

Grechnev S. Yu., Stefantsov D. A. **MODIFICATION OF LYaPAS FOR OPERATING SYSTEMS DEVELOPMENT.** A modification of LYaPAS for operating systems development is described. The initializing and finalizing codes are changed, the utilities for complexes are corrected, the memory usage is optimized, and the following features are introduced: the random memory access and the procedure address retrieval.
Keywords: *LYaPAS, operating system, Russian programming language.*

Zhukovskaja A. O., Stefantsov D. A. **OPERATIONAL SEMANTICS FOR LYaPAS.** The development of the operational semantics for LYaPAS is considered. The following two applications are possible: the proof of the complex-element references correctness by abstract interpretation method and the creation of a certified compiler.
Keywords: *operational semantics, LYaPAS, abstract interpretation, certified compiler.*

Safonov V. O. **THE PROGRAMMING-LIBRARIES MANAGEMENT SYSTEM FOR LYaPAS.** For programming language LYaPAS, a programming-libraries management system is proposed. The system is comprised of three main subsystems: a network service for storing libraries, a library creation utility, and a utility for managing the set of libraries installed on a local computer. The library format and the system of modular compilation

for LYaPAS are also described.
Keywords: *LYaPAS, modular compilation, procedure library.*

Stefantsov D. A., Tomskih P. A. **THE DEVELOPMENT OF AN OPERATING SYSTEM IN LYaPAS.** The development of OS LYaPAS for writing and executing programs in LYaPAS is described. Currently the creation of OS LYaPAS is in the stage of kernel development. The following functions are implemented: message output to screen, device-controllers initialization, interrupts handling, working with timer and keyboard, multitasking. Multitasking is demonstrated by a few parallel processes that can be suspended and restored with a key press. The further step in the development is the creation of a file system and memory management modules.
Keywords: *LYaPAS, operating system.*

SECTION 8

Anashkina N. V., Shurupov A. N. **SOLVING LINEAR INEQUALITIES SYSTEMS WITH LOCAL SEARCH ALGORITHMS.** Here, we present a new heuristic on the basis of Balas algorithm for solving systems of linear inequalities with Boolean variables. If a branch in a solution tree leads to a false solution, then a new branch is chosen with the help of simulated annealing technique. The experimental results of fulfilled comparison of new and classical (Balas and simulated annealing) heuristics are listed. Two variants of cost function — sum and maximum — were applied in the new heuristic. The plan of experiments concerned random systems of pseudo-Boolean linear inequalities. According to the results of comparison, the new heuristic is more effective. It was applied to a system of linear inequalities that describes LFSR with a Boolean threshold output function. This system grows exponentially with the length of the output. Some methods for reducing the system size are given. In all cases, the new heuristic allows to find the solution for LFSR sometimes being different from the original.
Keywords: *simulated annealing, Balas algorithm, pseudo-Boolean linear inequalities.*

Bogachkova I. A., Zaikin O. S., Kochemazov S. E., Otpuschennikov I. V., Semenov A. A. **APPLICATION OF ALGORITHMS SOLVING SAT PROBLEM TO CRYPTANALYSIS OF HASH FUNCTIONS OF MD FAMILY.** In this research, we consider the problems of searching for collisions in cryptographic hash functions from the MD family as variants of the Boolean Satisfiability problem (SAT). To construct the SAT encodings for MD4 and MD5 algorithms, we employ the Transalg system designed to automatically transform algorithmic descriptions of discrete functions to Boolean equations. For hash functions under consideration, the SAT encodings are much more compact than known analogues, because the several additional constraints based on the known differential attacks on these functions are used in these encodings. The solving time for the SAT instances, encoding the search for single block collisions for MD4, is on average less than 1 sec on an usual PC. To solve the SAT instances, encoding the search for two-block collisions for MD5, we employed parallel SAT solvers working on the computing cluster. As a result, we found a class of two-block collisions for MD5 with the first 10 zero bytes. We constructed several dozens of collisions of the proposed kind. Also, we considered the inversion problem for the MD4 hash function (the search for the preimage for a given hash value). To solve this problem, we developed a technique relying on the so called “switch variables”. Each switch variable is responsible for an additional constraint on several Boolean variables included in the SAT encoding. If a switch variable takes the value of Truth then the corresponding

constraint becomes enabled and should be taken into account by the SAT solving algorithm. Otherwise this constraint remains inactive. The use of switch variables made it possible to find new additional constraints (similar to "Dobbertin's constraints") and to improve the effectiveness of solving the inversion problem for 39-step MD4 by a hundredfold.
Keywords: *cryptographic hash functions, collisions of hash functions, MD4, MD5, Boolean satisfiability problem, SAT.*

Bykova V. V., Kirillov Y. I. **CALCULATION OF UPPER BOUNDS FOR GRAPH VERTEX INTEGRITY BASED ON THE MINIMAL SEPARATORS.** A vertex integrity of a graph is a generalization of a connectivity notion. It is believed that a graph is more integral if the connectivity of this graph is broken when you delete a larger number of vertices and the effect of these deletions is minimal. Measures of the integrity are introduced to use in the analysis and synthesis of fault-tolerant complex technical systems. One of such measure is a numerical parameter of the graph called the vertex integrity. The evaluation problem for this parameter is NP-hard. Let $G = (V, E)$ be a simple connected graph, V be a set of vertices and E be a set of edges, $n = |V|$. The vertex integrity of G is calculated by the formula $I(G) = \min\limits_{S \subseteq V} \{|S| + w(G - S)\}$ where $w(H)$ is the order of the largest connected component of a graph H. The minimum value is reached when S is a separator. Therefore, it is necessary to know all separators of the original graph. An algorithm, which constructs and analyses only all minimal separators, is proposed. This algorithm gives an upper bound for the vertex integrity of the graph. In the first stage, the algorithm computes the set M of all minimal separators of the graph G using a necessary and sufficient condition. The complexity of this stage polynomially depends on the number of vertices of the graph, namely $\mathrm{O}(n^3)$. In the second stage, each separator in M is substituted into the objective function to find the vertex integrity. The computational complexity of this stage linearly depends on the cardinality of M. The experimental results show that the calculated estimates are good and often achievable.
Keywords: *graph algorithms, graph vertex integrity, minimum separators.*

Kozhushko O. A. **CONSTRUCTION OF AN ERROR FUNCTION FOR SOLVING THE TEXT RANKING IDENTIFICATION PROBLEM.** In the paper, an error function for text ranking identification problem is proposed. The rationale of incorrect use of error functions for problems where the output values are real numbers is provided. An alternative is the usage of error functions taking values of relative variation ranking results. Also, a special case of identification problem formulation where a ranking result is considered as relevance class is proposed.
Keywords: *text ranking algorithm, system identification, error function.*

Kuznetsov A. A., Safonov K. V. **HALL'S POLYNOMIALS OVER BURNSIDE GROUPS OF EXPONENT THREE.** Let $B_k = B(k, 3)$ be the k-generator Burnside group of exponent 3. Levi and van der Waerden proved that $|B_k| = 3^{k+\binom{k}{2}+\binom{k}{3}}$ and B_k are nilpotent of class at most 3. For each B_k a power commutator presentation can be easily obtained using the system of computer algebra GAP or MAGMA. Let $a_1^{x_1} \dots a_n^{x_n}$ and $a_1^{y_1} \dots a_n^{y_n}$ be two arbitrary elements in the group B_k recorded in the commutator form. Then their product is equal to $a_1^{x_1} \dots a_n^{x_n} \cdot a_1^{y_1} \dots a_n^{y_n} = a_1^{z_1} \dots a_n^{z_n}$. Powers z_i are to be found based on the collection process, which is implemented in the computer algebra systems GAP and MAGMA. Furthermore, there is an alternative method for calculating products of elements of the group proposed by Ph. Hall. Hall showed that z_i are polynomial functions (over the field $\mathbb{Z}_3$ in this case) depending on the variables $x_1, \dots, x_i, y_1, \dots, y_i$ and

now called Hall's polynomials. Hall's polynomials are necessary in solving problems, which require multiple products of the elements of the group. The study of the Cayley graph structure for a group is one of these problems. The computational experiments carried out on the computer in groups of exponent five and seven showed that the method of Hall's polynomials has an advantage over the traditional collection process. Therefore, there is a reason to believe that the use of polynomials would be more preferable than the collection process in the study of Cayley graphs of B_k groups. It should also be noted that this method is easily software-implemented including multiprocessor computer systems. Previously unknown Hall's polynomials of B_k for $k \leqslant 4$ are calculated within the framework of this paper. For $k > 4$, the polynomials are calculated similarly but their output takes considerably more space.

Keywords: *periodic group, collection process, Hall's polynomials.*

Nikolaev M. V. **ON THE COMPLEXITY OF DISCRETE LOGARITHM PROBLEM IN A FINITE CYCLIC GROUP WITH THE EFFICIENT INVERSION.** Discrete logarithm problem in a finite group G with the efficient inversion consists in solving the equation $Q = nP$ with respect to n in the interval $(-N/2, N/2)$ for the specified $P, Q \in G$, $0 < N < |G| - 1$. If the inversion in the group G may be computed significantly faster than the group operation, then analogously to the solution of the classical discrete logarithm, we may speed up the algorithm. In 2010, S. Galbraith and R. Ruprai proposed an algorithm solving this problem with the average complexity $(1{,}36 + \mathrm{o}(1))\sqrt{N}$ of group operations in G where $N \to \infty$. We show that the average complexity of the algorithm for finding the solution of the discrete logarithm problem in the interval $(-N/2, N/2)$ equals $(1 + \varepsilon)\sqrt{\pi N/2}$ group operations.

Keywords: *discrete logarithm problem in interval, Gaudry — Schost algorithm.*

Tarkov M. S. **IMPLEMENTATION OF A NEURAL WTA-NETWORK ON THE MEMRISTOR CROSSBAR.** An algorithm for mapping the weighting coefficients matrix of a neural WTA ("Winner Takes All") network onto a memristor crossbar is proposed. The neural WTA network built on the basis of the memristor crossbar is simulated using the LTSPICE program. The simulation results can be used both in mathematical modelling and in the physical implementation of the neural networks with the memristor interconnections.

Keywords: *memristor, memristance, crossbar, neural network, weighting coefficients matrix, WTA.*