МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА

Приложение

№ 9 **Сентябрь 2016**

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

ТРУДЫ
Всероссийской конференции
«XV Сибирская научная школа-семинар с международным участием
“Компьютерная безопасность и криптография” — SIBECRYPT’16»
(Новосибирск, 5–10 сентября 2016 г.)



ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

РЕДАКЦИОННАЯ КОЛЛЕГИЯ ЖУРНАЛА
«ПРИКЛАДНАЯ ДИСКРЕТНАЯ МАТЕМАТИКА»

Агибалов Г. П., д-р техн. наук, проф. (председатель); Девянин П. Н., д-р техн. наук, проф. (зам. председателя); Черемушкин А. В., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ (зам. председателя); Панкратова И. А., канд. физ.-мат. наук, доц. (отв. секретарь); Алексеев В. Б., д-р физ.-мат. наук, проф.; Бандман О. Л., д-р техн. наук, проф.; Быкова В. В., д-р физ.-мат. наук, проф.; Глухов М. М., д-р физ.-мат. наук, академик Академии криптографии РФ; Евдокимов А. А., канд. физ.-мат. наук, проф.; Колесникова С. И., д-р техн. наук; Крылов П. А., д-р физ.-мат. наук, проф.; Логачев О. А., канд. физ.-мат. наук, доц.; Мясников А. Г., д-р физ.-мат. наук, проф.; Романьков В.А., д-р физ.-мат. наук, проф.; Салий В. Н., канд. физ.-мат. наук, проф.; Сафонов К. В., д-р физ.-мат. наук, проф.; Фомичев В. М., д-р физ.-мат. наук, проф.; Чеботарев А. Н., д-р техн. наук, проф.; Шойтов А. М., д-р физ.-мат. наук, чл.-корр. Академии криптографии РФ; Шоломов Л. А., д-р физ.-мат. наук, проф.

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

Всероссийская конференция «XV Сибирская научная школа-семинар с международным участием "Компьютерная безопасность и криптография" — SIBECRYPT'16» проведена Национальным исследовательским Томским государственным университетом и Институтом математики СО РАН им. С. Л. Соболева в сотрудничестве с Институтом криптографии, связи и информатики с 5 по 10 сентября 2016 г. в Новосибирске при финансовой поддержке РФФИ (грант № 16-07-20516-г).

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

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

Подписано к печати 09.08.2016.
Формат $60 \times 84\frac{1}{8}$. Усл. п. л. 15,9. Уч.-изд. л. 17,8. Тираж 300 экз. Заказ № 2000.

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

Бондаренко Л. Н., Шарапова М. Л. Обобщённые многочлены Нараяны и их q-аналоги 6
Волгин А. В. Об одном критерии проверки гипотезы о наличии вкраплений в двоичной цепи Маркова 9
Евдокимов А. А. Алгоритм распознавания полноты множества слов и динамика запретов 10
Кузьмин С. А. О достаточном условии для отсутствия возможности сокращения периода в старших двоичных разрядных последовательностях над примарными кольцами 12
Погорелов Б. А., Пудовкина М. А. О группах, порождённых преобразованиями смешанного типа и группами наложения ключа 14
Погорелов Б. А., Пудовкина М. А. О классификации дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса 16

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

Виткуп В. А. О специальном подклассе векторных булевых функций и проблеме существования APN-перестановок 19
Городилова А. А. О дифференциальной эквивалентности квадратичных APN-функций 21
Зуева И. А., Карпов В. А. Функции с вариационно-координатной полиномиальностью над группой 24
Коломеец Н. А. О расстоянии Хэмминга между двумя бент-функциями 27
Куценко В. А. О множестве расстояний Хэмминга между самодуальными бент-функциями 29
Покрасенко Д. П. Условия существования векторной булевой функции с максимальной компонентной алгебраической иммунностью 30
Сошин Д. А. Представление полубайтовых подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ алгебраическими пороговыми функциями 32
Токарева Н. Н. О множестве производных булевой бент-функции 35
Черемушкин А. В. О распределении ранга и оценке уровня аффинности квадратичных форм 36
Шушуев Г. И. Функции на расстоянии один от APN-функций от малого числа переменных 39

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

Агибалов Г. П., Панкратова И. А. К криптоанализу двухкаскадных конечно-автоматных криптографических генераторов 41
Власова В. В., Пудовкина М. А. О группе, порождённой раундовыми функциями алгоритма блочного шифрования «Кузнечик» 43

Заикин О. С., Отпущенников И. В., Семёнов А. А. Оценки стойкости шифров семейства Trivium к криптоанализу на основе алгоритмов решения проблемы булевой выполнимости 46
Коренева А. М., Мартышин В. Н. Экспериментальное исследование экспонентов раундовых перемешивающих матриц обобщённых сетей Фейстеля..... 48
Коренева А. М., Фомичёв В. М. О существенных переменных функции переходов модифицированного аддитивного генератора 51
Косолапов Ю. В., Турченко О. Ю. Поиск информационного сообщения в зашумлённых кодовых блоках при многократной передаче данных..... 55
Кяжин С. Н., Лебедев Ф. В. О точности матрично-графового подхода к оценке перемешивающих свойств преобразований 57
Кяжин С. Н., Фомичев В. М. Перемешивающие свойства двухкаскадных генераторов..... 60
Медведева Н. В., Титов С. С. Аналоги теоремы Шеннона для эндоморфных неминимальных шифров 62
Романько Д. А., Фомичев В. М. О способах построения криптографических генераторов с заданным показателем бесповторности выходных последовательностей..... 65
Рябко Б. Я. Применение двуликих процессов к генерированию псевдослучайных чисел 68
Фомичев М. В. О ключевом расписании блочных шифров без слабых ключей 70
Чижов И. В., Бородин М. А. Криптоанализ криптосистемы Мак-Элиса, построенной на $(k-1)$-подкодах кода Рида — Маллера 73

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Анисеня Н. И. Протокол безотказной луковой маршрутизации с подтверждением времени создания сообщения 76
Горбатенко Д. Е., Кочемазов С. Е., Семёнов А. А. О дискретно-автоматных моделях атак в компьютерных сетях 80
Девянин П. Н. О результатах формирования иерархического представления МРОСЛ ДП-модели 83
Кащеев М. Р., Косолапов Ю. В. Схема обеспечения конфиденциальности в алгоритме RAID-PIR..... 87
Колегов Д. Н., Брославский О. В., Олексов Н. Е. Метод запутывания программной реализации схемы HMAC для недоверенной среды 89
Колегов Д. Н., Линейцев П. А. Об идентификации защитных экранов веб-приложений в модели MitB 92
Колегов Д. Н., Ткаченко Н. О. Легковесная реализация механизма атрибутного управления доступом для СУБД на уровне защитного экрана 93

Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

Алехина М. А., Барсукова О. Ю. О надёжности схем в базисе Россера — Туркетта (в P_k)..... 96
Алехина М. А., Логвина О. А. Ненадёжность схем при слипаниях входов элементов. 98

Секция 6

ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ И ГРАФОВ

Абросимов М. Б., Моденова О. В. Уточнение нижней оценки числа дополнительных дуг минимального вершинного 1-расширения ориентации цепи 101
Абросимов М. Б., Сухов С. А. О количестве оптимальных 1-гамильтоновых графов с числом вершин до 26 и 28 103
Авезова Э. Я., Фомичев М. В. Об одном наследственном признаке в циклических полугруппах графов 105
Воблый В. А., Мелешко А. К. Перечисление помеченных цветочно-колёсных графов 109
Евдокимов А. А., Куценогая Е. П., Федоряева Т. И. О графах полного разнообразия шаров 110
Жаркова А. В. Об аттракторах в конечных динамических системах ориентаций полных графов 112
Жуковская А. О., Тренькаев В. Н. О простых условных экспериментах идентификации обратимых автоматов некоторого класса 115
Карандашов М. В. О транзитивности отображений, ассоциированных с конечными автоматами из групп AS_p 115

Секция 7

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

Егорушкин О. И., Колбасина И. В., Сафонов К. В. О совместности систем символьных полиномиальных уравнений и их приложении 119
Князев В. Н., Князева М. С. Транслятор языка ЛЯПАС-Т на язык ассемблера для ОС Windows и Linux 121
Стефанцов Д. А., Сафонов В. О., Першин В. В., Гречнев С. Ю., Томских П. А. Модульный транслятор с языка ЛЯПАС 122
Чушкин М. С., Шелехов В. И. Методы синтеза фрагментов предикатных программ 126

Секция 8

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

Грибанова И. А. Применение алгоритмов решения проблемы булевой выполнимости к построению разностных путей в задачах поиска коллизий криптографических хеш-функций семейства MD 129
Кузнецов А. А., Карчевский С. С. О вычислении функций роста конечных двупорождённых бернсайдовых групп периода 5 132

СВЕДЕНИЯ ОБ АВТОРАХ 136

АННОТАЦИИ ДОКЛАДОВ НА АНГЛИЙСКОМ ЯЗЫКЕ 141

Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.1 DOI 10.17223/2226308X/9/1

ОБОБЩЁННЫЕ МНОГОЧЛЕНЫ НАРАЯНЫ И ИХ q-АНАЛОГИ[1]

Л. Н. Бондаренко, М. Л. Шарапова

На введённых 312-избегающих ГС-перестановках порядка $r \geqslant 1$ рассматриваются производящие многочлены статистик rise, des и inv. Показано, что многочлены статистик rise и des являются обобщением известных многочленов Нараяны. Получены обратная производящая функция, алгебраическое уравнение для производящей функции и рекуррентная формула с кратными свёртками для обобщённых многочленов Нараяны. Для производящих многочленов пары $(\mathrm{des}, \mathrm{inv})$ найдены аналог полученной рекуррентной формулы и уравнение для производящей функции этих многочленов, частный случай которых приводит к соответствующим q-аналогам обобщённых многочленов Нараяны.

Ключевые слова: *312-избегающие ГС-перестановки, обобщённые многочлены Нараяны, производящая функция, обратная функция, свёртка, q-аналоги.*

Если все буквы слова $\sigma = \sigma_1 \dots \sigma_{rn}$ длины $|\sigma| = rn$ над алфавитом $\mathbb{N}_n = \{1, \dots, n\}$, где $r \geqslant 1$ — целочисленный параметр, стоящие между любыми двумя вхождениями символа $i \in \mathbb{N}_n$, не меньше этого i, то эту особенность σ назовем ГС-свойством, а множество всех перестановок мультимножества $\{1^r, \dots, n^r\}$, обладающих ГС-свойством (ГС-перестановок), обозначим $GS_{n,r}$.

Эти названия мотивированы применением И. Гесселем и Р. Стенли множества $GS_{n,2}$ для изучения полиномиальных последовательностей Стирлинга обоих родов [1], а также исследованием свойств чисел Эйлера порядка r, комбинаторная интерпретация которых связана с рассмотрением $GS_{n,r}$ [1–3].

Введем обобщение понятия рассматриваемой в [4, 5] 312-избегающей перестановки.

Определение 1. Слово $\sigma \in GS_{n,r}$ назовем 312-избегающей ГС-перестановкой порядка r, если не существует тройки индексов $i < j < k$, для которых выполняется неравенство $\sigma_j < \sigma_k < \sigma_i$, а множество всех таких перестановок обозначим $\widetilde{GS}_{n,r}$.

Для слова $\sigma \in \widetilde{GS}_{n,r}$ стандартным образом вводятся неотрицательные целочисленные функции (статистики): $\mathrm{rise}(\sigma) = |\{i \in \mathbb{N}_n : \sigma_{i-1} < \sigma_i, \sigma_0 = 0\}|$ — число подъёмов; $\mathrm{des}(\sigma) = |\{i \in \mathbb{N}_n : \sigma_i > \sigma_{i+1}, \sigma_{n+1} = 0\}|$ — число спусков; $\mathrm{inv}(\sigma) = |\{(i,j) \in \mathbb{N}_n^2 : i < j, \sigma_i > \sigma_j\}|/r$ — приведённое число инверсий.

Теорема 1. Производящие многочлены $\widetilde{A}_{n,r}(t) = \sum\limits_{k=1}^{n} \widetilde{A}_{n,r,k}\, t^k$ статистик rise и des на множестве $\widetilde{GS}_{n,r}$ совпадают и определяются равенством

$$\widetilde{A}_{n,r}(t) = \frac{1}{n} \sum_{k=1}^{n} \binom{n}{k} \binom{rn}{k-1} t^k, \tag{1}$$

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

где $\widetilde{A}_{n,r}(1) = C_{n,r+1} = \dfrac{1}{rn+1}\binom{(r+1)n}{n}$ — числа Фусса — Каталана [2].

Доказательство. Так как $\mathrm{rise}(\sigma) = \mathrm{des}(\pi)$, $\sigma, \pi \in \widetilde{GS}_{n,r}$, $\pi_i = \sigma_{rn+1-i}$, $i \in \mathbb{N}_{rn}$, то многочлены (1) статистик rise и des совпадают. Для вычисления коэффициента $\widetilde{A}_{n,r,k} = |\{\sigma \in \widetilde{GS}_{n,r} : \mathrm{rise}(\sigma) = k\}|$ сопоставим каждой перестановке $\sigma \in \widetilde{GS}_{n,r}$ слово $\tau = \tau_1 \dots \tau_{rn}$, $\tau_i = rn + 1 - \sigma_{rn+1-i}$, $i \in \mathbb{N}_{rn}$, упорядочиваемое с помощью единственного стека, и сформируем новую последовательность, в которую записывается 1, когда символ слова τ помещается в стек, и -1, когда он вынимается из стека, причём в соответствии с принципом «последним пришёл — первым ушёл» из стека вынимаются последовательно r одинаковых символов. В результате перестановке $\sigma \in \widetilde{GS}_{n,r}$ сопоставляется последовательность длины $2rn$, состоящая из одинакового числа 1 и -1 (число записанных подряд -1 кратно r), её частичные суммы неотрицательны, а $\mathrm{rise}(\sigma) = k$, если в этой последовательности имеется k переходов с 1 на -1.

Имеется $\binom{rn}{k-1}\binom{n-1}{k-1}$ пар k-композиций $A : a_1 + \ldots + a_k = rn + 1$ и $B : b_1 + \ldots + b_k = n$ взаимно простых чисел $rn + 1$ и n. Пусть циклическая последовательность $w = w(A, B)$ состоит из a_1 единиц, rb_1 минус единиц, a_2 единиц, rb_2 минус единиц и т. д., причём имеет ровно k пар (A_i, B_i), $i = 1, \ldots, k$, вида $A_i : a_i + a_{i+1} + \ldots + a_k + a_1 + \ldots + a_{i-1} = rn+1$, $B_i : b_i + b_{i+1} + \ldots + b_k + b_1 + \ldots + b_{i-1} = n$. Тогда по лемме Рени [2, 4] единственным способом можно разорвать w так, чтобы получилась последовательность, начинающаяся с 1, после удаления которой любая частичная сумма оставшейся последовательности неотрицательна. Таким образом, получена биекция циклических классов эквивалентности $\{(A_i, B_i) : i = 1, \ldots, k\}$ с множеством $\{\sigma \in \widetilde{GS}_{n,r} : \mathrm{rise}(\sigma) = k\}$ и

$$\widetilde{A}_{n,r,k} = \frac{1}{k}\binom{rn}{k-1}\binom{n-1}{k-1} = \frac{1}{n}\binom{n}{k}\binom{rn}{k-1}.$$

Отметим, что при $r = 1$ эта конструкция аналогична используемой в [4, 5], а $\widetilde{A}_{n,r}(1)$ легко вычисляется с помощью свёртки Вандермонда. ■

При $r = 1$ выражение (1) задает многочлены Нараяны, коэффициенты которых называются числами Нараяны. Эти многочлены и числа встречаются в ряде комбинаторных задач [4]. Поэтому в рассматриваемом обобщении назовем $\widetilde{A}_{n,r,k}$ числами Нараяны порядка r, а $\widetilde{A}_{n,r}(t)$ — многочленами Нараяны порядка r.

Следствие 1. Многочлены Нараяны порядка r находятся по формуле

$$\widetilde{A}_{n,r}(t) = \frac{1}{n!}\,\frac{\partial^{n-1}}{\partial v^{n-1}}((v+t)^n(v+1)^{rn})\bigg|_{v=0}. \tag{2}$$

Доказательство. Непосредственное вычисление (2) с помощью формулы Лейбница для $(n-1)$-й производной приводит к выражению (1). ■

Теорема 2. Производящей функции $v = \widetilde{A}_r(t, u) = \sum\limits_{n=1}^{\infty} \widetilde{A}_{n,r}(z)\, u^n$ отвечает обратная функция $u = \widetilde{A}_r^{-1}(t, v) = v(v+t)^{-1}(v+1)^{-r}$, и справедливо соотношение

$$\widetilde{A}_{0,r}(t) = 1,\ \widetilde{A}_{n+1,r}(t) = (t-1)\left\langle \widetilde{A}_{n,r}(t)\right\rangle^r + \left\langle \widetilde{A}_{n,r}(t)\right\rangle^{r+1},\ n \geqslant 0, \tag{3}$$

где $\langle P_n(t)\rangle^m = \sum\limits_{\substack{k_1+\ldots+k_m=n,\\ k_i\geqslant 0}} P_{k_1}(t)\ldots P_{k_m}(t)$ — m-кратная свёртка последовательности многочленов $P_0(t), P_1(t), \ldots, P_n(t)$, $\deg(P_k(t)) = k$, $k = 0, 1, \ldots, n$.

Доказательство. Первое утверждение теоремы 2 вытекает из (2) и теоремы Лагранжа [4]. Применение функции $v = \widetilde{A}_r(t,u)$, увеличенной на 1, к $u = \widetilde{A}_r^{-1}(t,v)$ даёт алгебраическое уравнение $u(v+1)^{r+1} + u(t-1)(v+1)^r - (v+1) + 1 = 0$. Так как коэффициент при u^n степенного ряда $(v+1)^{r+1}$ равен свертке $\left\langle \widetilde{A}_{n,r}(z)\right\rangle^{r+1}$, то сравнение коэффициентов в этом уравнении при степенях u даёт рекуррентное соотношение (3), причём при $t = 1$ уравнение и соотношение (3) соответствуют формулам из [2]. ■

Теорема 2 допускает q-обобщение.

Теорема 3. Справедливо рекуррентное соотношение

$$\widetilde{A}_{0,r}^{\mathrm{des,inv}}(t,q) = 1,\ \widetilde{A}_{n+1,r}^{\mathrm{des,inv}}(t,q) = (t-1)\left\langle \widetilde{A}_{n,r}^{\mathrm{des,inv}}(t,q)\right\rangle^r + \left\langle \widetilde{A}_{n,r}^{\mathrm{des,inv}}(t,q)\right\rangle^{r+1},\ n\geqslant 0, \quad (4)$$

где $\langle P_n(t,q)\rangle^m = \sum\limits_{\substack{k_1+\ldots+k_m=n,\\ k_i\geqslant 0}} q^{k_2+2k_3+\ldots(m-1)k_m} P_{k_1}(t,q)\ldots P_{k_m}(t,q)$ является q-аналогом m-кратной свёртки последовательности многочленов $P_0(t,q), P_1(t,q), \ldots, P_n(t,q)$, а производящая функция $\widetilde{A}_r^{\mathrm{des,inv}}(t,u;q) = \sum\limits_{n=0}^{\infty} \widetilde{A}_{n,r}^{\mathrm{des,inv}}(t,q)u^n$ удовлетворяет уравнению $\widetilde{A}_r^{\mathrm{des,inv}}(t,u;q) = 1 + u(\widetilde{A}_r^{\mathrm{des,inv}}(t,u;q) + t - 1)\widetilde{A}_r^{\mathrm{des,inv}}(t,qu;q)\ldots\widetilde{A}_r^{\mathrm{des,inv}}(t,q^r u;q)$.

Доказательство. Рекуррентное соотношение (4) для производящих многочленов пары $(\mathrm{des},\mathrm{inv})$ является q-обобщением выражения (3) и может быть получено применением метода математической индукции по r к словам из 1 и -1, используемым в доказательстве теоремы 1, причем для случая $r = 1$ применяется метод доказательства, аналогичный рассмотренному в [6] при $t = 1$. Соотношение (4) при $t = 1$ определяет q-многочлены Нараяны $\widetilde{B}_{n,r}(q) = \widetilde{A}_{n+1,r}^{\mathrm{des,inv}}(1,q)$ порядка r, совпадающие при $r = 1$ с многочленами из [6]. Уравнение для производящей функции $\widetilde{A}_r^{\mathrm{des,inv}}(t,u;q)$ соответствует рекуррентному соотношению (4). ■

Таким образом, рассмотрение статистик на множестве 312-избегающих ГС-перестановок порядка r позволяет получить естественным путём как обобщённые многочлены Нараяны, так и их q-аналоги.

ЛИТЕРАТУРА

1. *Gessel I. and Stanley R. P.* Stirling polynomials // J. Comb. Theory. Ser. A. 1978. V. 24. P. 24–33.
2. *Грэхем Р., Кнут Д., Паташник О.* Конкретная математика. Основание информатики. М.: Мир, 1998. 703 с.
3. *Бондаренко Л. Н., Шарапова М. Л.* Параметрические комбинаторные задачи и методы их исследования // Известия вузов. Поволжский регион. Физ.-мат. науки. 2010. № 4 (16). С. 50–63.
4. *Стенли Р.* Перечислительная комбинаторика. Т. 2. М.: Мир, 2009. 768 с.
5. *Кнут Д.* Искусство программирования для ЭВМ. Т. 1. М.: Мир, 1976. 720 с.
6. *Fürlinger J. and Hofbauer J.* q-Catalan numbers // J. Comb. Theory. Ser. A. 1985. V. 40. P. 248–264.

УДК 519.651 DOI 10.17223/2226308X/9/2

ОБ ОДНОМ КРИТЕРИИ ПРОВЕРКИ ГИПОТЕЗЫ О НАЛИЧИИ ВКРАПЛЕНИЙ В ДВОИЧНОЙ ЦЕПИ МАРКОВА

А. В. Волгин

Рассматривается модель побитового вкрапления в простые цепи Маркова с неизвестной матрицей переходных вероятностей, основанная на LSB-методе. Получено условие на взаимное асимптотическое соотношение длины отрезка исходной последовательности и объёма вкраплений, позволяющее гарантировать состоятельность статистического критерия выявления факта наличия вкраплений.

Ключевые слова: *цепи Маркова, вкрапления в псевдослучайные последовательности, статистические критерии различия гипотез.*

В [1] рассматриваются условия, при которых возможно гарантированно обнаружить факт наличия независимых вкраплений в простой конечной неразложимой и ацикличной цепи Маркова с неизвестной матрицей переходных вероятностей в рамках следующей модели: к каждому элементу исходной последовательности применяется случайное преобразование. При этом преобразования получены по схеме серий и являются независимыми. В данной работе получено дополнительное (по сравнению с [1]) условие на взаимное асимптотическое соотношение длины отрезка исходной последовательности и объёма вкраплений, позволяющее гарантировать состоятельность статистического критерия выявления факта наличия вкраплений.

Пусть $X = \{X_0, X_1, \ldots\}$ — простая конечная неразложимая и ацикличная цепь Маркова с двумя состояниями 0, 1 и фиксированной положительной матрицей переходных вероятностей $\Pi = (\pi_{a,b})_{2\times 2}$, $a, b \in \{0, 1\}$. Стационарное распределение цепи обозначим через $\pi = (\pi_0, \pi_1)$, $\pi_0, \pi_1 \in (0, 1)$. В процедуре внесения вкраплений используются две последовательности — $Z = \{Z_0, Z_1, \ldots\}$ и $\delta = \{\delta_0, \delta_1, \ldots\}$, $Z_i, \delta_i \in \{0, 1\}$, $i \geqslant 0$, которые являются реализациями испытаний в схеме Бернулли. При этом $\mathbf{P}\{Z_i = a\} = p_a$, $p_a \neq \pi_a$, $a \in \{0, 1\}$, и $\mathbf{P}\{\delta_i = 0\} = \tau$, $i \geqslant 0$, $p_a, \tau \in [0, 1]$. В результате внесения вкраплений образуется последовательность $Y = \{Y_0, Y_1, \ldots\}$:

$$Y_i = X_i \mathbf{I}\{\delta_i = 1\} + Z_i \mathbf{I}\{\delta_i = 0\}, \quad i \geqslant 0,$$

где через $\mathbf{I}\{A\}$ обозначается индикатор события A. При этом предполагается, что последовательности X, Z и δ являются независимыми.

Постановка задачи заключается в следующем. Наблюдается отрезок двоичной последовательности $(Y_0, \ldots, Y_{n-1})$ длины n. Относительно способа образования данного отрезка выдвигаются две сложные гипотезы $H_0 : \tau = 0$ и $H_1 : \tau > 0$ об отсутствии и наличии вкраплений в цепь Маркова X соответственно. При обеих гипотезах будем предполагать, что матрица Π, стационарное распределение π цепи Маркова X, а также величины p_a, $a \in \{0, 1\}$, и τ неизвестны. Рассмотрим схему серий, в которой

$$\tau = \tau(n) \to 0 \quad \text{при } n \to \infty.$$

Задача заключается в построении состоятельного критерия различия гипотез H_0 и H_1.

В [1] для выявления факта наличия вкраплений в цепь Маркова рассматривается статистика

$$S = \sum_{a,b,c\in\{0,1\}} \frac{\left(\nu_{abc} - \nu_{ab}\nu_{bc}/\nu_b\right)^2}{\nu_{ab}\nu_{bc}/\nu_b}, \tag{1}$$

где $a, b, c \in \{0, 1\}$,

$$\nu_{abc} = (n-2)^{-1} \sum_{i=0}^{n-3} \mathbf{I}\{Y_i = a, Y_{i+1} = b, Y_{i+2} = c\},$$

$$\nu_{ab} = (n-1)^{-1} \sum_{i=0}^{n-2} \mathbf{I}\{Y_i = a, Y_{i+1} = b\}, \quad \nu_a = n^{-1} \sum_{i=0}^{n-1} \mathbf{I}\{Y_i = a\},$$

при этом в [1] рассматривается не двоичный, а произвольный конечный алфавит состояний цепи Маркова.

Рассмотрим критерий проверки гипотезы H_0 против H_1, основанный на статистике (1):

$$\text{принимается гипотеза } \begin{cases} H_0, \text{ если } S < t_{\chi^2_2, 1-\alpha}, \\ H_1, \text{ если } S \geqslant t_{\chi^2_2, 1-\alpha}, \end{cases} \tag{2}$$

где $\alpha = \mathbf{P}\left\{S \geqslant t_{\chi^2_2,1-\alpha} \middle| H_0\right\}$ – вероятность ошибки первого рода; $t_{\chi^2_2,\alpha}$ – квантиль уровня α распределения χ-квадрат с двумя степенями свободы.

Теорема 1. Пусть в модели вкраплений $p_a \neq \pi_a$, $a \in \{0, 1\}$, и среди элементов матрицы переходных вероятностей П есть хотя бы один, отличный от $1/2$. Тогда при выполнении условий

$$\tau \to 0, \ n \to \infty, \tag{3}$$

$$\sqrt{n}\tau \to \infty, \ n \to \infty, \tag{4}$$

критерий (2) проверки гипотезы H_0 против альтернативы H_1 является состоятельным.

Замечание 1. При отсутствии вкраплений ($\tau \equiv 0$) и при наличии вкраплений во всех позициях последовательности X ($\tau \equiv 1$) гипотезы H_0 и H_1 неразличимы, поскольку в обоих случаях Y является простой однородной цепью Маркова (с глубиной зависимости 1 и 0 соответственно). Критерий будет состоятельным, когда вкраплений «не слишком много», что гарантируется условием (3), но в то же время когда число вкраплений превосходит по порядку квадратный корень из длины наблюдаемого отрезка последовательности X (условие (4)).

ЛИТЕРАТУРА

1. *Шойтов А. М.* О выявлении факта зашумления конечной цепи Маркова с неизвестной матрицей переходных вероятностей // Прикладная дискретная математика. Приложение. 2010. № 3. С. 44–45.

УДК 519.7 DOI 10.17223/2226308X/9/3

АЛГОРИТМ РАСПОЗНАВАНИЯ ПОЛНОТЫ МНОЖЕСТВА СЛОВ И ДИНАМИКА ЗАПРЕТОВ[1]

А. А. Евдокимов

Вводятся инвариантные операции и даётся описание алгоритма распознавания полноты множества слов. Приводится теорема о результатах работы алгоритма и их отношении к свойству полноты исходного множества слов. Формулируется

[1]Работа поддержана Новосибирским государственным университетом и грантом РФФИ, проект № 14-01-00507.

нерешённая задача об оценке мощностей полных тупиковых множеств слов.

Ключевые слова: *множество слов, полнота, динамика запретов, алгоритм распознавания.*

Задачи о полноте множества слов и избегаемости запрещённых подслов бесконечными символьными последовательностями были впервые сформулированы в [1] и исследованы в [2 – 4]. Литературу можно посмотреть в [4, 5] в контексте более широкой области исследования, называемой «Combinatorics on words».

Исследованию языков, определяемых заданием запрещённых подслов и иначе называемых в последние годы «антисловарями», посвящено большое число публикаций с указанием различных приложений. В частности, это задачи анализа и синтеза криптографических функций и символьных последовательностей, в которых важны информационные и сложностные характеристики, связанные с изучением взаимосвязи со свойствами их подфункций или подслов.

Множество S слов (запретов) в алфавите A называется *полным* (или *блокирующим*), если любая бесконечная последовательность букв из A не свободна от S, то есть содержит в качестве своего подслова хотя бы одно слово из S [1, 2].

Подмножество $T \subseteq S$, $T = \{X_1 a_{i_1}, \ldots, X_m a_{i_m}\}$, где $m = |A|$, образует тупиковую относительно S систему слов (ТСС), если

1) все последние буквы слов в T различны (т. е. это все m букв алфавита A);
2) для всех $i = 1, \ldots, m-1$ слово X_i есть суффикс слова X_{i+1}.

Если в S существует ТСС, то применение к ней Т-операции состоит в удалении в самом длинном слове $X_m a_{i_m}$ его последней буквы a_{i_m} (если в ТСС самое длинное слово не единственно, то выбираем любое). Удобно считать, что если $S = A$, то есть S — это множество всех букв алфавита A, то Т-операция применима к S и её результатом является пустое множество. Сочетая Т-операцию сокращения множества S с двумя другими естественными операциями сокращения — удалением из S одного из двух одинаковых слов и удалением слова X, если в S содержится подслово слова X, получаем последовательность множеств, которая в силу конечности S стабилизируется:

$$S \to S_1 \to S_2 \to \ldots \to S^*.$$

Теорема 1. Приведённые операции инвариантны относительно свойства множества S быть полным. Их применение (в любом порядке) распознает полноту множества S:

1) либо $S^* = \varnothing$, и тогда S — полное множество;
2) либо $S^* \neq \varnothing$ и к S^* неприменимы операции сокращения, и тогда S — неполное.

Основанный на теореме алгоритм распознавания полноты прост, но этап проверки наличия в S тупиковой системы слов, к которой применима Т-операция, трудоёмок. Однако, в отличие от полиномиального алгоритма в [3], этот алгоритм позволяет работать со словами различной длины в множестве S и получить сокращённое множество S^*, эквивалентное S.

Представляет интерес более широкая постановка вопроса о сохранении свойства полноты при изменениях в S, а также то, насколько свойство устойчиво к «ошибкам», например удалению букв в словах или самих слов из S. Расширяя неполные множества и сужая полные, можно находить границы перехода и управлять динамикой изменения свойства полноты и избегаемости запретов S. В этой связи важно получить ответ

на следующий вопрос: насколько велико может быть различие мощностей полных тупиковых (несокращаемых) множеств S, $S \subseteq A^n$? Например, как ведёт себя (по n при фиксированном m) функция

$$f(m,n) = \max |S_1|/|S_2|,$$

где $m = |A|$, а максимум берётся по всем парам $\{S_1, S_2\}$ полных тупиковых множеств, $S_1, S_2 \subseteq A^n$? Можно доказать, что эта функция не ограничена никакой константой. Более точные оценки её роста значительно прояснили бы структуру полных множеств слов.

ЛИТЕРАТУРА

1. *Евдокимов А. А., Крайнев В. А.* Задачи о полноте систем слов // XXII Обл. науч.-технич. конф. Тезисы. Новосибирск, 1979. С. 105–107.
2. *Евдокимов А. А.* Полные множества слов и их числовые характеристики // Методы дискретного анализа в исследовании экстремальных структур: сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1983. Вып. 39. С. 7–19.
3. *Евдокимов А. А.* Исследование полноты множеств слов и языков с запретами // Вестник Томского государственного университета. Приложение. 2004. № 9(1). С. 8–12.
4. *Evdokimov A. A. and Kitaev S. V.* Crucial words and the complexity of some extremal problems for sets of prohibited words // J. Comb. Theory. Ser. A. 2004. V. 105. P. 273–289.
5. *Berstel J. and Karhumäki J.* Combinatorics on words — a tutorial // Bull. EATCS. 2003. V. 79. P. 178–229.

УДК 512.624.5 DOI 10.17223/2226308X/9/4

О ДОСТАТОЧНОМ УСЛОВИИ ДЛЯ ОТСУТСТИЯ ВОЗМОЖНОСТИ СОКРАЩЕНИЯ ПЕРИОДА В СТАРШИХ ДВОИЧНЫХ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ НАД ПРИМАРНЫМИ КОЛЬЦАМИ

С. А. Кузьмин

Рассматриваются двоичные разрядные последовательности над примарными кольцами нечётной характеристики. Указано достаточное условие для отсутствия сокращения периода в старших разрядных последовательностях в 2 раза при наличии не всех элементов на цикле исходной линейной рекурренты.

Ключевые слова: *линейные рекуррентные последовательности, периоды последовательностей, примарные кольца, разрядные последовательности.*

В настоящее время наблюдается особый интерес к изучению p-ичных разрядных последовательностей над кольцами вычетов по модулю p^n. Это связано с тем, что данные последовательности обладают высокой линейной сложностью и могут быть использованы в датчиках псевдослучайных последовательностей. Со списком работ по данной тематике можно ознакомиться, например, в [1].

Большое внимание уделяется задаче восстановления линейных рекуррентных последовательностей (ЛРП) над примарными кольцами вычетов по их усложнению, особенно в тех случаях, когда ЛРП максимального периода (ЛРП МП) отображается в свою старшую координатную последовательность [2].

Меньше работ посвящено r-ичным разрядным последовательностям, где $r \neq p$, которые также могут быть рассмотрены как усложнения линейных рекуррент над простыми полями и кольцами Галуа. Такие последовательности рассматривались

А. С. Кузьминым в [3]. Им найдены все двоичные разрядные последовательности ЛРП МП над конечным простым полем нечётной характеристики, в которых наблюдается эффект сокращения периода. В [4] эти результаты обобщены и доказано, что сокращение периода в r-ичных разрядных последовательностях над конечным простым полем, где $r > 2$, невозможно.

Любой знак $u(i)$ некоторой ЛРП МП u над примарным кольцом представим в виде

$$u(i) = \sum_{s=0}^{k} u_s(i) 2^s,$$

где $k = [\log_2 p^n]$. Таким образом, последовательность вида $u_s = (u_s(0), u_s(1), \ldots)$, является s-й разрядной последовательностью ЛРП МП u над примарным кольцом. Обозначим $T(u)$, $T(u_l)$ периоды последовательностей u и u_l.

В [5] сформулирован результат о том, что при наличии всех элементов на цикле ЛРП МП u существует только один номер z двоичной разрядной последовательности над кольцом Галуа, зависящий от вида числа p и степени n, для которого $T(u_z) | (T(u)/2)$. Вопрос о возможности сокращения периода в 2 раза в противном случае остался незатронутым.

Лемма 1. Для всех возможных пар элементов a и b кольца $\mathbb{Z}_{p^n}$, таких, что выполняется соотношение $a + b \equiv 0 \pmod{p^n}$, справедлива следующая формула для нахождения числа μ_l пар, у которых совпадают l-е двоичные разряды:

$$\mu_l = 2 \min_l \left\lfloor \frac{(p^n - 1)/2 - 2^l + \min_l}{2^l} \right\rfloor + \min\left(2 \min_l, ((p^n - 1)/2 - 2^l + \min_l) \bmod 2^l\right) + \min_l,$$

где $\min_l = \min(((p^n - 1)/2) \bmod 2^l, 2^l - ((p^n - 1)/2 + 1) \bmod 2^l) + 1$.

Замечание 1. Заметим, что так как $1 \leqslant \min_l \leqslant 2^{l-1} - 1$, то верхняя и нижняя оценки числа μ_l могут быть получены тривиальным образом.

Полученное значение μ_l может быть использовано для доказательства следующих утверждения и теоремы.

Утверждение 1. Пусть u — ЛРП МП над кольцом $\mathbb{Z}_{p^n}$ с характеристическим многочленом $f(x)$, $\deg f = m$, пусть также на цикле последовательности u встречаются $2\mu_l$ различных элементов из $\mathbb{Z}_{p^n}$. Тогда для отсутствия сокращения периода в разрядной последовательности с номером $l > z$ (см. [5]) в 2 раза достаточно выполнения неравенства

$$p^{n-1}(p^m - 1) > (2\mu_l)^m. \tag{1}$$

Замечание 2. Данное утверждение носит скорее теоретический характер, на практике доля номеров двоичных разрядных последовательностей, для которых выполняется неравенство (1) в случае различных p, n, m и l, мала.

Теорема 1. Пусть u — ЛРП над примарным кольцом $\mathbb{Z}_{p^n}$. Если на цикле последовательности u встречается более $2\mu_l$ различных элементов, то $T(u_l) \not| (T(u)/2)$.

ЛИТЕРАТУРА

1. *Сачков В. Н., Горчинский Ю. Н., Зубков А. Н., Яблонский С. В.* Труды по дискретной математике. Т. 1. М.: ТВП, 1997. 280 с.
2. *Кузьмин А. С., Маршалко Г. Б., Нечаев А. А.* Восстановление линейной рекуррентной последовательности над примарным кольцом вычетов по её усложнению // Математические вопросы криптографии. 2010. Т. 1. Вып. 2. С. 31–56.

3. *Кузьмин А. С.* О периодах разрядов в r-ичной системе счисления знаков линейных рекуррентных последовательностей над конечными простыми полями // Безопасность информационных технологий. 1995. Вып. 4. С. 71–75.
4. *Кузьмин С. А.* Периоды разрядных последовательностей линейных рекуррент максимального периода над конечными простыми полями // Прикладная дискретная математика. 2015. № 1(27). С. 62–68.
5. *Кузьмин С. А.* О двоичных разрядных последовательностях над кольцами Галуа, допускающих эффект сокращения периода // Фундамент. и прикл. матем. 2015. Т. 20. № 1. С. 223–230.

УДК 519.7 DOI 10.17223/2226308X/9/5

О ГРУППАХ, ПОРОЖДЁННЫХ ПРЕОБРАЗОВАНИЯМИ СМЕШАННОГО ТИПА И ГРУППАМИ НАЛОЖЕНИЯ КЛЮЧА

Б. А. Погорелов, М. А. Пудовкина

Наиболее распространёнными группами наложения ключа итерационных алгоритмов блочного шифрования являются регулярное подстановочное представление V_n^+ группы векторного наложения ключа, регулярное подстановочное представление $\mathbb{Z}_{2^n}^+$ аддитивной группы кольца вычетов и регулярное подстановочное представление $\mathbb{Z}_{2^n+1}^\odot$ мультипликативной группы простого поля (2^n+1 — простое число). Рассматривается расширение группы $G_n = \langle V_n^+, \mathbb{Z}_{2^n}^+ \rangle$ преобразованиями и группами, естественными для криптографической практики. К числу таких преобразований и групп относятся: группы $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$ и $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$, подстановка псевдообращения над полем $\mathrm{GF}(2^n)$ или кольцом Галуа $\mathrm{GR}(2^{md}, 2^m)$.

Ключевые слова: *группа наложения ключа, аддитивная регулярная группа, сплетение групп подстановок, мультипликативная группа кольца вычетов, кольцо Галуа.*

Группы наложения ключа итерационных алгоритмов блочного шифрования являются, как правило, регулярными абелевыми. Среди них наиболее распространены следующие:

— V_n^+ — регулярное подстановочное представление группы векторного наложения ключа над полем $\mathrm{GF}(2)$. Оно является элементарной абелевой 2-группой и используется в AES, Р34.12-2015 «Кузнечик» и многих других алгоритмах блочного шифрования. Группа V_n^+ имеет $(2^n-1)\dots(2^n-2^{r-1})/(2^r-1)\dots(2^2-1)(2-1)$ изоморфных подгрупп порядка 2^r, $r=1,\dots,n$, и столько же систем импримитивности;

— $\mathbb{Z}_{2^n}^+$ — регулярное подстановочное представление аддитивной группы кольца вычетов. Оно используется, например, в алгоритме блочного шифрования ГОСТ 28147-89. Из цикличности группы следует, что у неё имеется $n-1$ собственных подгрупп и столько же систем импримитивности;

— $\mathbb{Z}_{2^n+1}^\odot$ — регулярное подстановочное представление мультипликативной группы простого поля, в которой элемент 2^n переобозначается как 0 (модульное умножение), а 2^n+1 — простое число. Как мультипликативная группа конечного поля она циклическая порядка 2^n с $n-1$ собственной подгруппой.

В этом смысле последние два способа наложения ключа предпочтительней, так как необходимо, чтобы слой s-боксов и линейный слой рассеивали меньшее число систем импримитивности.

Пусть $G_n = \left\langle V_n^+, \mathbb{Z}_{2^n}^+ \right\rangle$, $S(X)$ — симметрическая группа на множестве X, $G_1 \wr G_2$ — сплетение групп подстановок G_1, G_2.

В [1, 2] описано строение группы G_n и её свойства. В данной работе рассматривается расширение группа G_n преобразованиями и группами, естественными для криптографической практики. К числу таких преобразований и групп относятся: группы $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$ и $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$, подстановка псевдообращения над полем $\mathrm{GF}(2^n)$ или кольцом Галуа $\mathrm{GR}(2^{md}, 2^m)$.

Первоначально описаны свойства групп, порождённых G_n, $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$, $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$ для $d \in \{1, \ldots, n-1\}$, $n \geqslant 2$. Доказано, что если $n \geqslant 2$, то $\left\langle \mathbb{Z}_{2^d}^+ \times V_{n-d}^+, G_n \right\rangle = G_n$ для $d = 1, \ldots, n-1$ и

$$\left\langle G_n, V_{n-d}^+ \times \mathbb{Z}_{2^d}^+ \right\rangle = \begin{cases} S(V_n), & \text{если } d \in \{2, \ldots, n-1\}, \\ G_n, & \text{если } d = 1. \end{cases}$$

Кроме того,

$$\left\langle V_{d_1}^+ \times Z_{2^{d_0}}^+ \times V_{n-d}^+, G_n \right\rangle \approx S(V_d) \wr G_{n-d}$$

для любых $d \in \{3, \ldots, n\}$, $d_0 \in \{2, \ldots, n-d-1\}$, где $d_1 = n - d_0$.

Для $n \geqslant 2$ и подстановки $g_n : \mathrm{GF}(2^n) \to \mathrm{GF}(2^n)$, заданной условием

$$g_n : \lambda \mapsto \begin{cases} \lambda^{-1}, & \text{если } \lambda \neq 0, \\ 0, & \text{если } \lambda = 0, \end{cases}$$

доказаны равенства $\left\langle g_n, \mathbb{Z}_{2^n}^+ \right\rangle = \langle g_n, G_n \rangle = S(V_n)$.

Пусть $LT_2\left(\mathbb{Z}_{2^{n/2}}\right)$ — группа нижнетреугольных матриц из $GL_2\left(\mathbb{Z}_{2^{n/2}}\right)$. Для чётного числа $n \geqslant 4$ доказано, что

$$LT_2\left(\mathbb{Z}_{2^{n/2}}\right) < G_n, \langle G_n, GL_2\left(\mathbb{Z}_{2^{n/2}}\right)\rangle = S(V_n).$$

Рассмотрим теперь связь подстановочного представления $\mathbb{Z}_{2^n+1}^{\odot}$ мультипликативной группы кольца $\mathbb{Z}_{2^n+1}$ и группы G_n. Пусть $\mathbb{Z}_{2^n+1}^*$ — мультипликативная группа кольца $\mathbb{Z}_{2^n+1}$ и для произвольного числа $r \in \mathbb{Z}_{2^n+1}^*$ преобразование $b^{(r)} \in S\left(\mathbb{Z}_{2^n}\right)$ задано условием $b^{(r)} : x \mapsto rx \bmod (2^n + 1)$. Положим $B_n = \left\langle b^{(r)} : r \in \mathbb{Z}_{2^n+1}^* \right\rangle$. Доказано, что если $n \geqslant 2$, то $\langle B_n, G_n \rangle = S(V_n)$. Кроме того,

$$\langle B_d \times B_{n-d}, G_n \rangle \approx S(V_d) \wr S(V_{n-d}), \quad d = 1, \ldots, n-1.$$

Для фиксированных произвольных чисел $m, d \in \mathbb{N}$ положим $n = md$. Рассмотрим кольцо Галуа $\mathrm{GR}(2^{md}, 2^m)$. Известно [3], что существует элемент b порядка $2^d - 1$, принадлежащий мультипликативной группе кольца Галуа $\mathrm{GR}\left(2^{md}, 2^m\right)$. Рассмотрим преобразование $\tilde{u}_b^{(n)} : \mathrm{GR}\left(2^{md}, 2^m\right) \to \mathrm{GR}\left(2^{md}, 2^m\right)$, заданное условием $\tilde{u}_b^{(n)} : \alpha \mapsto b\alpha$ для каждого $\alpha \in \mathrm{GR}\left(2^{md}, 2^m\right)$. Доказаны равенства

$$\left\langle G_n, \tilde{u}_b^{(n)} \right\rangle = \left\langle G_n, GL_1\left(\mathrm{GR}(2^{md}, 2^m)\right)\right\rangle = S(V_n).$$

Положим $m = 2$, $n = 2d$ и рассмотрим кольцо Галуа $\mathrm{GR}(4^d,\ 4)$ характеристики 4. Определим биекцию $\tilde{s}_d^{(2)} : \mathrm{GR}(4^d,\ 4) \to \mathrm{GR}(4^d,\ 4)$ условием

$$\tilde{s}_d^{(2)} : 2\alpha_1 + \alpha_0 \mapsto \begin{cases} \alpha\alpha_0^{-2}, & \text{если } \alpha_0 \neq 0, \\ 2\alpha_1^{-1}, & \text{если } \alpha_0 = 0, \alpha_1 \neq 0, \\ 0, & \text{если } \alpha_0 = \alpha_1 = 0, \end{cases}$$

для каждого элемента $\alpha = 2\alpha_1 + \alpha_0 \in \mathrm{GR}(4^d, 4)$, где $\alpha_0, \alpha_1 \in \mathrm{GF}(2^d)$. Преобразование $\tilde{s}_d^{(2)}$ является аналогом подстановки g_n. Очевидно, что $\tilde{s}_d^{(2)}$ — инволюция. Доказано, что $\left\langle \tilde{s}_d^{(2)}, G_n \right\rangle = S(V_d) \wr S(V_d)$.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* Надгруппы аддитивных регулярных групп порядка 2^n кольца вычетов и векторного пространства // Дискретная математика. 2015. Т. 27. № 3. С. 74–94.
2. *Погорелов Б. А., Пудовкина М. А.* Орбитальные производные по подгруппам и их комбинаторно-групповые свойства // Дискретная математика. 2015. Т. 27. № 4. С. 94–119.
3. *Елизаров В. П.* Конечные кольца. М.: Гелиос АРВ, 2006.

УДК 519.7 DOI 10.17223/2226308X/9/6

О КЛАССИФИКАЦИИ ДИСТАНЦИОННО-ТРАНЗИТИВНЫХ ГРАФОВ ОРБИТАЛОВ НАДГРУПП ГРУППЫ ДЖЕВОНСА

Б. А. Погорелов, М. А. Пудовкина

Группа экспоненцирования $S_2 \uparrow S_n$, называемая также группой Джевонса, совпадает с группой $A\tilde{S}_n$, порождённой группой сдвигов на n-мерном векторном пространстве V_n над полем $\mathrm{GF}(2)$ и группой подстановочных $(n \times n)$-матриц $\tilde{S}_n$ над полем $\mathrm{GF}(2)$. Для группы подстановок $G \geqslant S_2 \uparrow S_n$ рассматривается её естественное действие на упорядоченных парах векторов из пространства V_n. Орбиты при таком действии называются орбиталами. Каждому орбиталу Γ ставится в соответствие граф с множеством вершин V_n и множеством рёбер Γ, называемый графом орбитала. Проводится классификация дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса. Показано, что среди дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса имеются графы, изоморфные следующим графам: полному графу K_{2^n}, полному двудольному графу $K_{2^{n-1},2^{n-1}}$, половинному $(n+1)$-кубу, сложенному $(n+1)$-кубу, графам знакопеременных форм, графу Тейлора, графу Адамара.

Ключевые слова: *граф орбитала, группа Джевонса, дистанционно-транзитивный граф, граф Хемминга.*

Группа экспоненцирования $S_2 \uparrow S_n$, называемая также группой Джевонса, совпадает с группой $A\tilde{S}_n$, порождённой группой сдвигов на n-мерном векторном пространстве V_n над полем $\mathrm{GF}(2)$ и группой подстановочных $(n \times n)$-матриц $\tilde{S}_n$ над полем $\mathrm{GF}(2)$. Группа Джевонса встречается в теории кодирования, теории графов, теории булевых функций, алгебраической комбинаторике и криптографии; в частности, она

— является группой изометрий метрики Хемминга на V_n;
— описывает множество преобразований, не распространяющих искажения;
— является группой инерции множества всех бент-функций.

Для группы подстановок $G \geqslant S_2 \uparrow S_n$ рассматривается также её естественное действие на упорядоченных парах векторов из пространства V_n. Орбиты при таком действии называются орбиталами. Каждому орбиталу Γ ставится в соответствие граф $\bar{\Gamma} = (V_n, \Gamma)$ с множеством вершин V_n и множеством рёбер Γ, называемый графом орбитала. В алгебраической комбинаторике группа Джевонса связана со схемой отношений Хемминга [1] на пространстве V_n, которая может задаваться алгеброй матриц смежности графов орбиталов группы $A\tilde{S}_n$. При этом орбиталы пронумерова-

ны таким образом, что орбита стабилизатора нулевого вектора группы $A\tilde{S}_n$ совпадает с множеством $\Delta_i^{(n)} \subset V_n$ всех векторов веса Хемминга i, а i-й орбитал есть $\Gamma_i^{(n)} = \left\{(\beta, \beta') \in V_n^2 : \beta \oplus \beta' \in \Delta_i^{(n)}\right\}$ для всех $i \in \{0, \ldots, n\}$, где $\oplus$ — бинарная операция покоординатного сложения векторов из V_n.

В [2, 3] проведена классификация всех надгрупп G группы $A\tilde{S}_n$, $A\tilde{S}_n \leqslant G \leqslant S(V_n)$, для $n \geqslant 4$. Она позволила в [4, 5] описать графы орбиталов всех надгрупп группы Джевонса и их группы автоморфизмов. В [5] среди графов орбиталов надгрупп группы Джевонса описаны графы, принадлежащие к таким известным классам, как дистанционно-транзитивные, антиподальные и двудольные. Заметим, что классификации дистанционно-транзитивных графов уделяется повышенное внимание более 40 лет (см. [1, 6 – 10] и др.). Это зачастую вызвано тем, что не только некоторые известные графы дистанционно-транзитивны, но также некоторые интересные группы являются группами автоморфизмов дистанционно-транзитивных графов. Так, дистанционно-транзитивными являются графы Хемминга, Джонсона, Гроссманна, полный двудольный и т. д. Описаны (см., например, [6]) все дистанционно-транзитивные графы, степени вершин которых не превосходят 13. Заметим, что из полной классификации групп ранга 3 [11] следует описание групп автоморфизмов дистанционно-транзитивных графов диаметра 2, называемых сильно регулярными.

В данной работе проводится классификация дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса. Показано, что среди дистанционно-транзитивных графов орбиталов надгрупп группы Джевонса имеются графы, изоморфные следующим графам: 1) полному графу K_{2^n}; 2) полному двудольному графу $K_{2^{n-1},2^{n-1}}$; 3) половинному $(n+1)$-кубу; 4) сложенному $(n+1)$-кубу; 5) сложенному половинному $(n+2)$-кубу; 6) графам знакопеременных форм; 7) графу Тейлора (для графов диаметра 3); 8) дополнению $2 \times 2^{n-1}$-решётки (для графов диаметра 3); 9) дополнению графа $2^{n-1}K_2$, состоящего из 2^{n-1} двухвершинных компонент связности; 10) графу Адамара (для графов диаметра 4); 11) графам инцидентности 2-$(2^{n-1}, u_i^{(n)}, 2u_{i-1}^{(n-2)})$ блок-схем (для графов диаметра 3 при нечётном $n \geqslant 5$), $i \in \{1, 3\}$, где

$$u_j^{(n)} = \sum_{k=0}^{\lfloor (n-j)/4 \rfloor} \binom{n}{4k+j}, \quad j = 0, 1, 2, 3.$$

При этом графы диаметра 2 изоморфны одному из следующих классов графов: 1) графу $K_{2^{n-1},2^{n-1}}$; 2) дополнению графа $2^{n-1}K_2$; 3) графам знакопеременных форм, группы автоморфизмов которых изоморфны ортогональным группам $AO_n^{(1)}$, $AO_n^{(2)}$ при чётном n.

ЛИТЕРАТУРА

1. *Баннаи Э., Ито Т.* Алгебраическая комбинаторика. М.: Мир, 1987.
2. *Погорелов Б. А.* Подметрики метрики Хемминга и теорема А.А. Маркова // Труды по дискретной математике. 2006. № 9. С. 190–219.
3. *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.
4. *Погорелов Б. А., Пудовкина М. А.* Подметрики Хемминга и их группы изометрий // Труды по дискретной математике. 2008. Т.11. № 2. С. 32–68.
5. *Погорелов Б. А., Пудовкина М. А.* Свойства графов орбиталов надгрупп группы Джевонса // Математические вопросы криптографии. 2010. Т.1. № 1. С. 55–84.

6. *Brouwer A. E., Cohen A. M., and Neumaier A.* Distance-Regular Graphs. Springer Verlag, 1989.
7. *Praeger C. E., Saxl J., and Yokoyama K.* Distance transitive graphs and finite simple groups // Proc. London Math. Soc. 1987. V. 55. P. 1–21.
8. *Ivanov A. A.* Distance-transitive graphs and their classification // Investigations in Algebraic Theory of Combinatorial Objects / eds. I. A. Faradzev et al. Dordrecht: Springer Science + Business Media, 1994. P. 283–378.
9. *Cohen A. M.* Distance-transitive graphs // Encycloped. Math. Applicat. 2004. V. 102. P. 222–249.
10. *Van Bon J.* Finite primitive distance-transitive graphs // European J. Combinatorics. 2007. V. 28. P. 517–532.
11. *Liebeck M. W. and Saxl J.* The finite primitive permutation groups of rank three // Bull. London Math. Soc. 1986. V. 18. P. 165–172.

Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/9/7

О СПЕЦИАЛЬНОМ ПОДКЛАССЕ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ И ПРОБЛЕМЕ СУЩЕСТВОВАНИЯ APN-ПЕРЕСТАНОВОК[1]

В. А. Виткуп

Известным открытым вопросом в области векторных булевых функций является проблема существования APN-перестановок от чётного числа переменных. Рассматривается множество векторных булевых функций специального вида, добавление к которым аффинной функции приводит к перестановке. Исследуются свойства этого множества, а также возможность и условия существования непустого пересечения с множеством APN-функций.

Ключевые слова: *векторная булева функция, APN-функция, взаимно однозначная функция, перестановка.*

Векторной булевой функцией (*S-блоком*) называется произвольное отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$. Векторную функцию можно рассматривать как набор из m координатных булевых функций от n переменных, т. е. $F = (f_1, \ldots, f_m)$. Далее в работе рассматриваются только функции вида $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Появление в 1990 г. дифференциального криптоанализа вызвало необходимость поиска функций, наиболее стойких к данному методу. Так, в 1992 г. было предложено понятие APN-функции, а затем и дифференциально δ-равномерной функции [1]. Векторная булева функция называется *APN-функцией* (почти совершенно нелинейной), если уравнение $F(x+a)+F(x) = b$ имеет не более двух решений для любых $a \in \mathbb{F}_2^n \setminus \{0\}$, $b \in \mathbb{F}_2^n$. Первый пример APN-функции был указан ещё в 1968 г. В. А. Башевым и в дальнейшем исследован Б. А. Егоровым [2]. Интересно, что именно эта функция была затем использована в качестве S-блока криптосистемы AES.

Центральное место в исследовании таких функций занимает проблема существования взаимно однозначных APN-функций (или *APN-перестановок*) при чётном n. В своё время была выдвинута гипотеза (и доказана для случая $n = 4$), что для чётного числа переменных APN-перестановок не существует, однако в 2009 г. Дж. Диллон и др. [3] опровергли это предположение, построив взаимно однозначную APN-функцию при $n = 6$. Более подробная информация содержится в [4, 5].

Настоящая работа посвящена изучению векторных функций со структурой множества значений определённого вида. Обозначим множество $M_y = \{x \in \mathbb{F}_2^n : F(x) = y\}$. Рассмотрим некоторую функцию F для произвольного n, такую, что для каждого y выполняется $|M_y| \in \{0, 2\}$, то есть множество всех аргументов функции разбивается на пары, на которых значение F совпадает. Будем обозначать класс таких функций $\mathcal{F}'_{n,n}$.

Две векторные функции F и G называются *аффинно эквивалентными*, если существуют аффинные перестановки A_1, A_2, такие, что выполнено $F = A_1 \circ G \circ A_2$. Заметим,

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

что взаимная однозначность, а также свойство функции быть APN сохраняются при таком преобразовании. Понятие аффинной эквивалентности расширяется следующим образом. Две векторные функции F и G называются *EA-эквивалентными* (расширенно аффинно эквивалентными), если существуют аффинные перестановки A_1, A_2 и аффинная функция A, такие, что выполнено $F = A_1 \circ G \circ A_2 + A$. Известно, что EA-эквивалентность сохраняет свойство функции быть APN, в то время как свойство взаимной однозначности может уже не сохраниться — прибавление аффинной функции может нарушить структуру перестановки.

Первая APN-перестановка от шести переменных была получена путём применения специального преобразования к некоторой APN-функции (которая изначально не являлась взаимно однозначной), такого, что эти функции CCZ-эквивалентны (другая эквивалентность более сложного вида, которая так же, как и EA-эквивалентность, сохраняет свойство функции быть APN). В этой работе мы пробуем реализовать похожую идею, однако в качестве преобразования рассмотрим частный случай EA-эквивалентности — когда преобразования A_1 и A_2 являются тождественными.

Хотелось бы выделить в множестве векторных булевых функций некоторый подкласс, состоящий из функций, отличающихся от перестановок на аффинную функцию, то есть таких, что добавление к ним аффинной функции приводит к взаимно однозначной функции. Если в таком классе при каких-то чётных n содержатся APN-функции, то мы бы получили конструктивное решение открытого вопроса о существовании взаимно однозначных перестановок от чётного числа переменных.

Лемма 1. Для любой векторной функции F из класса $\mathcal{F}'_{n,n}$ существует векторная функция S, каждая координатная булева функция которой сбалансированна или константна, такая, что $F + S$ — взаимно однозначная функция.

Напомним, что аффинные функции, отличные от константы, являются сбалансированными. Заметим, что произвольная аффинная векторная функция принадлежит множеству векторных функций S из леммы 1. Поэтому естественно предположить, что в классе $\mathcal{F}'_{n,n}$ может находиться искомый подкласс функций, отличающихся от перестановок на аффинную функцию.

Напомним, что под *расстоянием* между двумя булевыми функциями подразумевается расстояние Хэмминга между их векторами значений.

Лемма 2. Для любой булевой функции f чётного веса от n переменных, которая находится на расстоянии не более чем $2n + 2$ от константной функции, существует аффинная булева функция a, такая, что $a + f$ — сбалансированная функция.

Заметим, что все координатные булевы функции произвольной векторной функции F из класса $\mathcal{F}'_{n,n}$ имеют чётный вес. Значит, для векторных булевых функций, чьи координатные функции удовлетворяют условиям леммы 2, найдутся аффинные векторные функции, сумма с которыми даёт покоординатно сбалансированные векторные функции, частным случаем которых и являются перестановки.

Пусть K — множество всех таких функций F из $\mathcal{F}'_{n,n}$, что для каждой функции существует аффинная функция A, дающая в сумме с F взаимно однозначную функцию. Заметим, что множество K непусто. Действительно, для любого n в этом классе лежат функции $F_1 = (0, x_2, \ldots, x_n)$, $F_2 = (x_1, 0, x_2, \ldots, x_n)$, $\ldots$, $F_n = (x_1, x_2, \ldots, x_{n-1}, 0)$. Заметим, что если взять соответственно аффинные функции $A_1 = (x_1, 0, \ldots, 0)$, $A_2 = (0, x_2, 0, \ldots, 0)$, $\ldots$, $A_n = (0, \ldots, 0, x_n)$, то их суммы равны $A_i + F_i = (x_1, \ldots, x_n)$, то есть являются тождественной функцией, которая взаимно однозначна.

Сформулируем необходимое условие того, что функция из $\mathcal{F}'_{n,n}$ является APN-функцией.

Лемма 3. Пусть APN-функция F от n переменных принадлежит $\mathcal{F}'_{n,n}$, другими словами, множество наборов её аргументов разбивается на пары $x_{i,1}, x_{i,2}$, $i = 1, \ldots, 2^{n-1}$, такие, что для каждого i выполнено $F(x_{i,1}) = F(x_{i,2})$. Тогда для любых $j, k \in \{1, \ldots, 2^{n-1}\}$, $j \neq k$, справедливо $x_{j,1} + x_{j,2} + x_{k,1} + x_{k,2} \neq 0$.

Заметим, что из леммы 3 следует, в частности, что в классе $\mathcal{F}'_{2,2}$ не может быть APN-функций.

Гипотеза 1. Для любого $n > 2$ в классе $\mathcal{F}'_{n,n}$ есть APN-функции.

В результате компьютерных экспериментов при $n = 3$ обнаружено, что для каждой APN-функции из класса $\mathcal{F}'_{3,3}$, веса координатных функций которой равны 2 или 6, существует ровно 128 аффинных векторных функций, дающих в сумме с ней APN-перестановку. Для APN-функций с другими весами координатных функций также всегда существуют соответствующие аффинные функции. Естественно предположить далее, что для некоторых других n пересечение множества APN-функций с классом K также непусто. Заметим, что для $n = 4$ в классе K нет APN-функций, поскольку иначе существовала бы APN-перестановка от четырёх переменных, что, как известно, не так.

Гипотеза 2. Для некоторых значений $n \geqslant 5$ в классе K есть APN-функции.

Истинность гипотезы 2 для конкретных чётных значений n влечёт существование взаимно однозначных APN-функций для соответствующего числа переменных.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentily uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. *Глухов М. М.* О совершенно нелинейных и почти совершенно нелинейных функциях // Матем. вопр. криптограф. 2016. (в печати)
3. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An APN permutation in dimension six // Amer. Math. Soc. 2010. V. 518. P. 33–42.
4. *Туэжилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
5. *Carlet C.* Open questions on nonlinearity and on APN Functions // LNCS. 2015. V. 9061. P. 83–107.

УДК 519.7 DOI 10.17223/2226308X/9/8

О ДИФФЕРЕНЦИАЛЬНОЙ ЭКВИВАЛЕНТНОСТИ КВАДРАТИЧНЫХ APN-ФУНКЦИЙ[1]

А. А. Городилова

Для векторной булевой функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ определяется ассоциированная булева функция γ_F от $2n$ переменных по правилу: $\gamma_F(a, b) = 1$, где $a, b \in \mathbb{F}_2^n$, если $a \neq (0, \ldots, 0)$ и уравнение $F(x) + F(x + a) = b$ имеет решение, и $\gamma_F(a, b) = 0$ иначе. Вводится понятие дифференциально эквивалентных векторных булевых функций как функций, имеющих одинаковые ассоциированные булевы функции. Интересен вопрос описания классов дифференциальной эквивалентности почти

[1]Работа поддержана грантом РФФИ, проект 15-07-01328.

совершенно нелинейных (APN) функций, так как его решение может потенциально привести к новым конструкциям APN-функций. В работе начато изучение данного вопроса с исследования аффинных функций, прибавление которых к квадратичным APN-функциям не выводит за рамки их классов дифференциальной эквивалентности. Полностью описаны такие аффинные функции для известного класса APN-функций Голда. Получены вычислительные результаты для известных квадратичных APN-функций от малого числа переменных 2, ..., 8.

Ключевые слова: *векторная булева функция, почти совершенно нелинейная функция, дифференциальная эквивалентность.*

Отображение $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *почти совершенно нелинейной* функцией (APN-функцией), если для любых векторов $a, b \in \mathbb{F}_2^n$, $a \neq (0, \ldots, 0)$, уравнение $F(x) + F(x + a) = b$ имеет не более двух решений. APN-функции интересны для использования в криптографических приложениях в силу их оптимальной стойкости к дифференциальному методу криптоанализа. Обзорам APN-функций посвящены работы М. Э. Тужилина [1], А. Потта [2]. Некоторые открытые вопросы в области APN-функций представлены в работе К. Карле [3]. Например, открытому вопросу о существовании APN-подстановок посвящены работы М. М. Глухова [4], В. Н. Сачкова [5].

Для векторной функции F от n переменных определяется ассоциированная булева функция γ_F от $2n$ переменных по правилу $\gamma_F(a, b) = 1$, где $a, b \in \mathbb{F}_2^n$, если $a \neq (0, \ldots, 0)$ и уравнение $F(x) + F(x + a) = b$ имеет решение, и $\gamma_F(a, b) = 0$ иначе. Легко видеть, что F — APN-функция тогда и только тогда, когда $\mathrm{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$, где wt — вес Хэмминга булевой функции. Введём следующее определение.

Определение 1. Функции F и G называются *дифференциально эквивалентными*, если $\gamma_F = \gamma_G$. Обозначим класс дифференциальной эквивалентности F через $\mathcal{DE}_F$.

Говорят, что две векторные функции F и G *EA-эквивалентны*, если существуют аффинные взаимно однозначные функции A', A'' и аффинная функция A, такие, что $G = A' \circ F \circ A'' + A$. Дифференциальная и EA-эквивалентности сохраняют свойство функции быть почти совершенно нелинейной. Однако в настоящий момент не известно, вкладываются ли классы дифференциальной эквивалентности APN-функций в соответствующие классы EA-эквивалентности APN-функций. Ответ на этот вопрос может потенциально привести к новым конструкциям APN-функций.

Утверждение 1. Пусть F и G — EA-эквивалентные функции. Тогда $|\mathcal{DE}_F| = |\mathcal{DE}_G|$. Более того, если $G = A' \circ F \circ A'' + A$ и $\mathcal{DE}_F = \{F_1, \ldots, F_k\}$, то $\mathcal{DE}_G = \{A' \circ F_1 \circ A'' + A, \ldots, A' \circ F_k \circ A'' + A\}$.

Легко видеть, что класс дифференциальной эквивалентности любой APN-функции F содержит 2^{2n} тривиальных различных функций $F_{c,d}(x) = F(x + c) + d$, $c, d \in \mathbb{F}_2^n$. В [6] найден пример APN-функции от четырёх переменных, чей класс дифференциальной эквивалентности шире, чем тривиальный (состоящий из 2^{2n} функций $F_{c,d}$). В данной работе случай $n = 4$ рассмотрен полностью. В табл. 1 приведены значения мощностей классов дифференциальной эквивалентности APN-функций от малого числа переменных $n = 2, 3, 4$.

Поскольку задача описания класса дифференциальной эквивалентности в общем случае представляется сложной, в данной работе начато её рассмотрение применительно к квадратичным APN-функциям, а именно исследуется вопрос, когда функции F и $F + A$ дифференциально эквивалентны, где F — квадратичная APN-функция, а A — произвольная аффинная функция. Заметим, что для любой квадратичной

Таблица 1

n	Кол-во EA-классов	EA-представитель $F(x)$	$\deg(F)$	$\lvert\mathcal{DE}_F\rvert$
2	1	x^3	2	2^4
3	1	x^3	2	2^6
4	2	x^3	2	2^{10}
		$x^3 + (x^2 + x + 1)\,\mathrm{tr}(x^3)$	3	2^{10}

APN-функции 2^{2n} таких аффинных функций всегда существует, поскольку $F_{c,d}(x) = F(x + c) + d = F(x) + (F(x) + F(x + c) + d) = F(x) + A^F_{c,d}(x)$, где $A^F_{c,d}$ — аффинная функция в силу квадратичности F.

По аналогии с утверждением 1 справедливо следующее

Утверждение 2. Для квадратичной APN-функции F число различных аффинных функций A, таких, что F и $F + A$ дифференциально эквивалентны, инвариантно относительно EA-преобразования.

Для известного класса APN-функций Голда получена следующая теорема, полностью описывающая все аффинные функции, прибавление которых к исходной функции не выводит за рамки её класса дифференциальной эквивалентности. Напомним, что векторную функцию $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ можно рассматривать как функцию над конечным полем $\mathbb{F}_{2^n}$ и однозначно представлять в виде полинома степени не выше $2^n - 1$: $F(x) = \sum\limits_{i=0}^{2^n-1} a_i x^i$, где $a_i \in \mathbb{F}_{2^n}$. При этом степень функции равна $\max\{\mathrm{wt}(i) : \ a_i \neq 0\}$, где $\mathrm{wt}(i)$ — двоичный вес числа.

Теорема 1. Пусть F — APN-функция Голда от n переменных, $F(x) = x^{2^k+1}$ и $(k, n) = 1$. Тогда выполнены следующие утверждения:

1) если $n = 4t$ для некоторого t и $k = n/2 \pm 1$, то существуют в точности $2^{2n+n/2}$ различных аффинных функций A, таких, что F и $F + A$ дифференциально эквивалентны, при этом $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k} + \delta x^{2^j}$, где $\alpha, \lambda, \delta \in \mathbb{F}_{2^n}$; $\delta = \delta^{2^{n/2}}$; $j = k - 1$ при $k = n/2 + 1$ и $j = n - 1$ при $k = n/2 - 1$;
2) иначе существуют в точности 2^{2n} различных аффинных функций A, таких, что F и $F + A$ дифференциально эквивалентны, при этом $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k}$, где $\alpha, \lambda \in \mathbb{F}_{2^n}$.

Теорема 1 показывает, что среди APN-функций Голда существуют такие, чей класс дифференциальной эквивалентности шире, чем тривиальный. А именно это функции $F(x) = x^{2^{n/2\pm1}+1}$ при n, кратном 4 (заметим, что эти функции EA-эквивалентны). В табл. 2 приведены вычислительные результаты, полученные для всех известных EA-классов квадратичных APN-функций от 2 до 8 переменных. Отметим, что EA-классификация квадратичных APN-функций вплоть до 6 переменных известна полностью, а для 7 и 8 переменных найдена частичная классификация (см. [2]).

Как видно из табл. 2, для почти всех рассмотренных EA-классов существует только 2^{2n} тривиальных аффинных функций $A_{c,d}$. Исключения составляют следующие:

$n = 4$: APN-функция Голда x^3;

$n = 6$: APN-функция $u^7x^3 + x^5 + u^3x^9 + u^4x^{10} + x^{17} + u^6x^{18}$;

$n = 8$: APN-функция Голда x^9.

Таблица 2

n	Кол-во EA-классов	Кол-во аффинных функций A: $F + A \in \mathcal{DE}_F$
2	1	2^4
3	1	2^6
4	1	2^{10}
5	2	Для обоих классов: 2^{10}
6	13	Для одного класса: 2^{13}; для остальных 12 классов: 2^{12}
7	$\geqslant 487$	Для всех известных 487 классов: 2^{14}
8	$\geqslant 8179$	Для одного класса из известных 8179: 2^{20}; для остальных 8178 классов: 2^{16}

ЛИТЕРАТУРА

1. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3. С. 14–20.
2. *Pott A.* Almost perfect and planar functions // Des. Codes Cryptogr. 2016. V. 78. P. 141–195.
3. *Carlet C.* Open questions on nonlinearity and on APN functions // Arithmetic of Finite Fields. LNCS. 2015. V. 9061. P. 83–107.
4. *Глухов М. М.* О матрицах переходов разностей при использовании некоторых модулярных групп // Матем. вопр. криптограф. 2013. Т. 4. № 4. С. 27–47.
5. *Сачков В. Н.* Комбинаторные свойства дифференциально 2-равномерных подстановок // Матем. вопр. криптограф. 2015. Т. 6. № 1. С. 159–179.
6. *Городилова А. А.* О пересечении множеств значений производных APN-функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 25–27.

УДК 512.542.3 DOI 10.17223/2226308X/9/9

ФУНКЦИИ С ВАРИАЦИОННО-КООРДИНАТНОЙ ПОЛИНОМИАЛЬНОСТЬЮ НАД ГРУППОЙ

А. И. Зуева, А. В. Карпов

Определён класс функций с вариационно-координатной полиномиальностью над группой, являющийся обобщением класса ВКП-функций над примарным кольцом вычетов. Представлен алгоритм нахождения координат для элемента группы. Доказано, что класс ВКП-функций над $UT_n(\mathbb{Z}_p)$ не совпадает с классом полиномиальных функций. Указан способ обращения биективной ВКП-функции над $UT_n(\mathbb{Z}_p)$.

Ключевые слова: *функции над группой, функции с вариационно-координатной полиномиальностью, координатные функции.*

В [1] определён класс функций с вариационно-координатной полиномиальностью (ВКП-функций) над примарным кольцом вычетов, порождающий системы ВКП-уравнений, для решения которых применим метод покоординатной линеаризации.

В данной работе делается обобщение класса ВКП-функций на случай, когда полиномы рассматриваются над группой с нормальным рядом. Получающийся при этом класс ВКП-функций над группой даёт конструктивный пример дифференцируемых функций над группой, рассмотренных в [2].

Пусть задана группа $\mathbb{G}$ с нормальным рядом $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \ldots \trianglerighteq H_n = e$. Как и в случае примарного кольца вычетов, для определения класса ВКП-функций над группой необходимо определить понятие координатной функции полинома над группой.

Определение 1. *Полиномом* над группой $\mathbb{G}$ от переменной x будем называть выражение вида $p(x) = g_1 x^{\varepsilon_1} g_2 x^{\varepsilon_2} \dots g_m x^{\varepsilon_m}$, где все «коэффициенты» g_i — элементы группы $\mathbb{G}$, а экспоненты ε_i принимают значения 1 либо -1.

Каждый полином индуцирует функцию на $\mathbb{G}$ по следующему правилу:

$$p(g) = g_1 g^{\varepsilon_1} g_2 g^{\varepsilon_2} \dots g_m g^{\varepsilon_m}.$$

Определение 2. Функцию $p : \mathbb{G} \to \mathbb{G}$ будем называть *полиномиальной*, если она индуцирована некоторым полиномом над $\mathbb{G}$.

Определение 3. Для $k \in \{0, \dots, n-1\}$ будем называть функции $\gamma_k : \mathbb{G} \to H_k$ *координатными функциями группы* $\mathbb{G}$ *относительно нормального ряда*, если произвольный элемент $g \in \mathbb{G}$ однозначно представляется в виде произведения

$$g = \gamma_0(g)\gamma_1(g) \cdots \gamma_{n-1}(g).$$

Элемент $g^{(k)}$ подгруппы H_k, равный $g^{(k)} = \gamma_k(g)$, будем называть k*-й координатой* элемента g. Если задана функция $f : \mathbb{G} \to \mathbb{G}$, то k*-й координатной функцией* функции f будем называть отображение $\gamma_k f : \mathbb{G} \to H_k$, определяемое по правилу $\gamma_k f(g) = \gamma_k(f(g))$.

Координаты элемента группы определяются способом выбора представителей в факторах ряда и могут быть найдены с помощью алгоритма 1.

Алгоритм 1. Нахождение координат элемента группы

Вход: группа $\mathbb{G} = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_n = e$ с нормальным рядом, элемент $g \in \mathbb{G}$, функции выбора представителей в факторах ряда $s_0, \dots, s_{n-2}$ $(s_i : H_i/H_{i+1} \to H_i)$
Выход: набор координат $(\gamma_0(g), \dots, \gamma_{n-1}(g))$, $\gamma_i(g) \in H_i$ и $g = \gamma_0(g) \cdots \gamma_{n-1}(g)$

1: **Для всех** i от 0 до $n-2$
2: $\quad \overline{g} := gH_{i+1}$, $\gamma_i(g) := s_i(\overline{g})$
3: $\quad g := \gamma_i(g)^{-1} g$
4: $\gamma_{n-1}(g) := g$, конец

Определение 4. Функцию $f : \mathbb{G} \to \mathbb{G}$ будем называть ВКП-функцией, если существуют полиномы $p_0, \dots, p_{n-1}$, такие, что для произвольных $g \in \mathbb{G}$, $k \in \{0, \dots, n-1\}$ выполняется

$$\gamma_k f(g) = \gamma_k p_k(g).$$

Как видно из определения, класс ВКП-функций над группой определяется нормальным рядом в группе, способом выбора представителей в факторах ряда и тем, как понимать термин полинома над группой. Например, можно отказаться от требования полиномиальности либо рассматривать иначе определённые (например, так, как в [3]) полиномы. Далее полиномы понимаются в смысле определения 1.

С практической точки зрения наибольший интерес представляют конечные группы. Известно, что конечные нильпотентные группы (интересующие нас, как относительно простые некоммутативные группы) исчерпываются прямыми произведениями конечных p-групп, каждая из которых, в свою очередь, изоморфно вкладывается в $UT_n(\mathbb{Z}_p)$ [4]. Поэтому в качестве основной интерпретации будем рассматривать группу унитреугольных матриц $UT_n(\mathbb{Z}_p)$ с центральным рядом

$$UT_n(\mathbb{Z}_p) = UT_n^1(\mathbb{Z}_p) \trianglerighteq UT_n^2(\mathbb{Z}_p) \trianglerighteq \cdots \trianglerighteq UT_n^n(\mathbb{Z}_p) = e,$$

где $n \geqslant 3$ и $UT_n^i(\mathbb{Z}_p)$ — подгруппа, состоящая из унитреугольных матриц с $i-1$ нулевыми диагоналями над главной.

Очевидно, что класс ВКП-функций над произвольной группой включает в себя класс полиномиальных функций. Обратное включение не выполняется.

Теорема 1. Пусть $\mathbb{G} = UT_n(\mathbb{Z}_p)$ и $n \geqslant 3$. Тогда класс ВКП-функций над $\mathbb{G}$ не совпадает с классом полиномиальных функций.

Следующие теоремы дают критерий биективности ВКП-функции и формулу обращения биективной ВКП-функции над $UT_n(\mathbb{Z}_p)$.

Теорема 2. Пусть $\mathbb{G} = UT_n(\mathbb{Z}_p)$; $f : \mathbb{G} \to \mathbb{G}$ — ВКП-функция, заданная полиномами $p_0, \ldots, p_{n-2}$. Тогда f биективна на $\mathbb{G}$, если и только если выполняются следующие два условия:

1) p_0 биективен по модулю $UT_n^2(\mathbb{Z}_p)$;
2) степени полиномов $p_0, \ldots, p_{n-2}$ взаимно просты с p.

Теорема 3. Пусть $\mathbb{G} = UT_n(\mathbb{Z}_p)$; $f : \mathbb{G} \to \mathbb{G}$ — биективная ВКП-функция, заданная полиномами $p_0, \ldots, p_{n-2}$; $k \in \{2, \ldots, n-1\}$; v_k — обратная в смысле композиции ВКП-функция к f по модулю $UT_n^k(\mathbb{Z}_p)$. Тогда обратной к f по модулю $UT_n^{k+1}(\mathbb{Z}_p)$ является функция

$$v_{k+1}(x) = v_k(x)(x^{-1} f(v_k(x)))^{-m},$$

где $m = \deg(p_{k-1})^{-1} \pmod p$.

Рассмотрим группу $\mathbb{G} = UT_3(\mathbb{Z}_3)$ с функцией $s_0 : UT_3(\mathbb{Z}_3)/UT_3^2(\mathbb{Z}_3) \to UT_3(\mathbb{Z}_3)$, выбирающей в качестве представителя смежного класса матрицу с нулевой верхней клеткой. Тогда, например, $\gamma_0 \left(\begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, $\gamma_1 \left(\begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Построим следующие полиномы:

$$p_0(x) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x^{-1} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} x, \quad p_1(x) = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x.$$

Занумеруем матрицы из $UT_3(\mathbb{Z}_3)$ следующим образом:

$$I \left(\begin{pmatrix} 1 & a_1 & a_3 \\ 0 & 1 & a_2 \\ 0 & 0 & 1 \end{pmatrix} \right) = 1 + a_1 + 3a_2 + 9a_3.$$

Тогда построенные полиномы индуцируют следующие перестановки номеров:

$$p_0 : (1,6,8)(2,22,18)(3,14,25)(4,27,11)(5,16,21)(7,12,23)(9,20,13)(10,15,17)(19,24,26),$$

$$p_1 : (1,5,19,14,10,23)(2,22)(3,15,12,6,21,24)(4,20)(7,17,16,8,25,26)(11,13)(18,27).$$

Построим по p_0 и p_1 ВКП-функцию $f(x) = \gamma_0 p_0(x) \gamma_1 p_1(x)$:

$$f : (1,6,26)(2,22,9)(3,14,16)(4,27,11,13,18,20)(5,25,21,23,7,12)(8,19,15,17,10,24).$$

В качестве обратной к f по модулю $UT_3^2(\mathbb{Z}_3)$ возьмём функцию, индуцированную полиномом $p(x) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} x$. Степень p_1 равна 2, значит, $m = 2$ и обратная перестановка к f получается как $g(x) = p(x)(x^{-1}f(p(x)))^{-2}$:

$$g : (1, 26, 6)(2, 9, 22)(3, 16, 14)(4, 20, 18, 13, 11, 27)(5, 12, 7, 23, 21, 25)(8, 24, 10, 17, 15, 19).$$

Таким образом, при фиксированных нормальном ряде в группе и способе выбора представителей в факторах этого ряда определён класс ВКП-функций над группой. Функции класса задаются набором полиномов и получаются как произведение их координатных функций. Класс ВКП-функций над $UT_n(\mathbb{Z}_p)$ не совпадает с классом полиномиальных функций над $UT_n(\mathbb{Z}_p)$ (теорема 1). К ВКП-функциям применимы критерий биективности и формулы обращения дифференцируемых функций, которые в случае $\mathbb{G} = UT_n(\mathbb{Z}_p)$ принимают вид теорем 2 и 3 соответственно.

ЛИТЕРАТУРА

1. *Заец М. В.* О классе вариационно-координатно-полиномиальных функций над примарным кольцом вычетов // Прикладная дискретная математика. 2014. № 3. С. 12–27.
2. *Карпов А. В.* Обращение дифференцируемых перестановок над группой // Прикладная дискретная математика. Приложение. 2015. № 8. С. 30–33.
3. *Anashin V. S.* Solvable groups with operators and commutative rings having transitive polynomials // Algebra. Logika. 1982. No. 21(6). С. 627–646.
4. *Меньшов А. В.* Асимптотические свойства рациональных множеств и систем уравнений в свободных абелевых группах и разрешимость регулярных уравнений в классе нильпотентных групп: дис. ... канд. физ.-мат. наук. Омск, 2014.

УДК 519.7 DOI 10.17223/2226308X/9/10

О РАССТОЯНИИ ХЭММИНГА МЕЖДУ ДВУМЯ БЕНТ-ФУНКЦИЯМИ[1]

Н. А. Коломеец

Рассматривается расстояние Хэмминга между двумя бент-функциями. С использованием конструкции бент-функций на минимальном расстоянии друг от друга получен ряд возможных значений расстояния. Найдены всевозможные значения расстояния между бент-функциями из класса Мэйорана — МакФарланда.

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

Булевой функцией от n переменных называется отображение вида $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Расстоянием Хэмминга* $\mathrm{dist}(f, g)$ между двумя булевыми функциями f и g от n переменных называется количество значений аргументов, на которых значения функций различаются. Функция вида $\langle a, x\rangle \oplus c$, где $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$ и $\langle a, x\rangle = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$, называется *аффинной* булевой функцией. *Бент-функциями* называются булевы функции от чётного числа переменных, находящиеся на максимально возможном расстоянии от множества всех аффинных функций. Они предложены О. Ротхаусом [1]. Бент-функции имеют приложения в алгебре, комбинаторике, теории кодирования, криптографии [2]. Обозначим через $\mathcal{B}_{2k}$ множество всех бент-функций от $2k$ переменных.

[1]Работа поддержана грантом РФФИ, проект № 15-07-01328.

В данной работе рассматривается расстояние Хэмминга между двумя бент-функциями и носитель их суммы. Исследование возможных носителей связано с гипотезой Н. Н. Токаревой [3] о том, что любую булеву функцию степени не больше k от $2k$ переменных можно представить в виде суммы двух бент-функций из $\mathcal{B}_{2k}$. Следующая лемма даёт общий критерий принадлежности функции на расстоянии $|D|$ от бент-функции f к классу бент-функций.

Лемма 1. Пусть $f \in \mathcal{B}_{2k}$. Тогда $f \oplus \mathrm{Ind}_D \in \mathcal{B}_{2k}$, где $D \subseteq \mathbb{F}_2^{2k}$, тогда и только тогда, когда для всех $y \in \mathbb{F}_2^{2k}$ справедливо

$$\sum_{x \in D} (-1)^{f(x) \oplus \langle x,y \rangle} \in \{0, \pm 2^k\}.$$

Опишем всевозможные значения расстояния между бент-функциями из класса Мэйорана — МакФарланда M_{2k} [4], который содержит функции вида

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

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

Утверждение 1. Расстояние Хэмминга между двумя бент-функциями $f, g \in M_{2k}$ имеет вид $(n+2m)2^{k-1}$, где $0 \leqslant n \leqslant 2^k$, $n \neq 1$ и $0 \leqslant m \leqslant 2^k - n$, причём для любой бент-функции из M_{2k} существует бент-функция на данном расстоянии от неё. Носитель $f \oplus g$ представим в виде объединения аффинных подпространств размерностей $k-1$ и k.

Особый интерес представляют расстояния в $\mathcal{B}_{2k}$ в интервале от минимального возможного до удвоенного минимального, поскольку в [5] получены всевозможные носители суммы с точностью до аффинной эквивалентности. В [6] доказано, что между двумя бент-функциями достижимы расстояния вида $2^{k+1} - 2^t$, где $1 \leqslant t \leqslant k$.

С использованием конструкции бент-функций на минимальном возможном расстоянии 2^k (см., например, [7]) получены следующие расстояния между двумя бент-функциями.

Теорема 1. Для всех d вида $\ell 2^k - 2^t$, где $1 \leqslant t \leqslant k$ и $2 \leqslant \ell \leqslant 2^k - 2^{k-t+1} + 2$, существуют бент-функции $f, g \in \mathcal{B}_{2k}$, такие, что $\mathrm{dist}(f, g) = d$ и $\mathrm{dist}(f \oplus 1, g) = 2^{2k} - d$.

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. *Tokareva N. N.* On the number of bent functions from iterative constructions: lower bounds and hypothesis // Adv. Math. Commun. 2011. V. 5. No. 4. P. 609–621.
4. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.
5. *Kasami T. and Tokura N.* On the weight structure of Reed — Muller codes // IEEE Trans. Inform. Theory. 1970. V. 16. No 6. P. 752–759.
6. *Потапов В. Н.* Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Проблемы передачи информации. 2012. Т. 48. № 1. С. 54–63.
7. *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/9/11

О МНОЖЕСТВЕ РАССТОЯНИЙ ХЭММИНГА МЕЖДУ САМОДУАЛЬНЫМИ БЕНТ-ФУНКЦИЯМИ[1]

А. В. Куценко

Получен полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда со следующим ограничением: перестановка, фигурирующая в данной конструкции, должна быть элементом полной линейной группы соответствующего порядка. На основании этого результата сделан вывод о минимальном расстоянии Хэмминга между рассмотренными функциями.

Ключевые слова: *булева функция, бент-функция, преобразование Уолша — Адамара, самодуальная бент-функция, конструкция Мэйорана — МакФарланда.*

Булевой функцией f называется любое отображение $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. *Скалярным произведением* $\langle x, y\rangle$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_2^n$ называется число $\bigoplus\limits_{i=1}^{n} x_i y_i$, где операция $\oplus$ есть сложение по модулю 2. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{Z}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y\rangle}$. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{Z}_2^n$ [1]. Булева функция $\tilde{f}$ называется *дуальной* к бент-функции f, если $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ для каждого $x \in \mathbb{Z}_2^n$. Бент-функция f называется *самодуальной* (*анти-самодуальной*), если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). *Расстояние Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения, обозначается как $\mathrm{dist}(f, g)$.

Известна следующая конструкция бент-функций: *конструкция Мэйорана — МакФарланда* (1973): пусть π — любая перестановка на $\mathbb{Z}_2^{n/2}$, а h — произвольная булева функция от $n/2$ переменных. Тогда функция $f(x, y) = \langle x, \pi(y)\rangle \oplus h(y)$ является бент-функцией от n переменных [2]. Эта конструкция является достаточно богатой. В работе [3] найдены необходимые и достаточные условия самодуальности бент-функции, построенной с помощью конструкции Мэйорана — МакФарланда, в случае $\pi \in \mathrm{GL}(n/2, \mathbb{Z}_2)$.

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, T. Feulner, L. Sok, A. Wassermann и др.). В частности, в работе [3] перечислены все самодуальные бент-функции от 2, 4, 6 переменных и все квадратичные самодуальные бент-функции от 8 переменных. В [4] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных можно найти в [5].

В данной работе получен полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда со следующим ограничением: перестановка, фигурирующая в конструкции, должна быть элементом полной линейной группы соответствующего порядка.

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

Теорема 1. Пусть f, g — различные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана — МакФарланда при условии, что перестановка, фигурирующая в данной конструкции, является элементом $\mathrm{GL}(n/2, \mathbb{Z}_2)$. Если бент-функции f, g самодуальные, то

$$\mathrm{dist}(f,g) \in \{2^{n-1}, 2^{n-1}(1 \pm 1/2), 2^{n-1}\left(1 \pm 1/2^2\right), \ldots, 2^{n-1}\left(1 \pm 1/2^{n/2-1}\right), 2^n\}.$$

Следствие 1. Пусть f, g — различные самодуальные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана — МакФарланда при условии, что перестановка, фигурирующая в данной конструкции, является элементом $\mathrm{GL}(n/2, \mathbb{Z}_2)$. Тогда

$$\mathrm{dist}(f,g) \geqslant 2^{n-2}.$$

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
3. *Carlet C., Danielson L. E., Parker M. G., and Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
4. *Hou X.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. P. 183–198.
5. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. P. 395–406.

УДК 519.7 DOI 10.17223/2226308X/9/12

УСЛОВИЯ СУЩЕСТВОВАНИЯ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ С МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ[1]

Д. П. Покрасенко

Исследуется максимальная компонентная алгебраическая иммунность и её связь с матрицами специального вида. Получены ограничения на значения n, m, при которых возможно существование векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ с максимальной компонентной алгебраической иммунностью.

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

Важным криптографическим свойством булевых функций является алгебраическая иммунность, она была введена в работе [1]. *Алгебраической иммунностью* $\mathrm{AI}(f)$ булевой функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется минимальное число d, такое, что существует булева функция g степени d, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)g = 0$.

Данное понятие различными способами было обобщено на векторный случай. Одним из наиболее естественных обобщений является понятие компонентной алгебраической иммунности, введённое в [2]. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ называется минимальная алгебраическая иммунность компонентных функций $b \cdot F$ ($b \in \mathbb{Z}_2^m$, $b \neq 0$), т. е. $\mathrm{AI}_{\mathrm{comp}}(F) = \min\{\mathrm{AI}(b \cdot F) : b \in \mathbb{Z}_2^m, b \neq 0\}$, где $b \cdot F = b_1 f_1 \oplus \ldots \oplus b_m f_m$.

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

Для булевых функций от n переменных известно [3], что алгебраическая иммунность всегда меньше или равна $\lceil n/2 \rceil$, более того, существуют функции, имеющие $\mathrm{AI}(f) = \lceil n/2 \rceil$. В случае компонентной алгебраической иммунности векторных булевых функций также получено [2], что $\mathrm{AI}_{\mathrm{comp}}(F) \leqslant \lceil n/2 \rceil$. Данная работа посвящена изучению условий существования векторных булевых функций с максимальной компонентной алгебраической иммунностью равной $\lceil n/2 \rceil$.

Для каждой векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ 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 все мономы степени меньше $\lceil n/2 \rceil$, за исключением тождественно равного нулю монома. Матрица M'_F строится аналогично, только вместо $b \cdot F$ подставляется $b \cdot F \oplus 1$. Сопоставим вектор $a = (a_1, \ldots, a_n) \in \mathbb{Z}_2^n$ моному от n переменных, где $a_i = 1$ соответствует наличию в мономе переменной x_i. Нумерация столбцов идёт по вектору $b \in \mathbb{Z}_2^m$, $b \neq 0$; строки занумерованы векторами $a = (a_1, \ldots, a_n)$:

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

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

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

В работе [4] установлено, что векторная булева функция 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. В продолжение данной работы получено утверждение, поясняющее структуру матриц.

Введём новую матрицу M, которая строится из матрицы M_F приписыванием справа от неё матрицы M'_F. Таким образом получаем матрицу, у которой элементы — булевы функции, количество строк такое же, как у матриц M_F и M'_F, а количество столбцов увеличивается в 2 раза.

Утверждение 1. Если векторная булева функция $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ имеет максимальную компонентную алгебраическую иммунность $\mathrm{AI}_{\mathrm{comp}}(F) = \lceil n/2 \rceil$, то в любой строке матрицы M все элементы попарно различны.

При изучении максимальной компонентной иммунности возникает вопрос о существовании ограничений на значения n, m, а также на их связь друг с другом. Получено следующее соотношение.

Утверждение 2. Векторная булева функция $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ может иметь максимальную компонентную алгебраическую иммунность $\mathrm{AI}_{\mathrm{comp}}(F) = \lceil n/2 \rceil$ только для

таких n, m, для которых выполняется следующее условие:

$$m \leqslant 2^{\lceil (n+1)/2 \rceil} - 1.$$

ЛИТЕРАТУРА

1. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt 2004. LNCS. 2004. V. 3027. P. 474–491.
2. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, 2009. P. 104–116.
3. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt 2003. LNCS. 2003. V. 2656. P. 345–359.
4. *Pokrasenko D.* On the maximal component algebraic immunity of vectorial Boolean functions // J. Appl. Industr. Math. 2016. V. 10. P. 257–263.

УДК 512.13 DOI 10.17223/2226308X/9/13

ПРЕДСТАВЛЕНИЕ ПОЛУБАЙТОВЫХ ПОДСТАНОВОК АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ МАГМА И 2-ГОСТ АЛГЕБРАИЧЕСКИМИ ПОРОГОВЫМИ ФУНКЦИЯМИ

Д. А. Сошин

Работа посвящена реализации полубайтовых подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ алгебраическими пороговыми функциями (АПФ). Для каждой из подстановок алгоритмов Магма рассмотрен вопрос принадлежности линейных комбинаций координатных функций к классу АПФ. Для подстановок 2-ГОСТ предложено их задание через линейные комбинации АПФ.

Ключевые слова: *алгебраические пороговые функции, подстановки.*

В работе [1] вводится новый класс функций, который назван классом алгебраических пороговых функций.

Определение 1. Функция k-значной логики $f_n^k : \Omega_k^n \to \Omega_k$ называется *алгебраической пороговой*, если существуют целочисленные наборы $(c_0, c_1, \ldots, c_n)$, $(b_0, b_1, \ldots, b_k)$ и модуль m, такие, что для любого $\alpha \in \{0, \ldots, k-1\}$ выполняется

$$f_n^k(x_1,\ x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant r_m(c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n) < b_{\alpha+1},$$

где $r_m(y)$ — *функция взятия остатка* при делении целого числа y на модуль m ($r_m(y) \in \{0, 1, \ldots, m-1\}$); $\Omega_k = \{0, 1, \ldots, k-1\}$; $\Omega_k^n = \underbrace{\Omega_k \times \Omega_k \times \cdots \times \Omega_k}_{n}$.

Тройку $((c_0, c_1, \ldots, c_n); (b_0, b_1, \ldots, b_k); m\ )$ назовём *структурой алгебраической пороговой функции* f_n^k.

В [1] проведено исследование вопроса реализации булевых функций трёх переменных функциями из класса АПФ. Для этого доказана замкнутость данного класса относительно операций перестановки переменных, инвертирования переменных в смысле Лукашевича и инвертирования функции (геометрическая замкнутость). Геометрическим типом функции f назовём класс эквивалентности относительно указанных преобразований. Для булевых функций от трёх переменных доказано, что только геометрический тип с представителем $f(x_1, x_2, x_3) = x_1x_3 \vee x_2\overline{x_3}$ не задаётся через АПФ.

Для булевых функций от четырёх переменных существует ровно 222 геометрических типа, и из них 70 представителей содержат в качестве подфункции функцию от трёх переменных, не имеющую представление в виде АПФ, и поэтому не относятся к классу АПФ. Для 99 из оставшихся 152 геометрических типов найдено задание в виде АПФ. Важно отметить, что класс АПФ замкнут относительно фиксации переменных и включает в себя все линейные функции k-значной логики.

В стандарте ГОСТ Р 34.12-2015 [2] в качестве нелинейного биективного преобразования выступает набор подстановок π'_i, $i = 0, \ldots, 7$. Обозначим через $f_3^{(i)}, f_2^{(i)}, f_1^{(i)}, f_0^{(i)}$ координатные функции подстановки π'_i от старших разрядов к младшим соответственно. У каждой подстановки рассмотрены линейные комбинации координатных функций, и те, для которых нашлось АПФ-представление, приведены в табл. 1 со своими структурами.

Таблица 1

Представление линейных комбинаций координатных функций подстановок ГОСТ Р 34.12-2015 через АПФ

π'_i	Лин. комбинации	Структура АПФ	π'_i	Лин. комбинации	Структура АПФ
π'_1	$f_3^{(1)}$	$((0,3,1,3,0);(0,2,4);\ 4)$	π'_4	$f_3^{(4)}$	$((0,2,1,3,0);(0,2,4);\ 4)$
	$f_3^{(1)} \oplus f_2^{(1)} \oplus f_0^{(1)}$	$((7,5,1,3,6);(0,4,8);\ 8)$		$f_3^{(4)} \oplus f_2^{(4)} \oplus f_1^{(4)}$	$((0,5,5,6,2);(0,4,8);\ 8)$
	$f_3^{(1)} \oplus f_2^{(1)}$	$((6,1,3,6,3);(0,4,8);\ 8)$		$f_3^{(4)} \oplus f_2^{(4)} \oplus f_0^{(4)}$	$((0,6,1,6,3);(0,4,8);\ 8)$
	$f_2^{(1)} \oplus f_0^{(1)}$	$((6,3,3,1,6);(0,4,8);\ 8)$	π'_5	$f_2^{(5)} \oplus f_0^{(5)}$	$((0,3,2,5,7);(0,4,8);\ 8)$
π'_2	$f_2^{(2)}$	$((0,3,7,2,5);(0,4,8);\ 8)$		$f_2^{(5)} \oplus f_1^{(5)}$	$((6,7,5,2,6);(0,4,8);\ 8)$
	$f_1^{(2)} \oplus f_0^{(2)}$	$((1,2,5,6,3);(0,4,8);\ 8)$		$f_3^{(5)} \oplus f_2^{(5)}$	$((5,5,5,7,2);(0,4,8);\ 8)$
	$f_3^{(2)} \oplus f_2^{(2)}$	$((7,2,5,2,1);(0,4,8);\ 8)$		$f_3^{(5)} \oplus f_2^{(5)} \oplus f_0^{(5)}$	$((0,7,5,3,2);(0,4,8);\ 8)$
π'_3	$f_3^{(3)} \oplus f_0^{(3)}$	$((6,7,2,3,6);(0,4,8);\ 8)$	π'_6	$f_3^{(6)} \oplus f_1^{(6)}$	$((7,2,7,5,2);(0,4,8);\ 8)$
	$f_3^{(3)} \oplus f_2^{(3)} \oplus f_0^{(3)}$	$((3,2,7,2,5);(0,4,8);\ 8)$		$f_3^{(6)} \oplus f_2^{(6)} \oplus f_1^{(6)}$	$((6,1,6,5,6);(0,4,8);\ 8)$
π'_7	$f_0^{(7)}$	$((4,3,7,6,5);(0,4,8);\ 8)$			

Из табл. 1 видно, что функции $f_3^{(1)}$, $f_2^{(2)}$, $f_3^{(4)}$, $f_0^{(7)}$ являются алгебраическими пороговыми и имеют следующие задания:

$$f_3^{(1)} = 1 \quad \Leftrightarrow \quad r_4\left(3x_1 + 1x_2 + 3x_3\right) \geqslant 2, \quad f_2^{(2)} = 1 \quad \Leftrightarrow \quad r_8\left(3x_1 + 7x_2 + 2x_3 + 5x_4\right) \geqslant 4,$$
$$f_3^{(4)} = 1 \quad \Leftrightarrow \quad r_4\left(2x_1 + 1x_2 + 3x_3\right) \geqslant 2, \quad f_0^{(7)} = 1 \quad \Leftrightarrow \quad r_8\left(4 + 3x_1 + 7x_2 + 6x_3 + 5x_4\right) \geqslant 4.$$

Важно отметить, что функции $f_3^{(1)}$ и $f_3^{(4)}$ фиктивно зависят от переменной x_4 (x_4 — старший бит входного числа). Последнее влечёт ухудшение перемешивающих свойств нелинейного слоя.

Подстановка π'_5 представляется в виде каскадного соединения АПФ

$$\pi'_5 = \begin{pmatrix} f_3^{(5)} \\ f_2^{(5)} \\ f_1^{(5)} \\ f_0^{(5)} \end{pmatrix} = \begin{pmatrix} \varphi^{(0)} \oplus \varphi^{(3)} \\ \varphi^{(0)} \oplus \varphi^{(2)} \oplus \varphi^{(3)} \\ \varphi^{(0)} \oplus \varphi^{(1)} \oplus \varphi^{(2)} \oplus \varphi^{(3)} \\ \varphi^{(2)} \oplus \varphi^{(3)} \end{pmatrix}.$$

Функции $\varphi^{(0)}, \varphi^{(1)}, \varphi^{(2)}, \varphi^{(3)}$ задают соответствующие линейные комбинации $f_2^{(5)} \oplus$ $\oplus f_0^{(5)}$, $f_2^{(5)} \oplus f_1^{(5)}$, $f_3^{(5)} \oplus f_2^{(5)}$, $f_3^{(5)} \oplus f_2^{(5)} \oplus f_0^{(5)}$ из табл. 1 следующим образом:

$$\varphi^{(0)} = 1 \Leftrightarrow r_8(3x_1 + 2x_2 + 5x_3 + 7x_4) \geqslant 4, \quad \varphi^{(1)} = 1 \Leftrightarrow r_8(6 + 7x_1 + 5x_2 + 2x_3 + 6x_4) \geqslant 4,$$
$$\varphi^{(2)} = 1 \Leftrightarrow r_8(5 + 5x_1 + 5x_2 + 7x_3 + 2x_4) \geqslant 4, \quad \varphi^{(3)} = 1 \Leftrightarrow r_8(7x_1 + 5x_2 + 3x_3 + 2x_4) \geqslant 4.$$

В [3] предложен алгоритм блочного шифрования 2-ГОСТ, являющийся модификацией шифрсистемы ГОСТ 28147-89, отличающийся от последней лишь алгоритмом развертывания ключа, а также тем, что набор S-боксов фиксирован: $\pi_0 = \pi_1 = \pi_2 = \pi_3 = \pi'$, $\pi_4 = \pi_5 = \pi_6 = \pi_7 = \pi''$, где π' и π'' заданы нижними строками подстановок (табл. 2).

Таблица 2

Задание подстановок 2-ГОСТ

i	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$\pi'(i)$	6	A	F	4	3	8	5	0	D	E	7	1	2	B	C	9
$\pi''(i)$	E	0	8	1	7	A	5	6	D	2	4	9	3	F	C	B

В результате анализа подстановок π' и π'' каждую из них удалось задать через линейные комбинации пяти АПФ

$$\pi' = \begin{pmatrix} f'_3 \\ f'_2 \\ f'_1 \\ f'_0 \end{pmatrix} = \begin{pmatrix} g_1 \oplus g_2 \\ g_3 \oplus g_4 \\ g_3 \\ g_5 \end{pmatrix}, \qquad \pi'' = \begin{pmatrix} f''_3 \\ f''_2 \\ f''_1 \\ f''_0 \end{pmatrix} = \begin{pmatrix} v_1 \oplus v_2 \\ v_1 \oplus v_3 \\ v_1 \oplus v_4 \\ v_4 \oplus v_5 \end{pmatrix},$$

где функции $g_1, g_2, g_3, g_4, g_5, v_1, v_2, v_3, v_4, v_5$ — алгебраические пороговые:

$$\begin{aligned}
g_1 &= 1 \Leftrightarrow r_9\,(x_1 + 5x_2 + 2x_3 + 2x_4) \geqslant 6, & v_1 &= 1 \Leftrightarrow r_8\,(6 + 5x_1 + 5x_2 + 2x_3 + x_4) \geqslant 6,\\
g_2 &= 1 \Leftrightarrow r_7\,(5x_1 + 5x_2 + x_3 + 6x_4) \geqslant 2, & v_2 &= 1 \Leftrightarrow r_8\,(3 + 2x_1 + 4x_2 + x_3 + 5x_4) \geqslant 6,\\
g_3 &= 1 \Leftrightarrow r_8\,(7 + 6x_1 + 5x_2 + 6x_3 + x_4) \geqslant 4, & v_3 &= 1 \Leftrightarrow r_7\,(3 + x_1 + 6x_2 + 3x_3 + 4x_4) \geqslant 5,\\
g_4 &= 1 \Leftrightarrow r_8\,(2 + 5x_1 + 7x_2 + 3x_3 + 2x_4) \geqslant 4, & v_4 &= 1 \Leftrightarrow r_8\,(2 + x_1 + 6x_2 + 3x_3 + 2x_4) \geqslant 4,\\
g_5 &= 1 \Leftrightarrow r_8\,(3 + 5x_1 + x_2 + 2x_3 + 3x_4) \geqslant 4, & v_5 &= 1 \Leftrightarrow r_8\,(3x_1 + 2x_2 + 2x_3 + x_4) \geqslant 4.
\end{aligned}$$

Здесь x_1 — младший бит входного числа, x_4 — старший.

Класс АПФ сохраняет простоту реализации функций, основная сложность которой сводится к подсчёту скалярного произведения, как и для пороговых функций.

ЛИТЕРАТУРА

1. *Сошин Д. А.* Представление геометрических типов булевых функций от трех переменных алгебраическими пороговыми функциями // Прикладная дискретная математика. 2016. № 1(31). С. 32–45.
2. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
3. *Дмух А. А., Дыгин Д. М., Маршалко Г. Б.* Пригодная для низкоресурсной реализации модификация блочного шифра ГОСТ // Матем. вопр. криптограф. 2014. Т. 5. № 2. С. 47–55.

УДК 519.7 DOI 10.17223/2226308X/9/14

О МНОЖЕСТВЕ ПРОИЗВОДНЫХ БУЛЕВОЙ БЕНТ-ФУНКЦИИ[1]

Н. Н. Токарева

Верно ли, что любая уравновешенная булева функция от n переменных степени меньше $n/2$ является производной некоторой бент-функции от n переменных? В работе исследуется этот вопрос при малом числе переменных.

Ключевые слова: *бент-функции, производная, аффинная классификация.*

В работе продолжено исследование множества булевых бент-функций. Известно, что бент-функции [1] интересны для криптографических приложений [2]; актуальными в данной области остаются вопросы о числе бент-функций и способах их построения.

«Много» или «мало» бент-функций? Этим вопросом озадачиваются многие исследователи. Если исходить из предположения, что бент-функций много и они разнообразны, то разнообразными должны быть и их производные. Так ли это на самом деле? При малом числе переменных мы исследуем этот вопрос.

Производной булевой функции f от n переменных по направлению $y \in \mathbb{F}_2^n$ называется функция $D_y f(x) = f(x) + f(x+y)$. Напомним, что булева функция f от чётного числа переменных n называется *бент-функцией*, если её производная по любому ненулевому направлению y уравновешена, т. е. $D_y f$ одинаково часто принимает значения 0 и 1. Хорошо известно, что степень бент-функции не превосходит $n/2$.

Заметим, что булева функция g является производной некоторой булевой функции f тогда и только тогда, когда найдётся ненулевой вектор y, такой, что $g(x) + g(x+y) = 0$ для всех x. Напомним также, что если функция f отлична от константы, то степень её производной по любому ненулевому направлению меньше степени f.

Несложно доказать, что свойство быть производной некоторой бент-функции сохраняется при аффинном преобразовании, а именно: если булева функция g — производная некоторой бент-функции, то функция $g(Ax + b) + \lambda$ также обладает этим свойством, где A — невырожденная $n \times n$-матрица, b — произвольный вектор, λ — константа из $\mathbb{F}_2$.

В работе исследуется следующая гипотеза: *любая уравновешенная булева функция g от n переменных степени не выше $n/2 - 1$, такая, что $g(x) = g(x + y)$ для всех x при некотором y, является производной некоторой бент-функции от n переменных.*

На основе аффинной классификации булевых функций от малого числа переменных проверено, что при $n = 4, 6$ и в ряде случаев при $n = 8$ гипотеза верна; проверка продолжается.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015. 220 p.

[1]Работа поддержана грантом РФФИ, проект № 15-07-01328.

УДК 519.719.325 DOI 10.17223/2226308X/9/15

О РАСПРЕДЕЛЕНИИ РАНГА И ОЦЕНКЕ УРОВНЯ АФФИННОСТИ КВАДРАТИЧНЫХ ФОРМ

А. В. Черемушкин

Уровень аффинности двоичной функции определяется как минимальное число переменных, произвольная фиксация значений которых делает функцию аффинной. Обобщённый уровень аффинности определяется как минимальное число фиксаций линейных комбинаций переменных, некоторая фиксация значений которых делает функцию аффинной. Для квадратичной формы ранга $2r$ обобщённый уровень аффинности совпадает с r. Приводятся свойства распределения ранга случайной квадратичной формы и, как следствие, получается асимптотическая оценка обобщённого уровня аффинности квадратичных форм.

Ключевые слова: *двоичные функции, квадратичные формы, уровень аффинности.*

1. Распределение ранга квадратичных форм

Под квадратичной формой здесь понимается двоичная функция, степень нелинейности которой не превосходит двух. Каждую квадратичную форму от n переменных ранга $2r$, $1 \leqslant r \leqslant \lfloor n/2 \rfloor$, можно линейным преобразованием аргументов привести к виду

$$x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2r-1}x_{2r} \oplus l(x_1, \ldots, x_n),$$

где l — некоторая аффинная функция. Так как вид линейной функции l не влияет на значение ранга, то вероятность того, что квадратичная форма от n переменных имеет ранг $2r$, определяемую как относительную долю таких форм, можно записать в виде $p_{2r}(n) = Q_r(n)/2^{n(n-1)/2}$, где $Q_r(n)$ — число квадратичных форм от n переменных ранга $2r$. Из описания групп автоморфизмов квадратичных форм [1–3] следует, что

$$Q_r(n) = \frac{(2^n - 1)\ldots(2^n - 2^{2r-1})}{|\mathbf{Sp}(2r, 2)|},$$

где $\mathbf{Sp}(2r, 2)$ — симплектическая группа, имеющая прядок $|\mathbf{Sp}(2r, 2)| = 2^{r^2} \prod\limits_{i=1}^{r}(2^{2i} - 1)$.

При $1 \leqslant r \leqslant n/2 - 1$ справедливо соотношение

$$\frac{Q_r(n)}{Q_{r+1}(n)} = \frac{4}{(2^{n-2r} - 1)(2^{n-2r-1} - 1)} \left(1 - \frac{1}{2^{2r+2}}\right).$$

Поэтому числа $Q_r(n)$, $1 \leqslant r \leqslant n/2$, образуют монотонно возрастающую последовательность.

Оценим вероятность максимальности ранга.

При $n = 2k$ имеем

$$p_{2k}(2k) = \left(1 - \frac{1}{2^{2k-1}}\right)\left(1 - \frac{1}{2^{2k-3}}\right)\ldots\left(1 - \frac{1}{2}\right). \tag{1}$$

Аналогично при $n = 2k + 1$ имеем

$$p_{2k}(2k+1) = \left(1 - \frac{1}{2^{2k+1}}\right)\left(1 - \frac{1}{2^{2k-1}}\right)\ldots\left(1 - \frac{1}{2^3}\right).$$

В частности, $p_{2k-2}(2k-1) = 2p_{2k}(2k)$ при $k \geqslant 2$.

Верхнюю оценку вероятности $p_{2k}(2k)$ с наперёд заданной точностью можно получить путём перемножения только части сомножителей в произведении (1):

$$p_{2k}(2k) = \prod_{i=1}^{k}\left(1 - \frac{1}{2^{2i-1}}\right) < \prod_{i=1}^{14}\left(1 - \frac{1}{2^{2i-1}}\right) < 0{,}4194224428.$$

Нижнюю оценку вероятности $p_{2k}(2k)$ можно получить, используя подход из работы [4]:

$$\ln p_{2k}(2k) = \sum_{i=1}^{k}\ln\left(1 - \frac{1}{2^{2i-1}}\right) = -\sum_{i=1}^{k}\sum_{m=1}\frac{1}{m}\left(\frac{1}{2^{2i-1}}\right)^m =$$
$$= -\sum_{m=1}\frac{2^m}{m}\sum_{i=1}^{k}\left(\frac{1}{2^{2m}}\right)^i = -\sum_{m=1}\frac{2^{-m}}{m}\frac{1 - 1/(2^{2m})^k}{1 - 1/2^{2m}}.$$

При $k > s$ можно воспользоваться приближённой формулой

$$\ln p_{2k}(2k) > -\frac{2^{2m}}{2^{2m}-1}\ln 2 - \sum_{m=1}^{s-1}\frac{2^{-m}}{m}\left(\frac{1}{2^{2m}-1} - \frac{1}{2^{2r}-1}\right).$$

В частности, полагая $s = 8$, получаем, что при $k > 8$ имеет место нижняя оценка $p_{2k}(2k) > 0{,}41942244$. Поэтому при больших чётных $n = 2k$

$$0{,}4194224428 > p_{2k}(2k) > 0{,}41942244.$$

При больших нечетных $n = 2k+1$ получаем

$$0{,}8388448856 > p_{2k}(2k+1) = 2p_{2k+2}(2k+2) > 0{,}83884488.$$

Теорема 1. Пусть $k = [n/2]$, $n = 2k + \varepsilon$ и $0 \leqslant c \leqslant 1$. При $n \to \infty$ доля квадратичных форм от n переменных ранга меньшего, чем $2k - 2\left\lceil\sqrt{(\log_2 k)/2} + (c + (-1)^{\varepsilon})/2\right\rceil$, стремится к нулю. Поэтому для ранга почти всех квадратичных форм q от n переменных при $n \to \infty$ справедлива нижняя оценка:

$$r(q) \geqslant 2k - 2\left\lceil\sqrt{\frac{1}{2}\log_2 k} + \frac{c + (-1)^{\varepsilon}}{2}\right\rceil + 2.$$

Для математического ожидания ранга случайной квадратичной формы от n переменных можно привести следующую оценку.

Теорема 2. Пусть $k = [n/2]$. При $n \to \infty$ математическое ожидание ранга случайной квадратичной формы q от n переменных оценивается следующим образом:

1) при $n = 2k$ имеем

$$2k - 0{,}60196883564 < \mathrm{E}\, r(q) < 2k - 0{,}6019688356\,(1 - 1/2^n)\,;$$

2) при $n = 2k+1$ имеем

$$2k - 0{,}1625309417 < \mathrm{E}\, r(q) < 2k - 0{,}1625309415\,(1 - 1/2^n)\,.$$

2. Оценка уровня аффинности квадратичной формы

Уровень аффинности $\mathrm{la}(f)$ двоичной функции f определяется как минимальное число переменных, произвольная фиксация значений которых делает функцию аффинной. Обобщённый уровень аффинности $\mathcal{L}a(f)$ двоичной функции f определяется как минимальное число линейных комбинаций переменных, некоторая фиксация значений которых делает функцию аффинной. Эти параметры связаны неравенством [5] $\mathcal{L}a(f) \leqslant \mathrm{la}(f)$. Квадратичную форму от n переменных ранга $2r$ можно линейным преобразованием аргументов привести к виду

$$q(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2r-1}x_{2r} \oplus l(x_1, \ldots, x_n),$$

где $l(x_1, \ldots, x_n)$ — некоторая аффинная функция.

Поскольку обобщенный уровень аффинности квадратичной формы ранга $2r$ равен r, то из приведённых выше асимптотических оценок ранга вытекает

Следствие 1. Пусть $0 \leqslant c \leqslant 1$. При $n \to \infty$, $n = 2k + \varepsilon$, $0 \leqslant \varepsilon \leqslant 1$, доля квадратичных форм от n переменных, имеющих обобщённый уровень аффинности меньший, чем $k - \left\lceil \sqrt{(\log_2 k)/2} + (c + (-1)^{\varepsilon})/2 \right\rceil$, стремится к нулю. Для обобщённого уровня аффинности почти всех квадратичных форм от n переменных при $n \to \infty$ справедлива нижняя оценка:

$$\mathrm{la}(f) \geqslant \mathcal{L}a(f) \geqslant k - \left\lceil \sqrt{\frac{1}{2}\log_2 k} + \frac{c + (-1)^{\varepsilon}}{2} \right\rceil + 1.$$

Отсюда следует, что оценки уровня аффинности почти всех квадратичных форм из работы [5] не являются точными.

Следствие 2. Пусть $k = [n/2]$. При $n \to \infty$ математическое ожидание обобщённого уровня аффинности $\mathcal{L}a(q)$ случайной квадратичной формы q от n переменных оценивается следующим образом:

1) при чётных n

$$k - 0{,}30098441782 < \mathrm{E}\,\mathcal{L}a(q) < k - 0{,}3009844178\,(1 - 1/2^n)\,;$$

2) при нечётных n

$$k - 0{,}8126547085 < \mathrm{E}\,\mathcal{L}a(q) < k - 0{,}8126547075\,(1 - 1/2^n)\,.$$

ЛИТЕРАТУРА

1. *Dixon L. E.* Linear Groups with an Expositions to the Galois Field Theory. Leipzig: Publ. by B. G. Teubner, 1901.
2. *Дьедонне Ж.* Геометрия классических групп. М.: Мир, 1974.
3. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979.
4. *Рязанов Б. В., Чечета С. И.* О приближении булевой функции множеством случайных квадратичных форм // Дискретная математика. 1995. Т. 7. Вып. 3. С. 129–145.
5. *Буряков М. Л.* Асимптотические оценки уровня аффинности для почти всех булевых функций // Дискретная математика. 2008. Т. 20. Вып. 3. С. 73–79.

УДК 519.7 DOI 10.17223/2226308X/9/16

ФУНКЦИИ НА РАССТОЯНИИ ОДИН ОТ APN-ФУНКЦИЙ ОТ МАЛОГО ЧИСЛА ПЕРЕМЕННЫХ[1]

Г. И. Шушуев

Исследуется вопрос существования APN-функций на расстоянии один друг от друга. Доказано, что гипотеза о том, что таких APN-функций нет, выполнена для большинства известных APN-функций от не более чем восьми переменных.

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

В работе рассматриваются векторные булевы функции $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Каждая такая векторная булева функция единственным образом представляется в виде АНФ:

$$F(x) = \sum_{I \in \mathcal{P}(N)} (\prod_{i \in I} x_i) = \sum_{I \in \mathcal{P}(N)} a_I x^I,$$

где $\mathcal{P}(N)$ — множество всех подмножеств множества $N = \{1, \ldots, n\}$; a_I из $\mathbb{F}_2^n$. *Алгебраической степенью* функции F называется величина равная $\max\{|I| : a_I \neq (0, \ldots, 0), I \in \in \mathcal{P}(N)\}$. Функции с алгебраической степенью, не превосходящей 1, называются *аффинными*. Функция называется *дифференциально δ-равномерной* [1], 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 δ решений, где δ — целое положительное число. *Порядком* дифференциальной равномерности функции F называется минимальное возможное δ, такое, что F — дифференциально δ-равномерная функция. *Расстоянием* между векторными булевыми функциями F и G называется мощность множества $\{x \in \mathbb{Z}_2^n : F(x) \neq G(x)\}$.

Векторные булевы функции также известны как S-блоки — примитивные элементы шифров. Чем меньше порядок дифференциальной равномерности S-блока, тем выше стойкость шифра, в котором он используется, к дифференциальному криптоанализу [2]. Минимальный возможный порядок равен двум. Функция с порядком дифференциальной равномерности 2 называется APN-функцией (*Almost Perfect Nonlinear*).

В работе [3] поднимается вопрос существования APN-функции на расстоянии один от произвольной APN-функции и доказано, что для тех APN-функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, для которых выполнено

$$\forall x' \in \mathbb{F}_2^n \left(\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} (B_a(F) \oplus F(x' \oplus a)) = \mathbb{F}_2^n \right), \tag{1}$$

все функции на расстоянии один являются дифференциально равномерными порядка 4; таким образом, на расстоянии один от них нет APN-функций. В работе [3] выдвигается также гипотеза о том, что все APN-функции удовлетворяют этому условию.

Данный вопрос тесно связан с вопросом существования APN-функций максимальной алгебраической степени, а именно, если найдутся две APN-функции на расстоянии один, то одна из них обладает максимальной алгебраической степенью. В [4] доказано, что для большинства известных APN-функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ функция $x^{2^n-1} + F(x)$ алгебраической степени n не является APN-функцией.

[1]Работа поддержана грантом РФФИ, проект № 15-07-01328.

В данной работе исследуется вопрос: удовлетворяют ли APN-функции от малого числа переменных условию (1). Функции F и G из $\mathbb{F}_2^n$ в $\mathbb{F}_2^n$ называются *EA-эквивалентными*, если G представима в виде $G = A_1 \circ F \circ A_2 \oplus A$, где A, A_1 и A_2 — аффинные отображения из F_2^n в F_2^n; A_1 и A_2 являются перестановками.

Утверждение 1. Если векторные булевы функции F и G EA-эквивалентны и условие (1) выполнено для F, то оно выполнено и для G.

Прямым следствием данного утверждения является то, что если какая-то функция из класса EA-эквивалентности удовлетворяет условию (1), то все функции из этого класса также удовлетворяют этому условию. Таким образом, достаточно проверять только одного представителя класса EA-эквивалентности.

В [5] приведены представители классов EA-эквивалентности векторных булевых функций, которые покрывают все APN-функции от не более чем пяти переменных (10 классов) и все квадратичные APN-функции от шести переменных (13 классов). В [6] приведён список всех известных представителей классов EA-эквивалентности APN-функций от семи (490 классов) и восьми переменных (8180 классов). В данной работе с помощью компьютерных вычислений были проверены представители этих классов и установлено, что они удовлетворяют условию (1).

Утверждение 2. Условию (1) удовлетворяют все APN-функции от не более чем пяти переменных, все квадратичные APN-функции от шести переменных и все известные APN-функции от семи и восьми переменных.

Таким образом, на расстоянии один от любой такой APN-функции все функции являются дифференциально равномерными порядка 4, т. е. на расстоянии один от таких APN-функций нет других APN-функций.

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. *Шушуев Г. И.* Векторные булевы функции на расстоянии один от APN-функций // Прикладная дискретная математика. Приложение. 2014. № 7. С. 36–37.
4. *Budagyan L., Carlet C., Helleseth T., and Li N.* On the (non-)existence of APN (n,n)-functions of algebraic degree n. `ia.cr/2016/143`.
5. *Brinkmann M. and Leander G.* On the classification of APN functions up to dimension five // Des. Codes Cryptogr. 2008. V. 49. P. 273–288.
6. *Yu Y., Wang M., and Li Y.* A matrix approach for constructing quadratic APN functions // Des. Codes Cryptogr. 2014. V. 73. P. 587–600.

Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7 DOI 10.17223/2226308X/9/17

К КРИПТОАНАЛИЗУ ДВУХКАСКАДНЫХ КОНЕЧНО-АВТОМАТНЫХ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

Г. П. Агибалов, И. А. Панкратова

Сообщается о конечно-автоматном обобщении регистрового генератора (δ,τ)-шагов и об атаках на него с угрозой раскрытия начальных состояний и функций выходов автоматов и со сложностью, много меньшей сложности атаки грубой силы.

Ключевые слова: *конечный автомат, криптографический генератор, генератор (δ,τ)-шагов, криптоанализ, линеаризационная атака.*

Рассматриваемый здесь криптографический генератор (будем обозначать его G) представляет собой последовательное соединение двух абстрактных конечных автоматов над полем $\mathbb{F}_2$ — управляющего и управляемого. Первый является некоторым автономным автоматом $A_1 = (\mathbb{F}_2^n, \mathbb{F}_2, g_1, f_1)$ с множеством состояний $\mathbb{F}_2^n$, $n > 1$, выходным алфавитом $\mathbb{F}_2$, с функцией переходов $g_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ и функцией выходов $f_1 : \mathbb{F}_2^n \to \mathbb{F}_2$, а второй — некоторым неавтономным автоматом $A_2 = (\mathbb{F}_2, \mathbb{F}_2^m, \mathbb{F}_2, g_2, f_2)$ с входным и выходным алфавитами $\mathbb{F}_2$, с множеством состояний $\mathbb{F}_2^m$, $m > 1$, с функцией выходов $f_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2$ и функцией переходов $g_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2^m$, для которой существуют отображение $g : \mathbb{F}_2^m \to \mathbb{F}_2^m$ и различные целые неотрицательные числа δ и τ, такие, что для всех $u \in \mathbb{F}_2$ и $y \in \mathbb{F}_2^m$ если $u = 0$, то $g_2(u, y) = g^\delta(y)$, и если $u = 1$, то $g_2(u, y) = g^\tau(y)$, т. е. $g_2(u, y) = \neg u g^\delta(y) + u g^\tau(y)$, где, как обычно, $g^0(y) = y$ и $g^r(y) = g(g^{r-1}(y))$. Таким образом, генератор G — это конечный автономный автомат $G = A_1 \cdot A_2 = (\mathbb{F}_2^n \times \mathbb{F}_2^m, \mathbb{F}_2, h, f)$, где $h : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n \times \mathbb{F}_2^m$ и $h(x, y) = (g_1(x), g_2(f_1(x), y))$, $f(x, y) = f_2(f_1(x), y)$, $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_2^m$. Все функции в определении G, как видим, булевы, причём функции g_1 и g_2, g — векторные размерности n и m соответственно.

Генератор G функционирует в дискретном времени $t = 1, 2, \ldots$, в каждый момент t которого его автомат A_1, находясь в состоянии $x(t) = x_1(t)x_2(t)\ldots x_n(t) \in \mathbb{F}_2^n$, выдаёт выходной управляющий символ $u(t) = f_1(x(t))$ и переходит в следующее состояние $x(t + 1) = g_1(x(t))$, а автомат A_2 в этот момент, находясь в состоянии $y(t) = y_1(t)y_2(t)\ldots y_m(t) \in \mathbb{F}_2^m$, принимает от A_1 символ $u(t)$, выдаёт свой выходной символ $v(t) = f_2(u(t), y(t))$ и переходит в следующее состояние $y(t+1) = g_2(u(t), y(t))$. Значением $z(t)$ на выходе генератора G в момент t является значение $v(t)$ на выходе автомата A_2 в этот момент.

Предполагается, что значение любой функции в генераторе G на любом наборе значений её аргументов вычисляется за полиномиальное время от числа последних.

Можно показать, что в частном случае, когда функции g_1 и g являются функциями переходов некоторых регистров сдвига с линейной обратной связью и длиной n и m соответственно и $f_2(u, y_1, y_2, \ldots, y_m) = y_1$, генератор G функционально эквивалентен генератору (δ,τ)-шагов [1].

Функционирование генератора G во времени описывается формально следующей системой векторных булевых уравнений с переменными $x(t), y(t), u(t)$, $t = 1, 2, \ldots$:

$$\begin{cases} u(t) = f_1(x(t)), \\ x(t+1) = g_1(x(t)), \\ x(1) = x_1(1)x_2(1)\ldots x_n(1); \\ z(t) = f_2(u(t), y(t)), \\ y(t+1) = \neg u(t) g^{\delta}(y(t)) + u(t) g^{\tau}(y(t)), \\ y(1) = y_1(1)y_2(1)\ldots y_m(1); \\ t \geqslant 1. \end{cases}$$

Здесь подсистема E_1 из первого, второго и третьего уравнений описывает работу управляющего автомата A_1, подсистема E_2 из четвёртого, пятого и шестого уравнений — работу управляемого автомата A_2.

Ключом генератора G теоретически может быть любое непустое подмножество множества $\{x(1), y(1), f_1, g_1, f_2, g_2, g, \delta, \tau\}$. Требование стойкости криптографического генератора накладывает определённые ограничения на применяемые в нём булевы функции. Кроме того, не любую булеву функцию можно задать практически. В этой связи предполагается, что каждая функция в генераторе принадлежит некоторому классу, и этот класс, в том числе для функции в составе ключа, общеизвестен. При известном ключе и заданных других параметрах генератора уравнения данной системы позволяют однозначно вычислить порождаемую генератором выходную последовательность $z(1)z(2)\ldots$

Задача криптоанализа произвольного генератора G заключается в определении его ключа в известном классе по заданному конечному отрезку $\gamma = z(1)z(2)\ldots z(l)$ последовательности, порождаемой им на этом ключе. В такой постановке задача возникает в криптоанализе поточного шифра, использующего данный генератор, атакой на шифр с известным или выбираемым открытым текстом. Её решение может быть получено как решение конечной подсистемы S_l указанной системы уравнений с $t = 1, 2, \ldots, l$. В случае неединственности решения системы S_l обычно рекомендуется задаться более длинным отрезком γ.

Решение системы S_l может быть найдено атакой грубой силы, или исчерпывающим поиском, т. е. перебором возможных ключей с вычислением при каждом выбранном ключе k начального отрезка γ' длины l порождаемой последовательности и сравнением его с отрезком γ. В случае $\gamma' = \gamma$ ключ k принимается за ответ задачи. Сложность этой атаки определяется размером ключевого пространства. Так, если ключом генератора служит его начальное состояние, то сложность атаки равна 2^{n+m}. Если же ключом является какая-либо из функций генератора, то сложность атаки равна мощности класса этой функции.

В данной работе показано, что в генераторе G с линейным автоматом A_2 ключ $y(1)$ вскрывается с полиномиальной сложностью решением системы линейных уравнений, а ключ $(x(1), y(1))$ — линеаризационной атакой сложности не более 2^n. Предложен метод, позволяющий в произвольном генераторе G с известными g, δ, τ и f_2 вычислить по γ отрезок управляющей последовательности $\alpha = u(1)u(2)\ldots u(l-1)$ на выходе A_1 и тем самым открыть две возможности для криптоанализа такого G: 1) вычислить его ключ $(x(1), y(1))$ атакой «встреча посредине» со сложностью 2^m; 2) свести задачу криптоанализа G к криптоанализу автомата A_1 — найти его ключ по α. Сложность

метода полиномиальная, если $y(1)$ не входит в ключ, и не превосходит 2^m в противном случае. Ключ $x(1)$ автомата A_1 находится решением его системы уравнений E_1, а вскрытие ключа f_1 в A_1, в свою очередь, сводится к доопределению частичной булевой функции со значениями $u(t)$ на состояниях $x(t)$ для $t = 1, 2, \ldots, l-1$ до функции в классе функции f_1. Аналогично, к доопределению частичной булевой функции со значениями $z(t)$ на парах $(u(t), y(t))$ для $t = 1, 2, \ldots, l$ до функции в классе функции f_2 сводится вскрытие ключа f_2 произвольного генератора G. Осуществление подобного доопределения демонстрируется на классе, состоящем из всех булевых функций от большого числа переменных с малым количеством существенных аргументов из них.

ЛИТЕРАТУРА

1. *Фомичёв В. М.* Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003. 400 с.

УДК 519.7 DOI 10.17223/2226308X/9/18

О ГРУППЕ, ПОРОЖДЁННОЙ РАУНДОВЫМИ ФУНКЦИЯМИ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ «КУЗНЕЧИК»

В. В. Власова, М. А. Пудовкина

Одно из направлений исследований итерационных алгоритмов блочного шифрования заключается в описании свойств группы, порожденной множеством всех частичных раундовых функций. Алгоритм «Кузнечик» является новым российским стандартом блочного шифрования. Доказывается, что группа, порождённая множеством всех частичных раундовых функций алгоритма блочного шифрования «Кузнечик», является знакопеременной.

Ключевые слова: *«Кузнечик», ГОСТ Р 34.12-2015, знакопеременная группа.*

Частичные раундовые функции многих алгоритмов блочного шифрования, появившихся в последние годы, представимы в виде композиции преобразований, реализующих слой наложения ключа (X-слой), слой s-боксов (S-слой) и линейный слой (L-слой). Такие алгоритмы называются XSL-алгоритмами блочного шифрования. XSL-алгоритмом является американский стандарт блочного шифрования AES и российский стандарт блочного шифрования «Кузнечик», вступивший в силу в январе 2016 г. Групповым свойствам XSL-алгоритмов посвящены работы [1 – 4]. В [1] для алгоритма AES доказывается, что группа G, порождённая всеми частичными раундовыми функциями, совпадает со знакопеременной. В [3] получены условия, достаточные для примитивности группы G XSL-алгоритма, и доказано, что AES удовлетворяет данным условиям. В [4, 2] получены достаточные условия того, что группа G XSL-алгоритма равна знакопеременной. В [5] приведено исследование приложения группового подхода к построению и анализу криптографических систем.

В данной работе доказывается, что группа, порождённая множеством всех частичных раундовых функций алгоритма «Кузнечик», совпадает со знакопеременной. Для этого используется теорема 1 из [2].

Рассмотрим итерационный алгоритм блочного шифрования. Частичная r-раундовая функция шифрования f_k представима в виде композиции r частичных раундовых функций $g_{k_1}, \ldots, g_{k_r}$, где k_i — раундовый ключ из множества ключей шифрования i-го раунда $K^{(i)}$, $i = 1, \ldots, r$. Во многих алгоритмах множества раундовых ключей совпадают, потому далее в тексте $K^{(1)} = \ldots = K^{(r)} = K$. В работе рассматривается группа $G = \langle g_k \mid k \in K \rangle$.

Обозначим V_l — l-мерное векторное пространство над полем $\mathrm{GF}(2)$; $S(V_l)$ и $A(V_l)$ — соответственно симметрическая и знакопеременная группы, действующие на пространстве V_l; $+$ — операция покоординатного сложения по модулю 2 двоичных векторов. В рассматриваемом алгоритме блочного шифрования блоки текстов из множества V_{mn} представимы также как векторы из декартова произведения ${V_n}^m$, $m > 1$ и $n > 1$ — натуральные числа. Данные представления отождествляются.

Частичная раундовая функция $g_k : V_{mn} \to V_{mn}$ задана условием

$$g_k : (x_1, \ldots, x_n) \mapsto a(s_1(x_1 + k^{(1)}), \ldots, s_n(x_n + k^{(n)})),$$

где $k = (k^{(1)}, \ldots, k^{(n)})$ — раундовый ключ; $x_i, k^{(i)} \in V_m$; подстановки (s-боксы) $s_1, \ldots, s_n \in S(V_m)$ действуют на V_m; a — линейное преобразование из полной линейной группы преобразований пространства V_{mn}.

Приведём достаточные условия для выполнения равенства $G = \langle g_k \mid k \in K \rangle = A(V_{mn})$.

Линейному преобразованию $a : {V_n}^m \to {V_n}^m$ поставим в соответствие орграф $\Gamma(a)$ с множествами вершин $\{1, \ldots, n\}$ и дуг X, в котором дуга $(i, j) \in X$ тогда и только тогда, когда j-я координатная функция $a_j(x_1, \ldots, x_n)$ линейного преобразования a существенно зависит от x_i, где $x_1, \ldots, x_n \in V_m$.

Вектору $x = (x_1, \ldots, x_n) \in {V_n}^m$, поставим в соответствие множество $I(x) = \{i \in \{1, \ldots, n\} : x_i \neq 0_m\}$, где 0_m — нулевой вектор пространства V_m. Если I — подмножество вершин графа $\Gamma(a)$, то $J(I)$ — множество концов дуг с началом в множестве I.

Подстановке s_i поставим в соответствие подстановки

$$s_{i,k,k'} : x \mapsto s_i^{-1}(k' + s_i(x + k)),$$

где $k, k' \in V_m$, $i = 1, \ldots, n$. Обозначим через $H(s_i) = \langle s_{i,k,k'} \mid (k, k') \in V_m^2 \rangle$ порождённую данными подстановками группу.

Теорема 1 [2]. Пусть выполнены следующие условия:

1) граф $\Gamma(a)$ является примитивным;
2) для любого множества $L \subseteq \{1, \ldots, n\}$ выполнено неравенство

$$\max_{\{x \in V_{mn} : I(x) = L\}} |I(a(x))| \geqslant |L|;$$

3) группы $H(s_1), \ldots, H(s_n)$ являются 2-транзитивными и среди элементов данных групп существует такая подстановка $s \in S(V_m)$, что

$$|\{x \in V_m : s(x) = x\}| \notin \{0, 2^0, 2^1, 2^2, \ldots, 2^m\}.$$

Тогда $G = \langle g_k \mid k \in K \rangle = A(V_{mn})$.

Проверим выполнение данных условий для алгоритма блочного шифрования «Кузнечик» [6].

Для проверки условия 1 теоремы 1 рассмотрим свойства линейного преобразования a алгоритма «Кузнечик». Путём непосредственных вычислений найден орграф $\Gamma(a)$. Известно [7], что граф примитивен тогда и только тогда, когда он сильно связен и наибольший общий делитель длин всех его простых контуров равен 1. Экспериментально проверено выполнение условий, достаточных для примитивности орграфа $\Gamma(a)$.

Проверка условия 2 теоремы 1 осуществлялась с помощью [2, теорема 2], согласно которой условие 2 выполняется, в частности, если выполнено неравенство

$$2^{mn} < (2^m - 1)^{n-1}(2^m + 2^{m-1} - 2). \tag{1}$$

Справедливость неравенства (1) проверена с помощью непосредственных вычислений (левая часть неравенства (1) равна $3{,}4028 \cdot 10^{38}$, правая часть — $4{,}7881 \cdot 10^{38}$).

Для проверки условия 3 теоремы 1 найдена разностная матрица λ s-боксов алгоритма «Кузнечик». Данной матрице поставлен в соответствие граф $\Lambda(s_i)$, определяемый матрицей смежности $\lambda(s_i)\lambda(s_i)^{\mathrm{T}} = (m_{\alpha\beta})$, где $\lambda(s_i)^{\mathrm{T}}$ — транспонированная матрица $\lambda(s_i)$. Множеством вершин графа $\Lambda(s_i)$ является множество всех ненулевых векторов из V_m, вершины α и β соединены ребром тогда и только тогда, когда $m_{\alpha\beta} > 0$.

Согласно [2, теорема 3], для 2-транзитивности группы $H(s_i)$ необходима и достаточна связность графа $\Lambda(s_i)$. Экспериментально проверена связность графа $\Lambda(s_i)$ для s-боксов алгоритма «Кузнечик».

Выполнение второй части условия 3 теоремы 1 эквивалентно нахождению в разностной матрице s-боксов алгоритма «Кузнечик» элементов, отличных от степеней 2. Непосредственно проверено существование таких элементов в разностной матрице λ.

Теорема 2. Для алгоритма блочного шифрования «Кузнечик» группа G, порождённая множеством всех частичных раундовых функций, равна знакопеременной группе $A(V_{128})$.

ЛИТЕРАТУРА

1. *Wernsdorf R.* The round functions of RIJNDAEL generate the alternating group // LNCS. 2002. V. 2365. P. 143–148.
2. *Маслов А. С.* Об условиях порождения SA-подстановками знакопеременной группы // Труды института математики. 2007. Т. 15. № 2. С. 58–68.
3. *Caranti A., Dalla Volta F., Sala M., and Villani F.* Imprimitive permutation groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis. `http://arxiv.org/pdf/math/0606022.pdf`
4. *Caranti A., Dalla Volta F., and Sala M.* An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher // Designs, Codes and Cryptography. 2009. V. 52. P. 293–301.
5. *Глухов М. М., Погорелов Б. А.* О некоторых применениях групп в криптографии // Математика и безопасность информационных технологий. Материалы конф. в МГУ 28–29 октября 2004. М.: МЦНМО, 2005. С. 19–31.
6. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
7. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.

УДК 519.7 DOI 10.17223/2226308X/9/19

ОЦЕНКИ СТОЙКОСТИ ШИФРОВ СЕМЕЙСТВА TRIVIUM К КРИПТОАНАЛИЗУ НА ОСНОВЕ АЛГОРИТМОВ РЕШЕНИЯ ПРОБЛЕМЫ БУЛЕВОЙ ВЫПОЛНИМОСТИ[1]

О. С. Заикин, И. В. Отпущенников, А. А. Семёнов

Представлены результаты криптоанализа трёх поточных шифров семейства Trivium (Bivium, Trivium toy, Bivium toy). Криптоанализ осуществляется за счёт сведения обращения соответствующих дискретных функций к задаче о булевой выполнимости (SAT). Криптоанализ неослабленного шифра Bivium toy удалось осуществить на персональном компьютере. Задачи криптоанализа шифров Bivium и Trivium toy оказались более сложными, в связи с чем исследованы их ослабленные варианты. Соответствующие SAT-задачи были решены на вычислительном кластере и проекте добровольных распределённых вычислений SAT@home. При этом использована предложенная ранее техника распараллеливания по данным, согласно которой из множества переменных пропозициональной кодировки рассматриваемой задачи специальным образом выбирается некоторое подмножество, по которому исходная задача разбивается на независимые подзадачи.

Ключевые слова: *поточный шифр, шифр Trivium, шифр Bivium, криптоанализ, задача о булевой выполнимости.*

В [1] предложен поточный шифр Trivium, который состоит из трёх сдвиговых регистров специального вида. Первый из них включает 93 ячейки, второй — 84, третий — 111 ячеек (суммарная длина состояний регистров Trivium равна 288 битам). Trivium принимал участие в конкурсе eSTREAM и стал одним из победителей в «аппаратной» категории. С исследовательскими целями параллельно с Trivium его автор ввёл в рассмотрение шифр Bivium, в котором используются только два первых регистра Trivium.

В работе [2] выполнен скрупулёзный анализ возможных слабостей Trivium и Bivium. Как результат, описана атака, основанная на алгоритме восстановления внутренних состояний регистров, эксплуатирующем особенности уравнений шифрования рассматриваемых шифров. Сложность этой атаки для Bivium оказалась существенно меньше сложности полного перебора ключевого пространства. Несмотря на это, данная атака, к сожалению, плохо подходит для практической реализации из-за очень больших констант в оценке эффективности лежащего в её основе алгоритма. В работе [3] впервые было предложено использовать для криптоанализа Bivium SAT-подход. В [4 – 7] предложены последовательно улучшающиеся оценки времени SAT-криптоанализа Bivium. В [7] описана техника распараллеливания SAT, основанная на стохастическом оценивании времени обработки декомпозиционных множеств. Данная техника в применении к Bivium дала рекордную на настоящий момент оценку времени его криптоанализа.

В [8] введены в рассмотрение т. н. «игрушечные» версии шифров Trivium и Bivium — соответственно Trivium toy и Bivium toy. Авторы [8] позиционировали эти шифры как объекты для применения к ним новых методов криптоанализа, которые, возможно, будут полезны в дальнейшем при исследовании «полновесных» шифров.

[1]Работа частично поддержана РФФИ (гранты №14-07-00403-а, 15-07-07891-а и 16-07-00155-а) и советом по грантам Президента РФ (стипендия №СП-1184.2015.5).

В работе представлены результаты SAT-криптоанализа шифров Bivium, Bivium toy и Trivium toy. На примере криптоанализа Bivium продемонстрирована техника распараллеливания SAT, кратко описанная в [7]. Результаты криптоанализа Bivium toy и Trivium toy являются полностью новыми. Для сведения к SAT задач криптоанализа перечисленных шифров использован программный комплекс Transalg [9, 10]. Декомпозиционные представления получаемых SAT-задач обрабатывались посредством параллельного SAT-решателя PD-SAT [6].

Шифр Trivium toy получен из шифра Trivium уменьшением длины каждого регистра в 3 раза. Соответственно первый его регистр состоит из 31 ячейки, второй — из 28, третий — из 37 ячеек. Шифр Bivium toy, в свою очередь, получен из шифра Trivium toy отбрасыванием третьего регистра (по аналогии с построением Bivium на основе Trivium). Таким образом, задача криптоанализа (восстановления состояний регистров) Trivium toy заключается в нахождении 96 бит, а для Bivium toy — 59 бит.

Криптоанализ Bivium toy оказался очень простым — для его успешной реализации не потребовалось даже распараллеливать соответствующую SAT-задачу. Всего с помощью обычных (последовательных) SAT-решателей решено 10 задач криптоанализа Bivium toy в описанной постановке. Лучшие результаты при этом показал SAT-решатель rokk (один из призёров конкурса SAT Competition 2014): среднее время его работы на одном ядре процессора AMD Opteron 6276 составило около 2 мин.

Криптоанализ шифра Bivium кратко описан в [7]. Последние результаты в этом направлении заключаются в следующем. Для данного шифра удаётся осуществлять вариант «guess-and-determine»-атаки [11], в которой предполагаются известными значения 9 бит в последних ячейках второго регистра Bivium. Таким образом, требуется восстановить 168 неизвестных бит заполнения регистров Bivium (их суммарная длина равна 177 бит). При этом анализируются 200 бит ключевого потока. На решение данной задачи техникой, описанной в [7], уходит в среднем две недели работы проекта добровольных вычислений SAT@home.

В неослабленном варианте шифр Trivium toy оказался весьма стойким к SAT-криптоанализу. Это лишний раз подчёркивает, насколько удачны идеи, на которых он построен. Мы рассматривали задачу восстановления состояния регистров Trivium toy на основе 100 известных бит ключевого потока. На текущем этапе за приемлемое время удаётся осуществлять лишь вариант «guess-and-determine»-атаки, в которой известными предполагаются биты восстанавливаемого состояния, находящиеся в первых 16 ячейках второго регистра. Таким образом, в данной постановке необходимо найти оставшиеся 80 из 96 бит начального заполнения регистров. Решено 5 таких задач. Для решения каждой использовался решатель PD-SAT, обрабатывающий декомпозиционное семейство, построенное по 31 переменным, кодирующим первый регистр Trivium toy. Все эти задачи успешно решены на вычислительном кластере ИНЦ СО РАН «Академик В. М. Матросов». В среднем на каждую задачу потребовалось около суток работы двадцати 16-ядерных процессоров AMD Opteron 6276 (т. е. 320 процессорных ядер).

ЛИТЕРАТУРА

1. *Canniere C. D.* Trivium: A stream cipher construction inspired by block cipher design principles // LNCS. 2006. V. 4176. P. 171–186.
2. *Maximov A. and Biryukov A.* Two trivial attacks on Trivium // SAC'07. LNCS. 2007. V. 4876. P. 36–55.

3. *Mcdonald C., Charnes C., and Pieprzyk J.* Attacking Bivium with MiniSat. Technical Report 2007/040. ECRYPT Stream Cipher Project, 2007.
4. *Eibach T., Pilz E., and Volkel G.* Attacking Bivium using SAT solvers // LNCS. 2008. V. 4996. P. 63–76.
5. *Soos M., Nohl K., and Castelluccia C.* Extending SAT solvers to cryptographic problems // LNCS. 2009. V. 5584. P. 244–257.
6. *Заикин О. С., Семенов А. А.* Применение метода Монте-Карло к прогнозированию времени параллельного решения проблемы булевой выполнимости // Вычислительные методы и программирование: новые вычислительные технологии. 2014. Т. 15. № 1. С. 22–35.
7. *Semenov A. A. and Zaikin O. S.* Using Monte Carlo method for searching partitionings of hard variants of Boolean satisfiability problem // LNCS. 2015. V. 9251. P. 222–230.
8. *Lechtaler A. C., Cipriano M., Garcia E., et al.* Model design for a reduced variant of a Trivium type stream cipher // J. Computer Science & Technology. 2014. V. 14. No. 1. P. 55–58.
9. *Отпущенников И. В., Семенов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
10. *Otpuschennikov I. V., Semenov A. A., and Kochemazov S. E.* Transalg: a tool for translating procedural descriptions of discrete functions to SAT // Proc. 5th Intern. Workshop on Computer Science and Engineering: Information Processing and Control Engineering (WCSE 2015-IPCE). 2015. P. 289–294.
11. *Bard G. V.* Algebraic Cryptanalysis. Springer, 2009.

УДК 519.1 DOI 10.17223/2226308X/9/20

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ЭКСПОНЕНТОВ РАУНДОВЫХ ПЕРЕМЕШИВАЮЩИХ МАТРИЦ ОБОБЩЁННЫХ СЕТЕЙ ФЕЙСТЕЛЯ

А. М. Коренева, В. Н. Мартышин

Исследованы перемешивающие свойства раундовых функций обобщённых сетей Фейстеля, построенных на основе регистров сдвига длины 4 над множеством двоичных 32-мерных векторов. Рассмотрены регистровые функции с различным числом обратных связей регистра. Приведены результаты экспериментального исследования, направленного на выбор параметров регистровых функций, при которых реализуется наиболее быстрое перемешивание входных данных.

Ключевые слова: *обобщённая сеть Фейстеля, раунд шифрования, перемешивающая матрица, экспонент матрицы.*

Введение

Обозначим через $R(n, r, k)$ класс регистров сдвига длины n над множеством V_r двоичных r-мерных векторов с k обратными связями, $n, r > 1$, $k \geqslant 1$. Класс $R(n, r, k)$ обобщает класс $R(2, r, 1)$, относящийся к оригинальным сетям Фейстеля.

Увеличение длины базового регистра способствует увеличению производительности шифрования и вместе с тем числа раундов, достаточного для перемешивания входных данных. Свойства обобщённых сетей Фейстеля (ОСФ) исследовались как в зарубежных [1 – 4], так и в отечественных работах [5 – 7]. На основе ОСФ построены алгоритмы CAST-256, MARS, SMS4, CLEFIA, Piccolo, HIGHT и др. В [3] исследованы классы сетей $R(n, r, n/2)$, n — чётное (эти сети названы обобщёнными сетями Фейстеля 2-го типа). Отмечено, что вычислительная реализация таких сетей допускает распараллеливание и количество раундов, необходимых для перемешивания входных

данных, оценивается снизу величиной порядка n. С целью улучшения перемешивающих свойств сетей из класса $R(n, r, n/2)$ в [3] предложено заменить циклический сдвиг подблоков перестановками, что позволило понизить оценку числа раундов полного перемешивания подблоков до $2\log_2 n$.

В [4] исследованы классы сетей $R(n, r, 1)$, $R(n, r, n/2)$, $R(n, r, n-1)$ (ОСФ 1-го, 2-го и 3-го типа соответственно). С помощью орграфа перемешивания подблоков получены оценки числа раундов перемешивания входных подблоков: $(n-1)^2+1$ для $R(n, r, 1)$; n для двух других.

Отметим, что перемешивание входных подблоков не обеспечивает перемешивания битов (зависимости каждого бита выходного блока от всех входных битов), что сохраняет возможность применения некоторых криптоаналитических атак. Следовательно, исследование битового перемешивания для ОСФ является актуальным.

Работа посвящена перемешивающим свойствам раундовых функций ОСФ, построенных на основе классов регистров сдвига $R(4, 32, k)$, $k = 1, 2, 3$, т. е. ОСФ 1-го, 2-го и 3-го типа соответственно. Для исследования перемешивающих свойств используется оценочный матрично-графовый подход, который заключается в построении перемешивающей матрицы M для раундовой функции и экспериментальном определении значения её экспонента ($\exp M$). Значение $\exp M$ оценивает снизу число итераций, необходимое для полного перемешивания входных данных, то есть для обеспечения существенной зависимости каждой координатной булевой функции от всех входных переменных. Приведены результаты экспериментального исследования, направленного на выбор параметров регистровых функций, при которых реализуется наиболее быстрое полное перемешивание входных данных.

1. ОСФ на основе класса регистров сдвига $R(4,32,k)$

Сети классов регистров сдвига $R(4, 32, 1), R(4, 32, 2), R(4, 32, 3)$ реализуют преобразования $g^{(1)}, g^{(2)}, g^{(3)}$ соответственно:

$$g^{(1)}(X_1, X_2, X_3, X_4) = (F_q(X_1) \oplus X_2, X_3, X_4, X_1); \tag{1}$$

$$g^{(2)}(X_1, X_2, X_3, X_4) = (F_q(X_1) \oplus X_2, X_3, F_w(X_3) \oplus X_4, X_1); \tag{2}$$

$$g^{(3)}(X_1, X_2, X_3, X_4) = (F_q(X_1) \oplus X_2, F_w(X_2) \oplus X_3, F_v(X_3) \oplus X_4, X_1), \tag{3}$$

где $q, w, v, X_1, X_2, X_3, X_4 \in V_{32}$; (X_1, X_2, X_3, X_4) — открытый текст; q, w, v — раундовые ключи (подключи в случае схем типа 2 и 3); $F_a : V_{32} \to V_{32}$ — функция усложнения, реализуемая при раундовом ключе (подключе) $a \in \{q, w, v\}$. Схемы раунда шифрования для ОСФ 1-го, 2-го и 3-го типа представлены на рис. 1, выходные подблоки Y_1, Y_2, Y_3, Y_4 определены в соответствии с формулами (1)–(3).

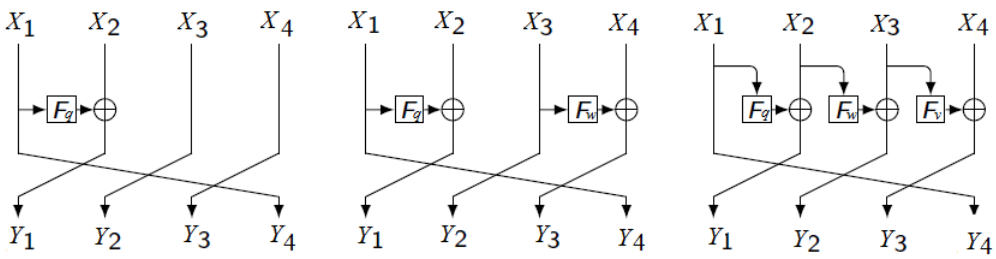


Рис. 1. Схемы раунда шифрования для ОСФ 1-го, 2-го и 3-го типов

2. Экспериментальное исследование перемешивающих свойств ОСФ при некоторых вариантах функции усложнения

Раундовые функции алгоритмов шифрования на основе ОСФ 2-го и 3-го типа могут использовать идентичные функции усложнения, что позволяет применить распараллеливание при вычислении раундовой функции. В эксперименте в качестве функции F_a, $a \in \{q, w, v\}$, использована функция усложнения отечественного алгоритма блочного шифрования ГОСТ 28147-89 (с различными вариантами подмешивания раундовых ключей), свойства которой хорошо изучены. Определим функцию усложнения F_a:

$$F_a(X_i) = T_{\text{left}}(S_{8,4}(X_i * a)),$$

где $a, X_i \in V_{32}$, $i = 1, 2, 3$; $*$ означает или XOR-суммирование двоичных векторов (обозначаемое $\oplus$), или сложение по модулю 2^{32} (обозначаемое $+$); $S_{8,4} = (S_1, \ldots, S_8)$; $S_1, \ldots, S_8$ — преобразования множества V_4 (s-боксы алгоритма ГОСТ 28147-89); T_{left} — циклический сдвиг векторов из V_{32} на 11 битов влево. Используя (1), (2) и (3), построим перемешивающие матрицы $M(g^{(1)})$, $M(g^{(2)})$, $M(g^{(3)})$. В матрицах $M(g^{(i)})$, $i = 1, 2, 3$, обозначим подматрицы размера 32×32: 0 — нулевая (состоящая из нулей) подматрица; E — единичная подматрица; $\Psi = \psi(i, j)$, где $\psi(i, j) = 1 \Leftrightarrow$ функция $g_j^{(i)}$ зависит существенно от переменной x_i, $i, j \in \{1, \ldots, 32\}$; $\Phi = \phi(i, j)$, где $\phi(i, j) = 1 \Leftrightarrow$ функция $g_j^{(i)}$ зависит существенно от переменной x_i, $i \in \{65, \ldots, 96\}$, $j \in \{65, \ldots, 96\}$; $\Lambda = \lambda(i, j)$, где $\lambda(i, j) = 1 \Leftrightarrow$ функция $g_j^{(i)}$ зависит существенно от переменной x_i, $i \in \{33, \ldots, 64\}$, $j \in \{33, \ldots, 64\}$. Таким образом, матрицы $M(g^{(i)})$, $i = 1, 2, 3$, имеют следующий вид:

$$M(g^{(1)}) = \begin{pmatrix} \Psi & 0 & 0 & E \\ E & 0 & 0 & 0 \\ 0 & E & 0 & 0 \\ 0 & 0 & E & 0 \end{pmatrix}, M(g^{(2)}) = \begin{pmatrix} \Psi & 0 & 0 & E \\ E & 0 & 0 & 0 \\ 0 & E & \Phi & 0 \\ 0 & 0 & E & 0 \end{pmatrix}, M(g^{(3)}) = \begin{pmatrix} \Psi & 0 & 0 & E \\ E & \Lambda & 0 & 0 \\ 0 & E & \Phi & 0 \\ 0 & 0 & E & 0 \end{pmatrix}.$$

В таблице приведены результаты вычислительного эксперимента по определению значений экспонентов перемешивающих матриц $M(g^{(1)})$, $M(g^{(2)})$, $M(g^{(3)})$ в зависимости от способов построения функций F_a.

Значения экспонентов перемешивающих матриц $M(g^{(1)})$, $M(g^{(2)})$, $M(g^{(3)})$

Функция F_a	$\exp M(g^{(1)})$	$\exp M(g^{(2)})$	$\exp M(g^{(3)})$
$T_{\text{left}}(S_{8,4}(X_i \oplus a))$	14	12	12
$T_{\text{left}}(S_{8,4}(X_i + a))$	9	7	7

В результате экспериментальных исследований получены некоторые рекомендации по выбору параметров функций обратной связи регистров сдвига, при которых реализуется наиболее быстрое полное перемешивание входных данных. В частности, к улучшению перемешивающих свойств приводит:

1) Замена циклического левого сдвига на 11 бит инволюцией координат вектора ($T_{\text{inv}}(x_1, \ldots, x_{32}) = (x_{32}, \ldots, x_1)$). При таком изменении $\exp M(g^{(1)}) = 8$, $\exp M(g^{(2)}) = 6$, $\exp M(g^{(3)}) = 6$.
2) Укрупнение s-боксов (использование преобразований $S_1, \ldots, S_4$ множества V_8). В этом случае $\exp M(g^{(1)}) = 8$, $\exp M(g^{(2)}) = 6$, $\exp M(g^{(3)}) = 6$.
3) Использование инволютивной перестановки битов в начальных подблоках, являющихся аргументами функции усложнения (для схемы 2-го типа это подблоки 2 и 4). В этом случае $\exp M(g^{(2)}) = 5$.

4) Замена циклического сдвига подблоков другой перестановкой. Например, в схеме 3-го типа можно заменить перестановку подблоков $\pi = \{4, 1, 2, 3\}$ на $\pi = \{4, 1, 3, 2\}$. В этом случае $\exp M(g^{(3)}) = 5$.

Выводы

Экспериментально получены значения экспонентов раундовых перемешивающих матриц ОСФ, построенных на основе регистров сдвига длины 4. Это позволяет сформулировать обоснованные рекомендации по выбору числа итераций раундового преобразования, при котором обеспечивается существенная зависимость каждой координатной функции выхода от всех переменных входа. Даны рекомендации по выбору параметров функций обратной связи регистров сдвига, при которых реализуется наиболее быстрое перемешивание входных данных.

ЛИТЕРАТУРА

1. *Nyberg K.* Generalized Feistel networks // ASIACRYPT'96. LNCS. 2005. V. 1163. P. 91–104.
2. *Hoang V. T. and Rogaway P.* On generalized Feistel networks // CRYPTO'2010. LNCS. 2010. V. 6223. P. 613–630.
3. *Suzaki T. and Minematsu K.* Improving the generalized Feistel // FSE'2010. LNCS. 2010. V. 6147. P. 19–39.
4. *Berger T P., Minier M., and Thomas G.* Extended generalized Feistel networks using matrix representation // LNSC. 2014. V. 8282. P. 289–305.
5. *Пудовкина М. А., Токтарев А. В.* Об оценке числа раундов с невозможными разностями в обобщённых алгоритмах шифрования Фейстеля // Прикладная дискретная математика. 2015. № 1. С. 37–51.
6. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3(17). С. 34–40.
7. *Коренева А. М.* О блочных шифрах, построенных на основе регистров сдвига с двумя обратными связями // Прикладная дискретная математика. 2013. № 6. С. 39–41.

УДК 519.1 DOI 10.17223/2226308X/9/21

О СУЩЕСТВЕННЫХ ПЕРЕМЕННЫХ ФУНКЦИИ ПЕРЕХОДОВ МОДИФИЦИРОВАННОГО АДДИТИВНОГО ГЕНЕРАТОРА

А. М. Коренева, В. М. Фомичёв

Исследован класс биективных регистров сдвига длины n над множеством V_r двоичных r-мерных векторов, $n, r > 1$, построенных на основе аддитивных генераторов по модулю 2^r, модифицированных с использованием подстановки множества V_r. Функция обратной связи таких регистров является композицией функции обратной связи аддитивного генератора и преобразования множества V_r. Задача точного определения существенных переменных для композиции нелинейных функций, как правило, сложна, однако использование комбинаторных свойств биекции $\mathbb{Z}_{2^r} \leftrightarrow V_r$ позволило полностью описать множество существенных переменных функции обратной связи исследуемых регистров.

Ключевые слова: *аддитивный генератор, существенная переменная, перемешивающие свойства.*

Введение

Работа посвящена исследованию подстановок регистров сдвига длины n над множеством V_r двоичных r-мерных векторов при $n, r > 1$. Данный класс подстановок (обозначим его $R(n, r)$) обобщает как класс $R(2, r)$, лежащий в основе сетей Фейстеля, так и подстановки множества состояний аддитивных генераторов (обозначим $R_{\mathrm{ad}}(n, r)$ этот подкласс класса $R(n, r)$).

Аддитивные генераторы исследуются с середины XX века. В [1] дан краткий обзор аддитивных генераторов чисел по модулю m, указаны их преимущества и недостатки. Один из первых аддитивных генераторов построен Дж. Ж. Митчелом и Д. Ф. Муром в 1958 г.: последовательность, генерируемая в соответствии с законом рекурсии $X_n = (X_{n-24} + X_{n-55}) \bmod m$, $n \geqslant 55$, где m — чётное число; $X_0, \ldots, X_{54}$ — произвольные целые не все чётные числа. Выбор чисел 24 и 55 обеспечивает длину периода $2^{55} - 1$ последовательности, составленной из младших двоичных разрядов чисел X_n. Позднее на основе аддитивных генераторов были построены криптографические алгоритмы Fish, Pike, Mush [2].

Известно, что аддитивные генераторы по модулю 2^r плохо перемешивают входные данные. В связи с этим представляет интерес изучение перемешивающих свойств модификаций аддитивных генераторов по модулю 2^r с помощью подстановки, применяемой к функции обратной связи. Заметим, что перемешивающие свойства регистров из $R(n, r)$ исследованы в [3, 4]. В [5] получены условия полного перемешивания для модификации аддитивного генератора с помощью инволютивной перестановки координат векторов из V_r. В настоящей работе с целью исследования перемешивающих свойств широкого класса модификаций описано множество существенных переменных функции, являющейся композицией функции обратной связи регистра из $R_{\mathrm{ad}}(n, r)$ и произвольной подстановки множества V_r.

1. Определяющие функции аддитивных генераторов и модификаций

Рассмотрим аддитивный генератор по модулю 2^r (регистр сдвига длины n над кольцом вычетов $\mathbb{Z}_{2^r}$), $r > 1$. Для $i \geqslant n$ знак X_i образуется в соответствии с законом рекурсии

$$X_i = (\sum_{j=0}^{n-1} a_j X_{j+i-n}) \bmod 2^r, \quad i \geqslant n, \tag{1}$$

где $a_1, \ldots, a_{n-1} \in \{0, 1\}$ и $a_0 = 1$. Из закона рекурсии (1) следует, что i-е разряды двоичного представления каждого из чисел $X_0, X_1, \ldots, X_{n-1}$ текущего состояния зависят только от r-го, …, i-го разрядов чисел предыдущего состояния, $i = 1, \ldots, r$, что исключает хорошие перемешивающие свойства преобразования множества состояний аддитивного генератора. Модифицируем аддитивный генератор с помощью преобразования g множества V_r, такой генератор назовем g-модификацией аддитивного генератора.

Обозначим через b биекцию $\mathbb{Z}_{2^r} \leftrightarrow V_r$, сопоставляющую числу $X_i \in \mathbb{Z}_{2^r}$ его двоичное представление (b^{-1} — обратная к b функция). Для g-модификации аддитивного генератора закон рекурсии имеет вид

$$X_i = b^{-1}(g(b((\sum_{j=0}^{n-1} a_j X_{j+i-n}) \bmod 2^r))), \quad i \geqslant n. \tag{2}$$

Обозначим через φ^g преобразование множества V_{nr}, которое реализуется g-модификацией

$$\varphi^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = (\overline{X}_1, \ldots, \overline{X}_{n-1}, f^g(\overline{X}_0, \ldots, \overline{X}_{n-1})). \tag{3}$$

Следовательно, φ^g есть преобразование регистра сдвига с обратной связью $f^g : V_{nr} \to V_r$, где

$$f^g(\overline{X}_0, \ldots, \overline{X}_{n-1}) = g(f(\overline{X}_0, \ldots, \overline{X}_{n-1})) = g(b((\sum_{j=0}^{n-1} a_j X_j) \bmod 2^r)). \qquad (4)$$

Функция обратной связи g-модификации является композицией функции f обратной связи аддитивного генератора и преобразования g множества V_r. Определим модифицированный аддитивный генератор как автономный автомат $A = (V_{nr}, V_r, h, \psi)$, где V_{nr} — множество состояний; V_r — выходной алфавит; $h = \varphi^g(\overline{X}_0, \ldots, \overline{X}_{n-1})$ — функция переходов; $\psi = f^g(\overline{X}_0, \ldots, \overline{X}_{n-1})$ — функция выходов. Исследуем множество существенных переменных функции переходов этого генератора.

2. Свойства биекции $\mathbb{Z}_{2^r} \leftrightarrow V_r$

Функцию f, определённую на множестве X, назовем постоянной на подмножестве $Q \subseteq X$, если ограничение f на Q есть константа. При $\tau = 1, \ldots, r-1$ выполнены следующие разбиения:

1) r-мерный куб V_r разбивается на $2^{r-\tau}$ подкубов $Q(c_{\tau+1}, \ldots, c_r)$ размерности τ вида
$$Q(c_{\tau+1}, \ldots, c_r) = \{(y_1, \ldots, y_\tau, c_{\tau+1}, \ldots, c_r) : y_1, \ldots, y_\tau \in \{0, 1\}\},$$
где $(c_{\tau+1}, \ldots, c_r) \in V_{r-\tau}$;
2) аддитивная группа $\mathbb{Z}_{2^r}$ разбивается на $2^{r-\tau}$ смежных классов вида $2^{r-\tau}\mathbb{Z}_{2^r} + a$ по подгруппе $2^{r-\tau}\mathbb{Z}_{2^r}$, где $a \in \mathbb{Z}_{2^{r-\tau}}$.

Такие системы подкубов и смежных классов обозначим соответственно Q_r^τ и $\mathbb{Z}_{2^r}^\tau$. С преобразованием g связано преобразование $\hat{g}$ группы $\mathbb{Z}_{2^r}$:

$$\hat{g}(Y) = b^{-1}(g(b(Y))).$$

Из формул (2)–(4) непосредственно следуют леммы 1 и 2.

Лемма 1. Биекция $b : \mathbb{Z}_{2^r} \leftrightarrow V_r$ индуцирует биекцию $\xi : Q_r^\tau \leftrightarrow \mathbb{Z}_{2^r}^\tau$ со свойством $\xi(Q(c_{\tau+1}, \ldots, c_r)) = 2^{r-\tau}\mathbb{Z}_{2^r} + b^{-1}(0, \ldots, 0, c_{\tau+1}, \ldots, c_r)$.

Обозначим $g_u(y_1, \ldots, y_r)$ координатные булевы функции преобразования g, u=$1, \ldots, r$.

Лемма 2. Функция $g_u(y_1, \ldots, y_r)$ постоянна на любом подкубе из системы Q_r^τ, если и только если $y_1, \ldots, y_\tau$ — фиктивные переменные координатной функции g_u, $u = 1, \ldots, r$.

3. Существенные переменные функции переходов

Обозначим: $\varphi^g_{u+rk}(\overline{X}_0, \ldots, \overline{X}_{n-1})$ — координатные булевы функции преобразования φ^g, $u = 1, \ldots, r$, $k = 0, 1, \ldots, n-1$; $D = \{d_0, \ldots, d_q\}$ — множество точек съёма регистра φ^g (то есть множество номеров существенных переменных функции обратной связи регистра φ^g), где $0 < q$, $0 = d_0 < \cdots < d_q < n$ и $j \in D \Leftrightarrow a_j = 1$; $E(\varphi^g_j)$ — множество номеров существенных переменных координатной функции φ^g_j, $j = 1, \ldots, nr$.

Из (3) следует, что $E(\varphi^g_{u+rk}) = \{u + r(k+1)\}$ при $u = 1, \ldots, r$ и $k = 0, 1, \ldots, n-2$. Осталось описать существенные переменные координатных функций при $k = n-1$. Из (4) следует $\varphi^g_{u+r(n-1)}(\overline{X}_0, \ldots, \overline{X}_{n-1}) = g_u(b((\sum_{j=0}^{n-1} a_j X_j) \bmod 2^r))$.

Теорема 1. Для множества переменных функции $\varphi^g_{u+r(n-1)}$, $u = 1, \ldots, r$, верно:

а) x_{v+rk} фиктивная при любом $k \notin D$, $v = 1, \ldots, r$;

б) x_{v+rk} фиктивная при любом $k \in D$, $v = 1, \ldots, \tau$, если переменные $y_1, \ldots, y_\tau$ фиктивные для функции g_u, $\tau \geqslant 1$;

в) x_{v+rk} существенная при $v = \theta, \ldots, r$ и при любом $k \in D$, если переменная y_θ существенная для функции g_u, $\theta \geqslant 1$.

Пример 1. Пусть g-модифицированный аддитивный генератор построен на основе регистра сдвига длины n над V_4, $D = \{0, i, n-1\}$, где $0 < i < n-1$. На рис. 1 изображена схема g-модификации аддитивного генератора, знаком «+» обозначено сложение по модулю 2^{32}.

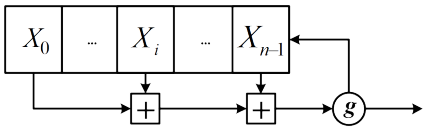


Рис. 1. Схема g-модификации аддитивного генератора

Пусть номера существенных переменных координатных функций преобразования g определены множествами $E(g_1) = \{2, 4\}$, $E(g_2) = \{3\}$, $E(g_3) = \{1\}$, $E(g_4) = \{4\}$. Тогда в соответствии с (3) и с теоремой 1, в получаем полное описание существенных переменных функции обратной связи g-модификации (таблица).

Номера существенных переменных функции переходов g-модификации

$k = 0, 1, \ldots, n-2$		$k = n-1$		
u	$E(\varphi^g_{u+rk})$	u	$E(g_u)$	$E(\varphi^g_{u+r(n-1)})$
1	$\{1 + r(k+1)\}$	1	$\{2, 4\}$	$\{2, 3, 4, 2 + ri, 3 + ri, 4 + ri, 2 + r(n-1), 3 + r(n-1), 4 + r(n-1)\}$
2	$\{2 + r(k+1)\}$	2	$\{4\}$	$\{4, 4 + ri, 4 + r(n-1)\}$
3	$\{3 + r(k+1)\}$	3	$\{1\}$	$\{1, 2, 3, 4, 1 + ri, 2 + ri, 3 + ri, 4 + ri, 1 + r(n-1), 2 + r(n-1), 3 + r(n-1), 4 + r(n-1)\}$
4	$\{4 + r(k+1)\}$	4	$\{3\}$	$\{3, 4, 3 + ri, 4 + ri, 3 + r(n-1), 4 + r(n-1)\}$

Выводы

С использованием комбинаторных свойств биекции $\mathbb{Z}_{2^r} \leftrightarrow V_r$ полностью описаны существенные переменные функции переходов модифицированного аддитивного генератора. Это позволяет изучать свойства перемешивающей матрицы (графа) преобразования множества состояний модифицированного аддитивного генератора.

ЛИТЕРАТУРА

1. *Кнут Д. Э.* Искусство программирования. Т. 2. Получисленные алгоритмы, 3-е изд. М.: Издательский дом «Вильямс», 2003.

2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.

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.

УДК 517.19 DOI 10.17223/2226308X/9/22

ПОИСК ИНФОРМАЦИОННОГО СООБЩЕНИЯ В ЗАШУМЛЁННЫХ КОДОВЫХ БЛОКАХ ПРИ МНОГОКРАТНОЙ ПЕРЕДАЧЕ ДАННЫХ

Ю. В. Косолапов, О. Ю. Турченко

Рассматривается модель защиты данных с помощью метода кодового зашумления. Предполагается, что кодируемые информационные блоки длины k содержат фиксированное сообщение m длины $l \leqslant k$ на фиксированной позиции q $(1 \leqslant q \leqslant k - l + 1)$, а наблюдатель получает зашумлённые кодовые слова длины n через двоичный симметричный канал с вероятностью ошибки $(1 - \Delta)/2$, $0 < \Delta \leqslant 1$. Целью наблюдателя является нахождение неизвестного ему сообщения m, когда позиция q неизвестна, а длина l известна. Предложен способ нахождения сообщения m и получена оценка количества наблюдаемых кодовых слов, достаточного для восстановления сообщения m этим способом.

Ключевые слова: *кодовое зашумление, многократная передача данных.*

Рассмотрим информационно-аналитическую систему (ИАС), в которой два легальных участника (отправитель и получатель) связаны каналом без помех, а пассивный наблюдатель подслушивает передаваемые данные по двоичному симметричному каналу с вероятностью ошибки $(1 - \Delta)/2$, $0 < \Delta \leqslant 1$. Такая система впервые была исследована в [1]. Предполагается, что перед передачей в канал данные кодируются с помощью метода случайного кодирования, а именно: для зафиксированных натуральных чисел k и n $(k < n)$ легальными участниками выбрана $((n-k)\times k)$-матрица P с элементами из поля $\mathbb{F}_2$, а каждый k-битный вектор s кодируется по правилу

$$\mathrm{Enc}(s) = (c_1|K) = c, \tag{1}$$

где $c_1 = s \oplus KP$; K — случайно и равновероятно выбранный вектор из $\mathbb{F}_2^{n-k}$; запись $a|b$ обозначает конкатенацию векторов a и b. Предполагается, что матрица P и правило кодирования (1) известны всем участникам ИАС (в том числе и наблюдателю). Поэтому, при отсутствии помех в канале между отправителем и получателем, правило декодирования имеет вид $\mathrm{Dec}(c) = KP \oplus c_1 = s$. У наблюдателя при подслушивании одного кодового слова из-за наличия помех возникает неопределённость относительно сообщения, которое было закодировано. Вычислению этой неопределённости посвящена, например, работа [2], а в [3] показано, что эта неопределённость может быть снята в рамках модели многократной передачи данных. В частности, в [3] найдена оценка количества зашумлённых кодовых сообщений, соответствующих одному информационному сообщению, достаточного для нахождения этого сообщения с заданными вероятностями ошибок первого и второго рода.

В настоящей работе рассматривается более сложная задача нахождения информационного сообщения в рамках модели многократной передачи данных, а именно предполагается, что в момент времени $t \in \mathbb{N}$ информационное сообщение $s^{(t)} \in \mathbb{F}_2^k$ имеет вид $s^{(t)} = (m_1^{(t)}|m|m_2^{(t)})$, $m_1^{(t)} \in \mathbb{F}_2^{q-1}$, $m \in \mathbb{F}_2^l$, $m_2^{(t)} \in \mathbb{F}_2^{k-[l+q]+1}$, где при $i \neq j$ в общем случае $\mathsf{P}\{m_1^{(i)} = m_1^{(j)}\} \neq 1$ и $\mathsf{P}\{m_2^{(i)} = m_2^{(j)}\} \neq 1$, а сообщение m постоянное для всех t. Предполагается также, что наблюдателю позиция q сообщения m неизвестна, а его длина l известна. Целью наблюдателя является нахождение неизвестного сообщения m при многократной передаче сообщений $s^{(t)}$, закодированных по правилу (1).

Задача решается в два этапа: сначала находится позиция q, а затем — само сообщение m. Для нахождения позиции q предлагается следующий способ. Выдвига-

ется гипотеза H_i о том, что $q = i$. В этом случае матрица P представима в виде $P = [P_1^{(i)}|P_2^{(i)}|P_3^{(i)}]$, где $P_1^{(i)}$ — первые $i-1$ столбцов матрицы P; $P_2^{(i)}$ — столбцы матрицы P с номерами от i до $i+l-1$; $P_3^{(i)}$ — последние $(k-(i+l)+1)$ столбцов матрицы P. В рамках гипотезы наблюдаемый в момент времени t вектор $z^{(t)} = c^{(t)} \oplus \theta^{(t)}$ имеет вид

$$z^{(t)} = (\widehat{m}_1^{(t)} \oplus K^{(t)} P_1^{(i)} \oplus \theta_1^{(t)} | \widehat{m} \oplus K^{(t)} P_2^{(i)} \oplus \theta_2^{(t)} | \widehat{m}_2^{(t)} \oplus K^{(t)} P_3^{(i)} \oplus \theta_3^{(t)} | K^{(t)} \oplus \theta_4^{(t)}),$$

где $\theta^{(t)} = (\theta_1^{(t)}|\theta_2^{(t)}|\theta_3^{(t)}|\theta_4^{(t)})$ — вектор помехи в двоичном симметричном канале.

Пусть $\tau(i) = \{i, \ldots, i+l-1\} \cup \{k+1, \ldots, n\}$ — множество координат. Построим выборку

$$Z_{\tau(i)} = \left(\widehat{z}_{\tau(i)}^{(1)}, \widehat{z}_{\tau(i)}^{(2)}, \ldots, \widehat{z}_{\tau(i)}^{(N)}\right), \tag{2}$$

где $\widehat{z}_{\tau(i)}^{(t)} = \pi_{\tau(i)}(z^{(t)})$ — проекция вектора $z^{(t)}$ на множество координат $\tau(i)$. Рассмотрим суммы $\widetilde{z}^{(t)} = \widehat{z}_{\tau(i)}^{(2t)} \oplus \widehat{z}_{\tau(i)}^{(2t-1)}$ и по ним сконструируем набор векторов:

$$\widetilde{Z} = \left(\widetilde{z}^{(1)} = \widehat{z}_{\tau(i)}^{(2)} \oplus \widehat{z}_{\tau(i)}^{(1)}, \widetilde{z}^{(2)} = \widehat{z}_{\tau(i)}^{(4)} \oplus \widehat{z}_{\tau(i)}^{(3)}, \ldots, \widetilde{z}^{(N/2)} = \widehat{z}_{\tau(i)}^{(N)} \oplus \widehat{z}_{\tau(i)}^{(N-1)}\right). \tag{3}$$

Утверждение 1. Если H_i — верная гипотеза ($i = q$), то выборка (3) представляет собой набор из зашумлённых кодовых слов линейного $[n-k+l, n-k]$-кода $\mathcal{D}^{(i)}$ с порождающей матрицей $[P_2^{(i)}|I_{n-k}]$, полученных из двоичного симметричного канала с вероятностью помехи $(1-\Delta^2)/2$.

В силу утверждения 1, проверка верности гипотезы H_i сводится к задаче распознавания кода по зашумлённому набору векторов. Заметим, что задача распознавания кода по зашумлённой выборке имеет несколько способов решения [4, 5]). В настоящей работе применяется метод из [4], идея которого состоит в том, что вес синдрома зашумлённого кодового слова в среднем меньше веса синдрома произвольного вектора. В соответствии с [4] для $h \in \mathbb{F}_2^v$, $\mathcal{Z} \subseteq \mathbb{F}_2^v$ и $T \geqslant 0$ обозначим через $\mathrm{ST}(h, \mathcal{Z}, T)$ статистический критерий, согласно которому принимается решение о том, что выборка $\mathcal{Z}$ является набором зашумлённых векторов из $h^\perp$, если $\sum\limits_{\widetilde{z} \in \mathcal{Z}} (h, \widetilde{z}) \leqslant T$.

Теорема 1 (C. Chabot, [4]). Пусть $h \in \mathbb{F}_2^v$, $w(h)$ — вес Хэмминга вектора h, $\mathcal{Z}$ — выборка из M векторов, полученная из двоичного симметричного канала с вероятностью ошибки p. При выборе статистического критерия $\mathrm{ST}(h, \mathcal{Z}, T)$ вероятности ошибок первого и второго рода не превышают α и β соответственно для

$$M = \left(\frac{b\sqrt{1-(1-2p)^{2w(h)}} - a}{(1-2p)^{w(h)}}\right)^2, \quad T = \frac{1}{2}(M + a\sqrt{M}), \tag{4}$$

где $a = \Phi^{-1}(\alpha)$; $b = \Phi^{-1}(1-\beta)$; $\Phi(x)$ — функция Лапласа.

Обозначим через $M(h, \alpha, \beta, p)$ объём выборки, вычисленный по формуле (4) для заданных h, α, β и p.

Утверждение 2. В рамках условий теоремы 1, для определения того, что выборка $\widetilde{Z}$ вида (3) является набором зашумлённых кодовых слов кода $\mathcal{D}^{(i)}$, размер $N/2$ выборки $\widetilde{Z}$ должен удовлетворять условию

$$N/2 \geqslant \max_{h \in \mathcal{H}_i} \{M(h, \alpha, \beta, (1-\Delta^2)/2)\},$$

где $\mathcal{H}_i$ — базис кода ${\mathcal{D}^{(i)}}^\perp$, состоящий из векторов малого веса.

Таким образом, для определения позиции q неизвестного сообщения m потребуется перехватить не менее $N_1 = 2\max\limits_i \max\limits_{h\in\mathcal{H}_i}\{M(h,\alpha,\beta,(1-\Delta^2)/2)\}$ зашумлённых кодовых сообщений, где $i \in \{1,\ldots,k-l+1\}$.

Пусть $q = i$ — определённая позиция сообщения m после наблюдения N_1 зашумлённых кодовых слов. Чтобы оценить необходимый объём выборки для восстановления сообщения m, используем метод восстановления фиксированного сообщения при кодовом зашумлении; метод описан в [3]. Если гипотеза H_i верная, то для применения этого метода нужно использовать выборку (2). Пусть N_2 — необходимое число перехватов для восстановления исходного сообщения m по выборке (2). Тогда минимальное число перехватов зашумлённых кодовых слов, необходимое для восстановления исходного сообщения m, равно $\max(N_1, N_2)$.

ЛИТЕРАТУРА

1. *Wyner A. D.* The wire-tap channel // Bell Sys. Tech. J. 1975. V. 54. P. 1355–1387.
2. *Коржик В. И., Яковлев В. А.* Неасимптотические оценки эффективности кодового зашумления одного канала // Пробл. передачи информ. 1981. Т. 17. № 4 С. 11–18.
3. *Иванов В. А.* Статистические методы оценки эффективности кодового зашумления // Труды по дискретной математике. 2002. Т. 6. С. 48–63.
4. *Chabot C.* Recognition of a code in a noisy environment // Proc. IEEE ISIT, June 2007. P. 2211–2215.
5. *Yardi A. D. and Vijayakumaran S.* Detecting linear block codes in noise using the GLRT // Proc. IEEE Intern. Conf. Communications (ICC), Budapest, Hungary, June 9–13, 2013. P. 4895–4899.

УДК 519.6 DOI 10.17223/2226308X/9/23

О ТОЧНОСТИ МАТРИЧНО-ГРАФОВОГО ПОДХОДА К ОЦЕНКЕ ПЕРЕМЕШИВАЮЩИХ СВОЙСТВ ПРЕОБРАЗОВАНИЙ

С. Н. Кяжин, Ф. В. Лебедев

Приведены экспериментальные результаты оценки точности матрично-графового подхода к исследованию перемешивающих свойств нелинейных преобразований. В качестве класса преобразований, для которого проводилась оценка, взяты все преобразования множества V_n двоичных n-мерных векторов, перемешивающий граф которых есть n-вершинный граф Виландта, а также раундовые подстановки алгоритмов блочного шифрования AES, «Кузнечик» и «Магма» (ГОСТ 28147-89). Установлено, что полученные при матрично-графовом подходе оценки точны для 25 % преобразований с перемешивающим графом Виландта ($n = 9, 10, 11$), а также для раундовой подстановки алгоритмов AES и «Кузнечик». Указанные оценки не являются точными для раундовых подстановок алгоритма «Магма» и для 75 % преобразований с перемешивающим графом Виландта.

Ключевые слова: *перемешивающие свойства, матрично-графовый подход, граф Виландта, AES, «Кузнечик», «Магма».*

Введение

Для оценки перемешивающих свойств с помощью композиции преобразований используют оценочный матрично-графовый подход [1, гл. 10]. Начиная с 2010 г., в журнале «Прикладная дискретная математика» опубликован ряд теоретических и прикладных работ, развивающих данный подход (обзор результатов до 2012 г. см. в [2]).

Перемешивающим графом преобразования g множества X^n называется n-вершинный орграф $\Gamma(g)$, где пара вершин (i,j) образует дугу в $\Gamma(g)$, если и только если i является существенной переменной координатной функции g_j. Матрица $M(g)$ смежности вершин графа $\Gamma(g)$ называется перемешивающей матрицей преобразования g. Преобразование называется совершенным, если все координатные функции зависят от всех переменных.

Многие криптографические функции, например алгоритмы блочного шифрования, являются итеративными (реализуется степень некоторого преобразования g), то есть перемешивающей матрицей реализуемой функции является $M(g^i)$, $i \in \mathbb{N}$. В общем случае $(M(g))^i \geqslant M(g^i)$, $i \in \mathbb{N}$. Следовательно, если матрица $(M(g))^i$ не положительна, то преобразование g^i не совершенно, $i \in \mathbb{N}$ [1, гл. 10]. На данном утверждении основан матрично-графовый подход к исследованию перемешивающих свойств, задача которого — определить наименьшее натуральное k, при котором $(M(g))^k > 0$ (такое k называется экспонентом матрицы $M(g)$, обозначается $\exp M(g)$). Вместо матрицы $(M(g))^i$ равносильно рассматривать её носитель — матрицу, в которой все положительные элементы заменены на 1. Точность матрично-графового подхода определяется различием матриц $(M(g))^i$ и $M(g^i)$, $i \in \mathbb{N}$.

В работе приведены результаты экспериментального исследования точности матрично-графового подхода для преобразований с перемешивающим графом Виландта (класс графов Виландта введён в [3]) и для раундовых подстановок ряда блочных шифров.

1. Точность матрично-графового подхода к оценке перемешивающих свойств нелинейных преобразований с перемешивающим графом Виландта

Обозначим через $G_W(n)$ множество всех нелинейных преобразований множества V_n вида $g = g' \oplus \alpha$ с перемешивающим графом Виландта, где $\alpha \in V_n$ и преобразование $g' : V_n \to V_n$ задано системой координатных функций:

$$g' = \{g_1(x_n), g_2(x_1), g_3(x_2), \ldots, g_{n-1}(x_{n-2}), g_n(x_{n-2}, x_{n-1})\}.$$

По результатам вычислительного эксперимента множество $G_W(10)$ разбивается на равномощные классы G_1, G_2, G_3, G_4. Каждому классу однозначно соответствует последовательность значений $d_{\mathrm{H}}((M(g))^i, M(g^i))$, $i = 2, \ldots, 100$, где $d_{\mathrm{H}}(M_1, M_2)$ — расстояние Хэмминга между матрицами M_1, M_2, определяемое как количество различных элементов. В табл. 1 приведены условия распределения преобразований по классам.

Таблица 1

$g_{10} = x_8x_9$ или $g_{10} = x_8x_9 \oplus x_8 \oplus x_9$	$g_{10} = x_8x_9 \oplus x_9$	$g_{10} = x_8x_9 \oplus x_8$	Условия принадлежности классам
G_1	G_3	G_2	$\|\alpha\|$ нечётный, $\alpha_9 = 0$
G_2	G_4	G_1	$\|\alpha\|$ чётный, $\alpha_9 = 1$
G_3	G_1	G_4	$\|\alpha\|$ нечётный, $\alpha_9 = 1$
G_4	G_2	G_3	$\|\alpha\|$ чётный, $\alpha_9 = 0$

Для преобразований $g \in \{G_1, G_2, G_3\}$ выполнено $(M(g))^k \neq M(g^k)$, начиная с некоторого $k \in \mathbb{N}$. Для преобразования $g \in G_4$ для любого $i \in \mathbb{N}$ выполнено равенство $(M(g))^i = M(g^i)$. При $n = 9, 11$ наблюдается аналогичное разбиение, что позволяет выдвинуть гипотезу о подобном разбиении данного множества преобразований на классы при любом $n > 2$.

Для преобразований $g \in G_W(n)$ выполнены свойства, связанные с перемешиванием.

Утверждение 1. Пусть полугрупповое преобразование $g \in G_W(n)$ имеет тип (d, m), $\gamma = \exp M(g)$. Если $d + m < \gamma$, то существует такое $i \in \mathbb{N}$, что $(M(g))^i > M(g^i)$.

Утверждение 2. Для любого $g \in G_W(n)$ найдётся такой вектор $\alpha \in V_n$, что для любого $i \in \mathbb{N}$ преобразование $(g \oplus \alpha)^i$ не является совершенным.

2. Точность матрично-графового подхода к оценке перемешивающих свойств раундовых подстановок шифров AES, «Кузнечик» и «Магма»

Пусть g_1, g_2 — раундовые подстановки алгоритмов блочного шифрования AES [4] и «Кузнечик» [5] соответственно, построенных на основе SP-сетей. Для $g \in \{g_1, g_2\}$ экспериментально определено, что $M(g^k) = (M(g))^k$ для $k = 2, \ldots, h$, где h — число раундов шифрования алгоритма ($h \in \{10, 12, 14\}$ при $g = g_1$, $h = 9$ при $g = g_2$).

Для алгоритма «Магма» [5], построенного на основе сети Фейстеля, матрично-графовый подход не является точным. В табл. 2 для раундовой подстановки g показана зависимость границы k, при которой $d_{\mathrm{H}}(M(g^i), (M(g))^i) = 0$ для $i \geqslant k$, от числа нулевых младших битов раундового ключа при условии, что все раундовые ключи равны.

Таблица 2

Число нулевых младших битов ключа	$\exp M(g)$	Значения k
0, …, 16	3	6
17, …, 20	3	7
21, …, 32	4	8

Выводы

Результаты оценочного матрично-графового подхода к исследованию перемешивающих свойств преобразований для некоторых преобразований абсолютно точны (для 25 % преобразований из множества $G_W(n)$, $n = 9, 10, 11$). Для многих других преобразований оценки не точны, но могут считаться практически приемлемыми.

Направление дальнейших исследований перемешивающих свойств преобразований следует увязать с глубоким изучением их алгебраических и комбинаторных свойств.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. FIPS PUB 197. Advanced Encryption Standard. NIST, 2001. 47 p.
5. ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015. 25 с.

УДК 519.1 DOI 10.17223/2226308X/9/24

ПЕРЕМЕШИВАЮЩИЕ СВОЙСТВА ДВУХКАСКАДНЫХ ГЕНЕРАТОРОВ

С. Н. Кяжин, В. М. Фомичев

С помощью матрично-графового подхода оценены перемешивающие свойства двухкаскадных генераторов: на основе последовательного соединения регистров сдвига; генераторов 1-2 шага; с перемежающимся шагом. Получены условия локальной примитивности (квазипримитивности) перемешивающих графов генераторов и верхние оценки соответствующих локальных экспонентов (квазиэкспонентов), которые при многих значениях параметров близки по порядку к сумме длин регистров генератора.

Ключевые слова: *регистр сдвига, генератор 1-2 шага, генератор с перемежающимся шагом, локальная примитивность, локальный экспонент.*

Введение

Важным свойством генератора гаммы является зависимость знаков гаммы γ_i от всех знаков начального состояния при $i > i_0$, где i_0 определяет длину холостого хода генератора. Для этого свойства необходима примитивность (локальная примитивность) перемешивающего графа преобразования множества состояний генератора.

Пусть $N_n = \{1, \ldots, n\}$; $I, J \subseteq N_n$, $I \neq \varnothing$, $J \neq \varnothing$; M — 0,1-матрица порядка $n{>}1$; $M(I \times J)$ — её подматрица размера $|I| \times |J|$, полученная из M удалением строк с номерами $i \notin I$ и столбцов с номерами $j \notin J$. Матрица M называется примитивной ($I \times J$-примитивной), если существует такое натуральное число γ, что $M^t > 0$ ($M^t(I \times J) > 0$) при любом $t \geqslant \gamma$. Наименьшее такое γ называется экспонентом ($I \times J$-экспонентом) матрицы M, обозначается $\exp M$ ($I \times J$-$\exp M$).

Матрица M называется $I \times J$-квазипримитивной, если при некотором натуральном δ подматрица $M^t(I \times J)$ не имеет нулевых строк для любого $t \geqslant \delta$. Наименьшее такое δ называется $I \times J$-квазиэкспонентом матрицы M, обозначается $I \times J$-$\mathrm{qexp}\, M$.

Под примитивностью ($I \times J$-примитивностью, $I \times J$-квазипримитивностью) орграфа Γ понимается соответствующее свойство его матрицы смежности M, при этом соответствующие экспоненты и локальные экспоненты орграфа Γ и матрицы M равны.

Цель работы — применить ранее полученные условия примитивности [1, с. 226] и локальной примитивности [2] орграфов для оценки перемешивающих свойств некоторых двухкаскадных генераторов.

Обозначим: V_r — множество двоичных r-мерных векторов; $S(f)$ — множество номеров существенных переменных функции f; s — сумма длин регистров генератора, $(x_1, \ldots, x_s)$ — начальное состояние регистров, m, n, r — длины регистров (m — управляющего, n, r — генерирующих), $m, n, r > 1$; h — преобразование множества V_s состояний генератора; h_i^t — i-я координатная функция преобразования h^t, $i = 1, \ldots, s$; $\Gamma(h)$ — перемешивающий s-вершинный орграф преобразования h; γ_t — t-й знак гаммы, $t = 1, 2, \ldots$

1. Последовательное соединение регистров сдвига

Пусть генератор построен на основе последовательного соединения двоичных регистров правого сдвига длины m и n с булевыми функциями обратной связи $f_1(x_1, \ldots, x_m)$ и $f_2(x_{m+1}, \ldots, x_{m+n})$ соответственно. Положим $S(f_1) = \{b_1, \ldots, b_\nu\}$,

$S(f_2) = \{c_1, \ldots, c_\mu\}$, где $1 \leqslant b_1 < \ldots < b_\nu = m$, $m+1 \leqslant c_1 < \ldots < c_\mu = m+n$, НОД$(b_1, \ldots, b_\nu) = d_1$, НОД$(c_1 - m, \ldots, c_\mu - m) = d_2$.

Уравнения гаммообразования: $\gamma_t = h^t_{m+n}(x_1, \ldots, x_{m+n})$. Таким образом, для анализа свойств гаммы генератора представляет интерес величина $N_{m+n} \times \{m+n\}$-exp $\Gamma(h)$.

Утверждение 1. Орграф $\Gamma(h)$ является $N_{m+n} \times \{m+n\}$-примитивным, если и только если $d_2 = 1$, в этом случае

$$N_{m+n} \times \{m+n\}\text{-exp}\,\Gamma(h) \leqslant n + \max\{m, \rho_2\} + g(c_1 - m, \ldots, c_\mu - m),$$

где $\rho_2 = \max\limits_{l=1,\ldots,\mu} \{c_l - c_{l-1}\}$; $c_0 = m$.

Следствие 1. Если $c_1 = m+1$, то $\Gamma(h)$ является $N_{m+n} \times \{m+n\}$-примитивным и $N_{m+n} \times \{m+n\}$-exp $\Gamma(h) = n - 1 + \max\{m, \rho_2\}$.

Утверждение 2. Орграф $\Gamma(h)$ является $N_m \times \{m+n\}$-примитивным, если и только если $(d_1, d_2) = 1$, в этом случае

$$N_m \times \{m+n\}\text{-exp}\,\Gamma(h) \leqslant \rho_1 + m + n + g(b_1, \ldots, b_\nu, c_1 - m, \ldots, c_\mu - m),$$

где $\rho_1 = \max\limits_{l=1,\ldots,\nu} \{b_l - b_{l-1}\}$; $b_0 = 1$.

Следствие 2. Если $c_1 = m+1$, то $\Gamma(h)$ является $N_m \times \{m+n\}$-примитивным и $N_m \times \{m+n\}$-exp $\Gamma(h) = m + n - 1$.

2. Генератор 1-2 шага

Генератор 1-2 шага построен на основе управляющего и генерирующего линейных регистров сдвига (ЛРС) длины m и n. Преобразование h нелинейное в силу неравномерности движения генерирующего регистра, определяемого управляющей функцией $u(x_1, \ldots, x_m)$.

Пусть управляющий и генерирующий регистры правого сдвига имеют соответственно длины $m > 2$ и $n > 2$ и функции обратной связи $f_{\text{у}}(x_1, \ldots, x_m)$ и $f_{\text{г}}(x_{m+1}, \ldots, x_{m+n})$. Положим $S(f_{\text{у}}) = \{b_1, \ldots, b_\nu\}$, $S(f_{\text{г}}) = \{c_1, \ldots, c_\mu\}$, где $1 \leqslant b_1 < \ldots < b_\nu = m$, $m+1 \leqslant c_1 < \ldots < c_\mu = m+n$.

Уравнения гаммообразования имеют вид $\gamma_t = h^t_{m+n}(x_1, \ldots, x_{m+n})$. Оценим величину $N_{m+n} \times \{m+n\}$-exp $\Gamma(h)$, важную для анализа гаммы генератора.

Утверждение 3. Граф $\Gamma(h)$ является $N_{m+n} \times \{m+n\}$-примитивным и

$$N_{m+n} \times \{m+n\}\text{-exp}\,\Gamma(h) = \max\{m, \rho\} + \lambda(\lambda - 1) + \lceil n/2 \rceil, \tag{1}$$

где $\lambda = \lceil (c_1 - m)/2 \rceil$; $\rho = \max\{\lceil (c_2 - c_1)/2 \rceil, \ldots, \lceil (c_\mu - c_{\mu-1})/2 \rceil\}$.

Следствие 3. Граф $\Gamma(h)$ является $N_m \times \{m+n\}$-примитивным и

$$N_m \times \{m+n\}\text{-exp}\,\Gamma(h) = m + \lambda(\lambda - 1) + \lceil n/2 \rceil. \tag{2}$$

Приведём числовые примеры. Пусть $m = 7$, $n = 20$, $S(u) = \{m\}$.

При $S(f_{\text{г}}) = \{m+n-1, m+n\}$ выполнено $\lambda = \lceil (n-1)/2 \rceil = 10$, $\rho = 1$. Тогда из (1) и (2) следует: $N_7 \times \{27\}$-exp $\Gamma(h) = N_{27} \times \{27\}$-exp $\Gamma(h) = 107$.

При $S(f_{\text{г}}) = \{m+2, m+n\}$ выполнено $\lambda = 1$, $\rho = \lceil (n-2)/2 \rceil = 9$. Тогда из (1) и (2) следует: $N_7 \times \{27\}$-exp $\Gamma(h) = 17$, $N_{27} \times \{27\}$-exp $\Gamma(h) = 19$.

3. Генератор с перемежающимся шагом

Генератор с перемежающимся шагом построен на базе двоичных ЛРС: управляющего ЛРС длины m и двух генерирующих ЛРС длины n и r с функциями обратной связи $f_{\text{у}}(x_1,\dots,x_m)$, $f_1(x_{m+1},\dots,x_{m+n})$ и $f_2(x_{m+n+1},\dots,x_{m+n+r})$ соответственно. В зависимости от знака управления сдвигается информация либо в первом, либо во втором генерирующем ЛРС, в силу чего преобразование h генератора нелинейное.

Пусть $J_1=\{m+1,\dots,m+n\}$, $J_2=\{m+n+1,\dots,m+n+r\}$, $S(f_{\text{у}})=\{b_1,\dots,b_\nu\}$, $S(f_1)=\{c_1,\dots,c_\mu\}$, $S(f_2)=\{d_1,\dots,d_\sigma\}$, где $1\leqslant b_1<\ldots<b_\nu=m$, $m+1\leqslant c_1<\ldots<c_\mu=m+n$ и $m+n+1\leqslant d_1<\ldots<d_\sigma=m+n+r$.

Уравнения гаммообразования имеют вид:

$$\gamma_t=h^t_{m+n}(x1,\dots,xm+n)\oplus h^t_{m+n+r}(x_1,\dots,x_m,x_{m+n+1},\dots,x_{m+n+r}).$$

Таким образом, для анализа свойств гаммы генератора представляют интерес величины $N_{m+n+r}\times\{m+n,m+n+r\}$-$\exp\Gamma(h)$ и $N_{m+n+r}\times\{m+n,m+n+r\}$-$\operatorname{qexp}\Gamma(h)$.

Утверждение 4. Граф $\Gamma(h)$ является:

а) $N_m\times\{m+n,m+n+r\}$-, $(N_m\cup J_1)\times\{m+n\}$- и $(N_m\cup J_2)\times\{m+n+r\}$-примитивным, при этом

$$\begin{gathered}N_m\times\{m+n,m+n+r\}\text{-}\exp\Gamma(h)=m+\max\{n,r\}-1,\\ N_m\times\{m+n,m+n+r\}\text{-}\operatorname{qexp}\Gamma(h)=m+\min\{n,r\}-1,\\ \delta_1=(N_m\cup J_1)\times\{m+n\}\text{-}\exp\Gamma(h)=m+n-1,\\ \delta_2=(N_m\cup J_2)\times\{m+n+r\}\text{-}\exp\Gamma(h)=m+r-1;\end{gathered}$$

б) не $N_{m+n+r}\times\{m+n,m+n+r\}$-примитивным, но $N_{m+n+r}\times\{m+n,m+n+r\}$-квазипримитивным, и

$$N_{m+n+r}\times\{m+n,m+n+r\}\text{-}\operatorname{qexp}\Gamma(h)=\max\{\min\{\delta_1,\delta_2\},n-1,r-1\}.$$

ЛИТЕРАТУРА

1. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/9/25

АНАЛОГИ ТЕОРЕМЫ ШЕННОНА ДЛЯ ЭНДОМОРФНЫХ НЕМИНИМАЛЬНЫХ ШИФРОВ

Н. В. Медведева, С. С. Титов

Рассматриваются некоторые аналоги теоремы Шеннона для эндоморфных совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров. Построены примеры минимальных по включению совершенных и транзитивных шифров.

Ключевые слова: *совершенные шифры, эндоморфные шифры, неминимальные шифры.*

В основе изучения совершенных шифров лежит математическая модель шифра. 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 $\lambda > 1$, $\mu \geqslant \lambda$. Это означает, что открытые и шифрованные тексты представляются словами (ℓ-граммами, $\ell \geqslant 1$) в алфавитах X и Y соответственно. Согласно [2, 3], под *шифром* Σ_B будем понимать совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей. Шифры, для которых апостериорные вероятности открытых текстов совпадают с их априорными вероятностями, называются *совершенными*. В работе [1] полностью описаны *эндоморфные* ($|X| = |Y|$) совершенные шифры с минимально возможным числом ключей ($|K| = |Y|$). Согласно теореме К. Шеннона [1], эндоморфные совершенные шифры с минимально возможным числом ключей исчерпываются шифрами табличного гаммирования со случайной равновероятной гаммой.

Существование неэндоморфных ($|X| < |Y|$) шифров [3, пример 2.2.10], а также шифров, минимальных не по числу ключей, а по включению (т. е. шифров, содержащих минимально возможное множество ключей зашифрования с ненулевыми вероятностями), оправдывает получение аналогов (обобщений) теоремы Шеннона для других совершенных шифров. К этому также приводит и задача изучения минимальных (по включению) транзитивных шифров, так как совершенный шифр является транзитивным. Допускает обобщение и само понятие совершенного по Шеннону шифра, что подтверждается изучением современных аналогов совершенных шифров [3].

В данной работе для обобщений теоремы Шеннона и построения примеров шифров используется вероятностная модель Σ_B, в которой, согласно подходу [2, 3], шифр задаётся распределением вероятностей ключей при $\ell = 1$.

Для эндоморфного ($\lambda = \mu$) шифра перечисляются в некотором порядке все возможные $\pi = \lambda!$ подстановок зашифрования, соответствующих ключам $k \in K$ и определённым им вероятностям P_k ключей. При этом допускается, что некоторые вероятности P_k могут быть равны нулю — это означает, что соответствующая подстановка не используется в данном шифре. Получившийся π-мерный набор P вероятностей P_k ключей будем рассматривать как точку π-мерного пространства $\mathbb{R}^\pi$. Распределение биграмм, триграмм и т. д. может задаваться распределениями вероятностей при $\ell = 2, 3, \ldots$

Задача описания шифров в вероятностной модели Σ_B приводит к описанию множества точек в пространстве $\mathbb{R}^\pi$, которые являются распределениями вероятностей ключей того или иного шифра. В работах [4–6] описано множество (полиэдр) матриц вероятностей ключей и множество вероятностей шифробозначений неэндоморфных совершенных шифров в случае, когда мощность λ множества шифрвеличин равна двум.

По теореме Шеннона, минимальные по числу ключей эндоморфные совершенные шифры соответствуют тем точкам пространства $\mathbb{R}^\pi$, у которых все координаты равны нулю, кроме λ ненулевых координат, равных $1/\lambda$, а сам набор координат соответствует набору ключей (подстановок), образующих латинский квадрат. Поскольку множество точек пространства $\mathbb{R}^\pi$, соответствующих совершенным шифрам, образует выпуклое множество (полиэдр), то и выпуклая оболочка этих точек также соответствует совершенным шифрам. Возникает вопрос: будет ли полученный таким образом полиэдр множеством распределений всех эндоморфных совершенных шифров?

Для $\lambda = \mu \in \{2, 3\}$ ответ положительный. При $\lambda = \mu = 2$ — это классический шифр Вернама со сложением по модулю 2. При $\lambda = \mu = 3$ и $K = \{k_1, k_2, \ldots, k_6\}$ имеем следующую таблицу зашифрования со всеми $\pi = 3! = 6$ подстановками из

$X = \{x_1, x_2, x_3\}$ в $Y = \{1, 2, 3\}$, в которой точки $\mathsf{P}^{(1)}$ и $\mathsf{P}^{(2)}$ соответствуют латинским квадратам (табл. 1).

Таблица 1

№	K	x_1	x_2	x_3	P_k	$\mathsf{P}_k^{(1)}$	$\mathsf{P}_k^{(2)}$
1	k_1	1	2	3	P_1	1/3	0
2	k_2	1	3	2	P_2	0	1/3
3	k_3	2	1	3	P_3	0	1/3
4	k_4	2	3	1	P_4	1/3	0
5	k_5	3	1	2	P_5	1/3	0
6	k_6	3	2	1	P_6	0	1/3

Утверждение 1. Любой эндоморфных совершенный шифр с мощностью множества шифрвеличин, равной трём, задаётся распределением вероятностей

$$\mathsf{P} = \alpha\,\mathsf{P}^{(1)} + \beta\,\mathsf{P}^{(2)} = \alpha\left(\frac{1}{3}, 0, 0, \frac{1}{3}, \frac{1}{3}, 0\right)^{\mathrm{T}} + \beta\left(0, \frac{1}{3}, \frac{1}{3}, 0, 0, \frac{1}{3}\right)^{\mathrm{T}} = \left(\frac{\alpha}{3}, \frac{\beta}{3}, \frac{\beta}{3}, \frac{\alpha}{3}, \frac{\alpha}{3}, \frac{\beta}{3}\right)^{\mathrm{T}},$$

$\alpha, \beta \geqslant 0$, $\alpha + \beta = 1$, лежащим в выпуклой оболочке точек $\mathsf{P}^{(1)}, \mathsf{P}^{(2)} \in \mathbb{R}^6$.

Это утверждение означает, что искомое выпуклое множество (полиэдр) — отрезок в шестимерном пространстве.

При $\lambda = \mu > 3$ выпуклая оболочка совершенных по Шеннону шифров с минимальным числом ключей является лишь частью множества точек, соответствующих совершенным шифрам. Например, при $\lambda = \mu = 4$ существуют минимальные (по включению) совершенные шифры, не содержащие в себе наборов ключей (подстановок), образующих латинский квадрат.

Пример 1. Рассмотрим эндоморфный шифр в случае, когда мощность множества шифрвеличин равна четырём. Пусть $X = \{x_1, x_2, x_3, x_4\}$ — множество шифрвеличин; $Y = \{1, 2, 3, 4\}$ — множество шифробозначений, $K = \{k_1, k_2, \ldots, k_\pi\}$ — множество ключей. Таблица зашифрования данного шифра, составленная из единичной и всех шести одноцикловых подстановок группы S_4, приведена в табл. 2.

Таблица 2

№	K	x_1	x_2	x_3	x_4	P_k
1	k_1	1	2	3	4	1/4
2	k_2	2	4	1	3	1/8
3	k_3	3	1	4	2	1/8
4	k_4	4	3	1	2	1/8
5	k_5	3	4	2	1	1/8
6	k_6	2	3	4	1	1/8
7	k_7	4	1	2	3	1/8

Это совершенный эндоморфный шифр. Здесь одноцикловые подстановки f группы S_4 обладают свойством: для каждой подстановки f имеется ровно четыре различных других одноцикловых подстановок g, таких, что $f(i) = g(i)$, $i = 1, 2, 3, 4$. Следовательно, максимальные четырехстолбцовые латинские прямоугольники в этой таблице состоят из трёх строк вида e, f, f^{-1} и латинских квадратов нет.

Пример 2. Рассмотрим таблицы зашифрования эндоморфных шифров при $\lambda = \mu = 4$ с произвольными вероятностями ключей (табл. 3 и 4).

Таблица 3

№	K	x_1	x_2	x_3	x_4
1	k_1	1	4	3	2
2	k_2	1	3	2	4
3	k_3	2	1	3	4
4	k_4	3	2	4	1
5	k_5	4	2	1	3

Таблица 4

№	K	x_1	x_2	x_3	x_4
1	k_1	4	1	2	3
2	k_2	3	4	1	2
3	k_3	2	3	4	1
4	k_4	1	2	4	3
5	k_5	4	1	3	2
6	k_6	2	3	1	4

Это минимальные (по включению) транзитивные шифры, которые не могут быть совершенными ни при каких распределениях вероятностей ключей, причём из их таблиц зашифрования невозможно извлечь латинский квадрат.

Таким образом, в работе рассмотрена задача обобщения теоремы Шеннона для эндоморфных совершенных шифров. Построены примеры, показывающие, что минимальность шифра по числу ключей и минимальность по включению приводят к разным постановкам задач.

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. *Медведева Н. В., Титов С. С.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.
5. *Медведева Н. В., Титов С. С.* Неэндоморфные совершенные шифры с двумя шифрвеличинами // Прикладная дискретная математика. Приложение. 2015. № 8. С. 63–66.
6. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.

УДК 519.1 DOI 10.17223/2226308X/9/26

О СПОСОБАХ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ С ЗАДАННЫМ ПОКАЗАТЕЛЕМ БЕСПОВТОРНОСТИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Д. А. Романько, В. М. Фомичев

В связи с понятием слабого ключа итеративного симметричного блочного шифра исследованы некоторые способы построения ключевого расписания, обеспечивающего отсутствие повторений в последовательности раундовых ключей. На основе генератора «1-2 шага», использующего линейные регистры сдвига длины n и m с максимальной длиной периода, построен автономный автомат с выходным алфавитом V_m, у которого при любом начальном состоянии отрезок длины 2^{m-1} выходной последовательности не содержит повторяющихся векторов.

Ключевые слова: *блочный шифр, раундовый ключ, r-бесповторная последовательность, r-бесповторный автомат, показатель бесповторности.*

Введение

При криптографическом анализе DES-алгоритма введено понятие слабого ключа, т. е. основного ключа, порождающего 16 одинаковых раундовых ключей. В [1, с. 298] для r-раундового блочного алгоритма использовано понятие μ-слабого ключа, порождающего ровно μ различных раундовых ключей, $1 \leqslant \mu < r$. Показано, что при определённых условиях использование слабых ключей ослабляет криптографические свойства итеративного блочного шифра. Поэтому представляет интерес задача построения ключевого расписания, генерирующего при любом основном ключе r различных раундовых ключей. Для решения применим теоретико-автоматный подход.

Основные обозначения:

— V_n — множество двоичных n-мерных векторов, $n \in \mathbb{N}$;
— $V_{n,0}$ — множество ненулевых двоичных n-мерных векторов, $n \in \mathbb{N}$;
— ЛРСmax-n — линейный регистр левого сдвига длины n максимального периода, $n \in \mathbb{N}$.

1. Бесповторность последовательностей и автономных автоматов

Пусть $X_{\to} = \{x_0, x_1, \ldots\}$ — конечная или бесконечная последовательность над X и $|X| = k$.

В последовательности $X_{\to}$ i-й r-граммой называется слово $(x_i, x_{i+1}, \ldots, x_{i+r-1})$ длины r в алфавите X, $i = 0, 1, 2, \ldots$; r-грамму назовём бесповторной, если она не содержит одинаковых символов. Последовательность r-грамм последовательности $X_{\to}$ обозначим $X^r_{\to}$.

Последовательность назовём r-бесповторной, если все её r-граммы бесповторные. Чисто периодическая последовательность $X_{\to}$ с длиной периода t является r-бесповторной, если бесповторными являются её i-е r-граммы при $i = 0, \ldots, t-1$.

Показателем бесповторности $X_{\to}$ (обозначение $\operatorname{urp} X_{\to}$) назовём наибольшее натуральное r, при котором последовательность $X_{\to}$ является r-бесповторной. Очевидно, $\operatorname{urp} X_{\to} \leqslant k$, и если последовательность $X_{\to}$ r-бесповторная, то она и r'-бесповторная при любом $r' \leqslant r$.

Автономный автомат $A = (S, Y, h, f)$, где S — множество состояний, Y — выходной алфавит, h — функция переходов, f — функция выходов, называется r-бесповторным, если при любом начальном состоянии A генерирует бесповторное выходное слово длины r. Показатель бесповторности инициального автомата A_s определим как показатель бесповторности выходной последовательности при начальном состоянии $s \in S$ и обозначим $\operatorname{urp} A_s$. Показателем бесповторности автомата A назовём $\operatorname{urp} A = \min\limits_{s \in S}\{\operatorname{urp} A_s\}$.

2. Примеры r-бесповторных автономных автоматов $A = (S, Y, h, f)$

1. Пусть $S = V_{n,0}$, $Y = V_r$, h — подстановка двоичного линейного регистра левого сдвига с примитивным характеристическим многочленом, $f(y_1, \ldots, y_n) = (y_1, \ldots, y_r)$, $r \geqslant n$. Автомат генерирует r-граммы линейной рекуррентной последовательности $X_{\to}$ (порядка n) максимального периода. Следовательно, $\operatorname{urp} X^r_{\to} = 2^n - 1$ при $r \geqslant n$.

2. Пусть $S = V_n$, $Y = V_r$, h — полноцикловая подстановка двоичного нелинейного регистра сдвига длины n, $f(y_1, \ldots, y_n) = (y_1, \ldots, y_r)$, $r \geqslant n$. Автомат генерирует r-граммы нормальной рекуррентной последовательности (де Брейна). Отсюда $\operatorname{urp} X^r_{\to} = 2^n$ при $r \geqslant n$.

Для построения ключевого расписания r-раундового блочного шифра без слабых ключей представляет интерес построение r-бесповторного автомата, где $\lambda > l \geqslant r$, $r \leqslant 32$ (здесь λ — длина основного бинарного ключа, l — длина раундовых бинарных ключей). Для построения такого автомата рассмотрим криптографический генератор «1-2 шага».

3. Криптографический генератор «1-2 шага»

Рассмотрим автономный автомат $A = (V_{n,0} \times V_{m,0}, V_{m,0}, h, \psi)$ с множеством состояний $V_{n,0} \times V_{m,0}$, выходным алфавитом $V_{m,0}$, функцией переходов h и функцией выходов ψ. При состоянии автомата $s = (y_1, \ldots, y_n, x_1, \ldots, x_m)$ выполнено $\psi(s) = (x_1, \ldots, x_m)$ и $h(s) = (\delta(y_1, \ldots, y_n), g^{a+1}(x_1, \ldots, x_m))$, где δ и g суть подстановки, реализуемые ЛРСmax-n и ЛРСmax-m соответственно, $a = f(y_1, \ldots, y_n)$, f — равновероятная булева функция, в простейшем случае $f(y_1, \ldots, y_n) = y_n$. Таким образом, «продвижение» генерирующего ЛРСmax-m в состоянии s равно $a + 1$, то есть 1 или 2 в зависимости от знака a, выработанного управляющим ЛРСmax-n. После $2^n - 1$ тактов «продвижение» генерирующего ЛРСmax-m равно $\tau = 2^n + 2^{n-1} - 1 - f(0, \ldots, 0)$ при любом начальном состоянии $s \in V_{n,0} \times V_{m,0}$.

Обозначим: $X_{\rightarrow}(s)$ — выходная последовательность автомата A при начальном состоянии s; $X_{\rightarrow}(s, t)$ — подпоследовательность последовательности $X_{\rightarrow}(s)$, составленная из первых t символов. Известно [1, с. 317], что длина периода последовательности $X_{\rightarrow}(s)$ равна $t = (2^n - 1)(2^m - 1)/\sigma$ при любом начальном состоянии s, где $\sigma = (\tau, 2^m - 1)$.

Теорема 1. При любом начальном состоянии s последовательность $X_{\rightarrow}(s, 2^{m-1})$ автомата A является бесповторной.

Справедливость теоремы следует из того, что $X_{\rightarrow}(s, 2^{m-1})$ есть бесповторная выборка (размера 2^{m-1}) с переменным шагом $1 - 2$ из периодического отрезка последовательности состояний ЛРСmax-m.

Отметим, что на основе автомата A можно построить ключевое расписание, удовлетворяющее указанным требованиям. Для этого следует положить: состояние s — основной ключ, длина основного бинарного ключа $\lambda = m + n$, длина раундовых бинарных ключей $l = m$, где $m > 5$. Тогда при любом числе раундов $r \leqslant 32$ выполнено условие бесповторности последовательности раундовых бинарных ключей. В частности, параметры ключевого расписания алгоритма DES достигаются при $m = 48$, $n = 8$, а параметры ключевого расписания алгоритма ГОСТ 28147-89 — при $m = 32$, $n = 224$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.

УДК 519.722 DOI 10.17223/2226308X/9/27

ПРИМЕНЕНИЕ ДВУЛИКИХ ПРОЦЕССОВ К ГЕНЕРИРОВАНИЮ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ[1]

Б. Я. Рябко

Описываются случайные процессы, у которых энтропия может быть сколь угодно близка к нулю, но при этом, как для полностью случайных последовательностей, частота встречаемости любого двоичного слова u стремится к $2^{-|u|}$, где $|u|$ — длина u. Это позволяет строить генераторы псевдослучайных чисел с доказанными свойствами, что представляет большой интерес для криптографических систем защиты информации.

Ключевые слова: *случайные числа, псевдослучайные числа, энтропия Шеннона.*

Генераторы случайных и псевдослучайных чисел (ГСЧ и ГПСЧ) находят широкое применение в системах защиты информации, причём используемые в таких системах генераторы должны удовлетворять целому ряду требований, одно из которых — статистическая неотличимость порождаемых генератором последовательностей от бернуллиевских с $p(0) = p(1) = 1/2$ [1]. С другой стороны, ГПСЧ по своему построению существенно отличаются от бернуллиевских процессов: энтропия (на символ) у выходной последовательности значительно меньше одного бита, тогда как у полностью случайной — один (см. описание схемы ГПСЧ, например, в [2, 3]). Напомним определение энтропии стационарного процесса μ: условная энтропия порядка m, $m = 1, 2, \ldots$, и (предельная) энтропия даются равенствами $h_m = -\sum\limits_{u\in\{0,1\}^{m-1}} \mu(u) \sum\limits_{v\in\{0,1\}} \mu(v/u) \log \mu(v/u)$, $h_\infty = \lim\limits_{m\to\infty} h_m$ [4].

В работе описываются процессы, для которых с вероятностью 1 в порождаемой последовательности $x_1 x_2 \ldots$ для каждого двоичного слова u выполняется равенство

$$\lim_{t\to\infty} \nu_t(u)/(t - |u|) = 2^{-|u|},$$

где $\nu_t(u)$ — число встреч слов u в последовательности $x_1 \ldots x_{|u|}$, $x_2 \ldots x_{|u|+1}, \ldots$, $x_{t-|u|+1} \ldots x_t$, что должно выполняться для полностью случайных последовательностей. Однако энтропия процесса может быть много меньше единицы, что обычно выполняется для ГПСЧ.

Сначала определим два семейства процессов $T_{k,\pi}$ и $\bar{T}_{k,\pi}$, где $k = 1, 2, \ldots$ и $\pi \in (0, 1)$ — параметры. Оба процесса — марковские цепи связности, или памяти k, которые генерируют буквы из алфавита $\{0, 1\}$. Определим их матрицы переходов по индукции: матрица для $T_{1,\pi}$ определяется равенствами $P_{T_{1,\pi}}(0/0) = \pi$, $P_{T_{1,\pi}}(0/1) = 1 - \pi$ (очевидно, $P_{T_{1,\pi}}(1/0) = 1 - \pi$, $P_{T_{1,\pi}}(1/1) = \pi$). Процесс $\bar{T}_{1,\pi}$ определяется равенствами $P_{\bar{T}_{1,\pi}}(0/0) = 1 - \pi$, $P_{\bar{T}_{1,\pi}}(0/1) = \pi$. Предположим теперь, что $T_{k,\pi}$ и $\bar{T}_{k,\pi}$ определены. Тогда $T_{k+1,\pi}$ и $\bar{T}_{k+1,\pi}$ определяются так:

$$P_{T_{k+1,\pi}}(0/0u) = P_{T_{k,\pi}}(0/u),\ P_{T_{k+1,\pi}}(1/0u) = P_{T(k,\pi)}(1/u),$$
$$P_{T(k+1,\pi)}(0/1u) = P_{\bar{T}(k,\pi)}(0/u),\ P_{T(k+1,\pi)}(1/1u) = P_{\bar{T}(k,\pi)}(1/u),$$

[1]Работа поддержана грантом РФФИ, проект № 15-29-07932.

и наоборот,

$$P_{\bar{T}(k+1,\pi)}(0/0u) = P_{\bar{T}(k,\pi)}(0/u),\ P_{\bar{T}(k+1,\pi)}(1/0u) = P_{\bar{T}(k,\pi)}(1/u),$$
$$P_{\bar{T}(k+1,\pi)}(0/1u) = P_{T(k,\pi)}(0/u),\ P_{\bar{T}(k+1,\pi)}(1/1u) = P_{T(k,\pi)}(1/u)$$

для каждого $u \in \{0,1\}^k$ (здесь vu — конкатенация слов v и u). Например,

$$P_{T(2,\pi)}(0/00) = \pi,\ P_{T(2,\pi)}(0/01) = 1-\pi,\ P_{T(2,\pi)}(0/10) = 1-\pi,\ P_{T(2,\pi)}(0/11) = \pi.$$

Будем считать, что начальное распределение равномерное на $\{0,1\}^k$, т. е. $P\{x_1 \dots x_k = u\} = 2^{-k}$ для $u \in \{0,1\}^k$.

Теорема 1. Пусть последовательность $x_1x_2\dots$ порождается процессом $T(k,\pi)$ (или $\bar{T}(k,\pi)$), $k \geqslant 1$ и u — двоичное слово длины k. Тогда

i) имеет место
$$P(x_{j+1} \dots x_{j+k} = u) = 2^{-|u|}; \tag{1}$$

ii) для каждого $\pi \in (0,1)$ энтропия h_k процессов $T(k,\pi)$ и $\bar{T}(k,\pi)$ равна 1 бит, тогда как предельная энтропия h_∞ равна $-(\pi \log_2 \pi + (1-\pi)\log_2(1-\pi))$.

Определение 1. Назовём случайный процесс *двуликим k-го порядка*, если для него выполняются свойства *i* и *ii*.

Поясним название «двуликие». Если мы рассматриваем слова длины, не превосходящей k, то они все равновероятны (энтропия равна 1), т. е. такие, какие должны быть у полностью случайного процесса. С другой стороны, если длина слова больше k, то энтропия меньше единицы, распределение вероятностей слов отличается от равномерного и процесс явно не «полностью случайный».

Рассмотрим на простом примере свойства этих процессов. Возьмём возможные типичные последовательности для $T(1,\pi)$ и $\bar{T}(1,\pi)$ для $\pi = 1/5$. Пусть последовательности такие: 010101101010100101 … и 000011111000111111000 … Каждая последовательность содержит примерно половину единиц и нулей и поэтому энтропия первого порядка равна 1, что должно выполняться для полностью случайной последовательности. С другой стороны, последовательности не выглядят как случайные, так как они содержат слишком длинные подпоследовательности вида 101010 … или 000 … 11111 … Поэтому энтропия второго и высших порядков меньше 1. Другими словами, данные последовательности имитируют полностью случайные, если учитываются только слова длины 1; при большей длине это не выполняется.

Следующая теорема показывает, что, в некотором смысле, двуликих процессов довольно много.

Теорема 2. Пусть $X = x_1x_2\dots$ и $Y = y_1y_2\dots$ — случайные процессы и процесс $Z = z_1z_2\dots$ задаётся равенствами $z_1 = x_1 \oplus y_1$, $z_2 = x_2 \oplus y_2$, … Тогда если X — двуликий процесс k-го порядка ($k \geqslant 1$), то Z тоже двуликий k-го порядка.

Двуликие процессы k-го порядка имитируют полностью случайные только при длине слова, не превосходящей k. Оказывается, существуют процессы, для которых это свойство выполняется для слов любой длины.

Теорема 3. Существуют процессы, для которых (1) выполняется для слов любой длины.

В работе показано, как на основе двуликих процессов могут быть построены ГСЧ и ГПСЧ с доказанными статистическими свойствами.

ЛИТЕРАТУРА

1. *Rukhin A., Soto J., Nechvatal J., et al.* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology, 2010.
2. *Barker E. and Kelsey D.* Recommendation for Random Bit Generator (RBG) Constructions (DRAFT NIST Special Publication 800-90C). National Institute of Standards and Technology, 2012.
3. *Рябко Б. Я., Фионов А. Н., Шокин Ю. И.* Криптография и стеганография в информационных технологиях. Новосибирск: Наука, 2015.
4. *Cover T. M. and Thomas J. A.* Elements of Information Theory. N.Y., USA: Wiley-Interscience, 2006.

УДК 519.1 DOI 10.17223/2226308X/9/28

О КЛЮЧЕВОМ РАСПИСАНИИ БЛОЧНЫХ ШИФРОВ БЕЗ СЛАБЫХ КЛЮЧЕЙ

В. М. Фомичев

Исследовано ключевое расписание симметричного r-раундового блочного шифра, при котором все раундовые ключи различны. Ключевое расписание реализуется как последовательное соединение автоматов: автономного автомата A, генерирующего выходную последовательность бинарных векторов с длиной периода не меньше r, и внутренне автономного автомата с постоянной памятью, в которой записан основной ключ блочного шифра. Рассмотрен пример, использующий в качестве автомата A линейный регистр сдвига с максимальной длиной периода.

Ключевые слова: *блочный шифр, раундовый ключ, бесповторная последовательность, показатель бесповторности последовательности.*

Введение

Используем следующие обозначения:
V_n — множество двоичных n-мерных векторов, $n \in \mathbb{N}$;
$X_{\to} = \{x_0, x_1, \ldots\}$ — последовательность над множеством X;
$\Gamma(A)$ — граф автомата Мили A;
$\langle H \rangle$ — линейная оболочка множества векторов H.

Свойства ключевого расписания, характеризующие взаимосвязи основного ключа с раундовыми ключами, являются определяющими при оценке стойкости итеративного блочного шифра (ИБШ) относительно ряда методов криптоанализа: согласования, дифференциального и др. Например, нежелательно ключевое расписание, при котором генерируемая из основного ключа последовательность раундовых ключей содержит определённое число повторяющихся элементов. Так, по отношению к основному ключу при криптографическом анализе DES-алгоритма введено понятие слабого ключа, то есть основного ключа, порождающего 16 одинаковых раундовых ключей. В [1, с. 298] для r-раундового блочного алгоритма это понятие обобщено до μ-слабого ключа, порождающего в наборе раундовых ключей $q_1, \ldots, q_r$ ровно μ различных элементов, $1 \leqslant \mu < r$. Показано, что при определённых условиях использование слабых ключей может привести к негативным последствиям с точки зрения обеспечения конфиденциальности данных. Криптографические свойства ИБШ считаются хорошими, если шифрующие подстановки близки по свойствам к случайным подстановкам, в частности, когда набор раундовых ключей $q_1, \ldots, q_r$ есть случайная бесповторная

выборка из множества двоичных векторов заданной размерности. В связи с этим возникает задача построения ключевого расписания, исключающего возможность повторений раундовых ключей в генерируемом наборе.

1. Постановка задачи

Рассмотрим ключевое расписание θ для итеративного r-раундового блочного алгоритма, $n, m, r \in \mathbb{N}$. Функция $\theta : V_n \to V_{mr}$ отображает основной n-битовый ключ $k = (k_1, \ldots, k_n)$ в набор m-битовых раундовых ключей $q_1, \ldots, q_r$. Функцию θ зададим системой координатных функций $\{\theta_1, \ldots, \theta_r\}$, где $\theta_i : V_n \to V_m$ отображает основной n-битовый ключ в раундовый ключ q_i, $i = 1, \ldots, r$. Обычно выполнены соотношения $m < n < mr$, при этих соотношениях функция θ не сюръективная и, следовательно, система функций $\{\theta_1, \ldots, \theta_r\}$ алгебраически зависимая.

Требуется построить функцию θ со свойством: при любом ключе $(k_1, \ldots, k_n) \in V_n$ набор $\theta_1(k_1, \ldots, k_n), \ldots, \theta_r(k_1, \ldots, k_n)$ состоит из r различных m-мерных векторов. Такую функцию θ назовем ключевым расписанием без слабых ключей. В [2] такая функция построена на основе генератора «1-2 шага».

2. Бесповторность последовательностей и автономных автоматов

Последовательности $X_\to = \{x_0, x_1, \ldots\}$ над конечным множеством X однозначно соответствует последовательность r-грамм $X^r_\to = \{(x_i, x_{i+1}, \ldots, x_{i+r-1})\}$, где $i = 0, 1, \ldots, l - r$ для конечной последовательности $X_\to$ длины $l > r$ и $i = 0, 1, 2, \ldots$, если $X_\to$ бесконечная. Назовём r-грамму $(x_0, x_1, \ldots, x_{r-1})$ *бесповторной*, если $x_i \neq x_j$ при $i \neq j$, $i, j \in 0, 1, \ldots, r - 1$. Последовательность $X_\to$ назовём *r-бесповторной*, если последовательность $X^r_\to$ состоит из бесповторных r-грамм (тогда $X_\to$ является ρ-бесповторной, где $1 \leqslant \rho \leqslant r$). *Показателем бесповторности* $X_\to$ (обозначается $\mathrm{urp}X_\to$) назовём наибольшее r, при котором $X_\to$ является r-бесповторной.

Из определений следует, что периодическая последовательность $X_\to$ с длиной периода t является r-бесповторной, если бесповторными являются r-граммы $(x_i, x_{i+1}, \ldots, x_{i+r-1})$, $i = 0, 1, \ldots, t - 1$.

Пусть $A = (S, Y, h, f)$ — перестановочный автономный автомат, где S, Y — соответственно внутренний и выходной алфавиты; $h : S \to S$ — биективная функция переходов; $f : S \to Y$ — функция выходов. Известно, что автомат A при начальном состоянии s_0, проходя периодическую последовательность состояний $\{s_0, s_1, \ldots, s_{\tau-1}\}$ с длиной периода τ, генерирует периодическую выходную последовательность $\{y_0, y_1, \ldots, y_{\tau-1}\}$ с длиной периода t, где t делит τ, $y_i = f(s_i)$, $i = 0, 1, \ldots$

Рассмотрим слабо инициальный автомат [1, с. 148] $(A, W) = ((S, W), Y, h, f)$, $\varnothing \neq W \subseteq S$, где W — множество допустимых начальных состояний автомата. В частности, при фиксированном начальном состоянии $s \in S$ имеем инициальный автомат (обозначаемый A_s).

Автомат A (автомат (A, W)) называется *r-бесповторным*, если r-бесповторной является выходная последовательность автомата при любом начальном состоянии $s \in S$ ($s \in W$). *Показателем бесповторности* автомата A (автомата (A, W), инициального автомата A_s) назовём наибольшее натуральное r, такое, что выходная последовательность автомата A является r-бесповторной при любом начальном состоянии $s \in S$ (при любом $s \in W$, при фиксированном $s \in S$). Обозначим показатели бесповторности автоматов A, (A, W) и A_s соответственно через $\mathrm{urp}A$, $\mathrm{urp}(A, W)$ и $\mathrm{urp}A_s$.

Утверждение 1.

а) $\mathrm{urp}A = \min\limits_{s\in S}\{\mathrm{urp}A_s\}$, $\mathrm{urp}(A, W) = \min\limits_{s\in W}\{\mathrm{urp}A_s\}$;

б) $\mathrm{urp}A_s$ не превышает длины периода выходной последовательности автомата A_s;

в) если состояния s и z принадлежат общему циклу графа автомата A, то $\mathrm{urp}A_s = \mathrm{urp}A_z$.

3. Схема ключевого расписания без слабых ключей

Пусть $p, m, u \in \mathbb{N}$, где $1 < p \leqslant u \leqslant r$. Обозначим $A = (V_p, V_u, h, f)$ — автономный автомат, где V_p — внутренний алфавит, V_u — выходной алфавит, $h : V_p \to V_p$ — функция переходов, $f : V_p \to V_u$ — функция выходов; $G = (V_u, V_{um}, V_m, \phi)$ — автомат с постоянной памятью [1, с. 148], т. е. внутренне автономный автомат с тождественной функцией переходов, где V_u — входной алфавит, V_{um} — внутренний алфавит, V_m — выходной алфавит. Определим функцию выходов $\phi : V_u \times Vu_m \to V_m$ — если в памяти автомата G записана система векторов $k^{(1)}, \ldots, k^{(u)}$ из V_m, то $\phi(\alpha, k^{(1)}, \ldots, k^{(u)}) = \alpha_1 k^{(1)} \oplus \ldots \oplus \alpha_u k^{(u)}$ при входном символе $\alpha = (\alpha_1, \ldots, \alpha_u) \in V_u$.

Рассмотрим последовательное соединение управляющего автономного автомата A и генерирующего автомата G, обозначаемое $A \to G$. Представим n-битовый секретный ключ k в виде набора m-битовых подключей: $k = (k^{(1)}, \ldots, k^{(u)})$.

Теорема 1. Если автомат A_s генерирует t-бесповторную периодическую последовательность с длиной периода t и в памяти автомата G записана линейно независимая система векторов $k^{(1)}, \ldots, k^{(u)}$, то автомат $(A \to G)_z$ генерирует при $z = (s, k^{(1)}, \ldots, k^{(u)})$ t-бесповторную периодическую последовательность с длиной периода t и $\mathrm{urp}(A \to G)_z = t$.

Доказательство. Выходная последовательность автомата $A \to G$ состоит из элементов линейной оболочки $\langle k^{(1)}, \ldots, k^{(u)}\rangle$. Если $\alpha, \beta \in V_u$ и $\alpha \neq \beta$, то $\phi(\alpha, k^{(1)}, \ldots, k^{(u)}) \neq \phi(\beta, k^{(1)}, \ldots, k^{(u)})$ в силу линейной независимости системы векторов $k^{(1)}, \ldots, k^{(u)}$. Тогда в силу t-бесповторности выходной последовательности автомата A_s последовательность $\{\phi(\alpha_i, k^{(1)}, \ldots, k^{(u)}) : i = 0, 1, \ldots, t-1\}$ состоит из различных векторов, то есть автомат $(A \to G)_z$ является t-бесповторным. Вместе с тем $\phi(\alpha_i, k^{(1)}, \ldots, k^{(u)}) = \phi(\alpha_{i+t}, k^{(1)}, \ldots, k^{(u)})$, $i = 0, 1, \ldots$, значит, $\mathrm{urp}(A \to G)_z = t$. ■

4. Выбор параметров ключевого расписания без слабых ключей

Рассмотрим данную схему в качестве альтернативы ключевому расписанию блочного шифра ГОСТ 28147-89. Параметры в этом случае принимают значения $p = u = 8$, $m = 32$. Автомат A построим на основе линейного регистра сдвига длины 8 с примитивным характеристическим многочленом, выходными символами являются 8-граммы (байты) линейной рекуррентной последовательности. Следовательно, автомат A генерирует 255-бесповторную последовательность байтов. В соответствии с теоремой 1 автомат $(A \to G)_z$ при любом ненулевом состоянии s автомата A и линейно независимой системе векторов $k^{(1)}, \ldots, k^{(8)}$ генерирует 255-бесповторную периодическую последовательность 32-битовых векторов с длиной периода 255 и $\mathrm{urp}(A \to G)_z = 255$.

Для ключевого расписания без слабых ключей 32-раундового блочного шифра достаточно взять любую бесповторную выборку размера 32 из выходной последовательности автомата $(A \to G)_z$, полученную при любом ненулевом состоянии s автомата A.

Ограничение на секретный ключ, связанное с линейной независимостью векторов, не является сильным. Если векторы $k^{(1)}, \ldots, k^{(8)}$ выбраны случайно равновероятно

из V_{32}, то вероятность линейной независимости системы равна $\prod_{i=0}^{7}(1-2^{i-32})$, то есть превышает $1-2^{24}$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Романько Д. А., Фомичев В. М.* О способах построения криптографических генераторов с заданным показателем бесповторности выходных последовательностей // Прикладная дискретная математика. Приложение. 2016. № 9. С. 65–67.

УДК 004.056.55 DOI 10.17223/2226308X/9/29

КРИПТОАНАЛИЗ КРИПТОСИСТЕМЫ МАК-ЭЛИСА, ПОСТРОЕННОЙ НА $(k-1)$-ПОДКОДАХ КОДА РИДА — МАЛЛЕРА

И. В. Чижов, М. А. Бородин

Описаны два вида криптосистем Мак-Элиса, построенных на подкодах кода Рида — Маллера. Изучен вопрос эквивалентных ключей для этих криптосистем. Получен результат о сводимости одной криптосистемы к другой. Приведены алгоритмы, которые позволяют применить атаку Чижова — Бородина к рассматриваемым криптосистемам для некоторых параметров кодов Рида — Маллера.

Ключевые слова: *криптосистема Мак-Элиса, подкоды Рида — Маллера, автоморфизмы кодов Рида — Маллера, произведение Шура, квадрат кода.*

Криптосистема Мак-Элиса предложена в 1978 г. Р. Дж. Мак-Элисом. Её стойкость основана на предположении сложности декодирования кода общего положения. Оригинальная криптосистема Мак-Элиса строится на двоичных кодах Гоппы. Для повышения эксплуатационных характеристик В. М. Сидельников предложил использовать коды Рида — Маллера [1]. Однако в 2007 г. Л. Миндера и А. Шокроллахи предложили достаточно эффективную атаку на такую криптосистему [2]. Кроме того, в 2013 г. Бородин и Чижов ещё больше понизили стойкость этой криптосистемы, а также построили полиномиальную атаку в случае использования кода Рида — Маллера $RM(r,m)$ с такими параметрами, что $(r, m-1)=1$ [3].

Бывает, что атаки на кодовые криптосистемы, работающие в случае использования полного кода, оказываются бесполезными в случае использования некоторых подкодов кода. Так была предложена криптосистема Бергера — Луадро, построенная на подкодах кода Рида — Соломона. В работе рассматриваются два аналога криптосистемы Бергера — Луадро, построенных на $(k-1)$-подкодах кода Рида — Маллера $RM(r,m)$.

Пусть V_n — множество всех двоичных векторов длины n. Известно, что с каждой булевой функцией $f(x_1,x_2,\ldots,x_m) : V_m \to V_1$ можно связать вектор значений $\Omega_f = (f(0,0,\ldots,0), f(0,0,\ldots,1),\ldots,f(1,1,\ldots,1))$. В дальнейшем не будем делать различий в обозначениях между булевой функцией и её вектором значений. Каждая булева функция может быть представлена полиномом Жегалкина: $f(x_1,x_2,\ldots,x_m) = \bigoplus_{u=(u_1,u_2,\ldots,u_m)\in V_m} g_f(u)x^u$, здесь $x^u = x_1^{u_1}x_2^{u_2}\ldots x_m^{u_m}$ и $x_i^{u_i} = x_i$, если $u_i = 1$, и $x_i^{u_i} = 1$, если $u_i = 0$, а $g_f(u)$ — некоторая булева функция.

Определение 1. Степенью булевой функции называется наименьшее целое положительное число d, такое, что $g_f(u) = 0$ для всех u веса больше d, т. е. $\mathrm{wt}(u) > d$.

Определение 2. Кодом Рида — Маллера $RM(r,m)$ называется множество всех векторов значений булевых функций от m переменных, степень которых не превосходит r.

Базисом кода являются все мономы степени r от m переменных:

$$1,\ x_1,\ \ldots,\ x_{m-1},\ x_1x_2,\ \ldots,\ x_{m-1}x_m,\ \ldots,\ x_1x_2\cdots x_r,\ \ldots,\ x_{m-r-1}\cdots x_m. \qquad (1)$$

Для двоичного набора $\alpha = (\alpha_{m-1},\ldots,\alpha_0)$ символом $|\alpha|$ обозначим представление двоичной строки в виде десятичного числа α, т. е. $|\alpha| = \alpha_0 + 2\alpha_1 + \ldots + 2^{m-1}\alpha_{m-1}$. Введём отношение порядка для векторов $\alpha, \beta \in V_m$. Будем считать, что $\alpha < \beta$, если либо $\mathrm{wt}(\alpha) < \mathrm{wt}(\beta)$, либо $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta)$ и $|\alpha| < |\beta|$. Тогда можно ввести отношение порядка на множестве мономов: $x^\alpha < x^\beta$, если $\alpha < \beta$.

Определение 3. Стандартной формой порождающей матрицы кода $RM(r,m)$ будем называть матрицу, составленную из всех векторов значений мономов (1), стоящих в порядке возрастания.

Обозначим также символом $\mathbf{A}(r,m)$ множество всех таких наборов $\alpha = (\alpha_{m-1}, \ldots,\alpha_0)$, что моном x^α входит в стандартную форму порождающей матрицы кода $RM(r,m)$.

Устройство криптосистемы первого типа $McElRM1(r,m)$. Для генерации ключей строится стандартная форма порождающей матрицы R кода $RM(r,m)$. Далее выбирается случайная двоичная невырожденная $(k\times n)$-матрица $H = (h_{ij})$ и случайная подстановка $\sigma \in S_n$, представленная в виде перестановочной $(n\times n)$-матрицы P_σ. Затем вычисляется матрица $G' = H\cdot R\cdot P_\sigma = H\cdot R^\sigma$ и из неё удаляется первая строка, получается $((k-1)\times n)$-матрица G. *Секретным ключом* криптосистемы является набор $(H, P_\sigma) = (H,\sigma)$, а *открытым ключом* — матрица G и (r,m) — параметры кода Рида — Маллера, однако, ради удобства, параметры в открытый ключ не включены.

Устройство криптосистемы второго типа $McElRM2(r,m)$. Для генерации ключей строится стандартная форма порождающей матрицы R кода $RM(r,m)$. Далее выбирается случайный номер i, $1 \leqslant i \leqslant k$. Из матрицы R удаляется строка с номером i. Получившуюся в результате матрицу обозначим через $R[i]$. Выбирается случайная двоичная невырожденная $((k-1)\times n)$-матрица $H = (h_{ij})$ и случайная перестановочная $(n\times n)$-матрица $P_\sigma = (p_{ij})$. Вычисляется матрица $G = H\cdot R[i]\cdot P_\sigma = H\cdot (R[i])^\sigma$. *Секретным ключом* криптосистемы является набор $(H, P_\sigma, i) = (H,\sigma,i)$, а *открытым ключом* — матрица G.

Определение 4. Два секретных ключа (H_1,σ_1) и (H_2,σ_2) называются *эквивалентными*, если соответствующие им открытые ключи G_1 и G_2 равны.

В работе решается задача восстановления секретного ключа криптосистемы или эквивалентного ему по открытому ключу.

Пусть (H,σ) — некоторый секретный ключ криптосистемы $McElRM1(r,m)$; G — соответствующий ему открытый ключ; $\sigma_{A,b}$ — некоторый автоморфизм кода Рида — Маллера. Тогда для порождающей матрицы R кода Рида — Маллера существует единственная матрица $H_{A,b}$ (невырожденная), что $H_{A,b}R = R\sigma_{A,b}$.

Теорема 1. Пусть $[(H,\sigma)]$ — класс эквивалентности секретного ключа (H,σ) криптосистемы $McElRM1$. Тогда $\{(HH_{A,b}, \sigma_{A,b}^{-1}\sigma) : \sigma_{A,b} \in \mathrm{Aut}(RM(r,m))\} \subseteq [(H,\sigma)]$.

Пусть C — произвольный $(k-1)$-подкод кода Рида — Маллера $RM(r,m)$. Рассмотрим такой моном $f_{\min} = x^{\alpha_{\min}}$, что для всех $\alpha' < \alpha_{\min}$ моном $x^{\alpha'} \in C$, а $f_{\min} \notin C$. Такой

моном существует и единственный. Пусть $\alpha = \alpha_{\min}$. Для всех $\alpha' > \alpha$ либо моном $x^{\alpha'} \in C$, либо $x^{\alpha'} \oplus x^{\alpha} \in C$, т. е. $x^{\alpha'} \oplus a(\alpha')x^{\alpha} \in C$ для некоторого $a(\alpha') \in \{0, 1\}$. Введём вектор $a = (a(\alpha') : \alpha' \in \mathbf{A}(r, m))$. Тогда код C однозначно определяется векторами α и a. Будем в дальнейшем такой код обозначать символом $C_{\alpha,a}(r, m)$, причём $a(\alpha') = 0$ для всех $\alpha' < \alpha$ и $a(\alpha) = 1$. Отметим, что открытый ключ G криптосистемы первого типа — это порождающая матрица кода $C^{\sigma}_{\alpha,a}$ для некоторого α и a.

Для построения атаки на криптосистему первого типа используем идеи работы [3].

Определение 5. Пусть C и B — два линейных $[n, k]$-кода. Произведением $C \circ B$ назовём код, состоящий из всех возможных произведений кодовых слов $c \cdot b$, $c \in C$, $b \in B$. Здесь $c \cdot b = (c_1 \cdot b_1, c_2 \cdot b_2, \ldots, c_n \cdot b_n)$, если $c = (c_1, \ldots, c_n)$ и $b = (b_1, \ldots, b_n)$.

Доказаны следующие теоремы.

Теорема 2. Пусть $r_1 + r_2 \leqslant m$. Пусть также $\alpha^1 \in \mathbf{A}(r_1, m)$, $\alpha^2 \in \mathbf{A}(r_2, m)$, причём выполнено одно из двух условий:

1) $\alpha^1 \neq \alpha^2$, $\alpha^1, \alpha^2 > 0$;
2) $\alpha^1 = \alpha^2 = \alpha$ и $\mathrm{wt}(\alpha) \geqslant 2$.

Тогда для любых a^1 и a^2 выполняется равенство

$$C_{\alpha^1,a^1}(r_1, m) \circ C_{\alpha^2,a^2}(r_2, m) = RM(r_1 + r_2, m).$$

Теорема 3. Пусть $2r < m$. Тогда для любых α, таких, что $\mathrm{wt}(\alpha) = 1$, либо $C_{\alpha,a}(r, m) \circ C_{\alpha,a}(r, m) = RM(2r, m)$, либо существует такой автоморфизм $\sigma_{A,b}$ кода Рида — Маллера $RM(r, m)$, что $C_{\alpha,a}(r, m) \circ C_{\alpha,a}(r, m) = C^{\sigma_{A,b}}_{1,0}(2r, m)$.

Общая схема атаки на криптосистему первого типа $McElRM1(r, m)$:

Ш а г 1. По матрице G построить порождающую матрицу кода $RM^{\sigma}(r, m)$.

Ш а г 2. Применить атаку Чижова — Бородина к этой матрице.

Для реализации первого шага предложен полиномиальный по сложности алгоритм, корректность работы которого доказывается при помощи теорем 2 и 3. Входным значением для алгоритма является открытый ключ криптосистемы $McElRM1(r, m)$ — матрица G, которая соответствует подкоду $C^{\sigma}_{\alpha,a}$. Выходным значением является порождающая матрица кода $RM^{\sigma}(r, m)$. Алгоритм применим для следующих параметров: $2r \leqslant m - 1$ при любом $\mathrm{wt}(\alpha)$ и для $2r \geqslant m$ при $\mathrm{wt}(\alpha) \leqslant m - r - 1$.

ЛИТЕРАТУРА

1. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. № 2. С. 3–20.
2. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347–360.
3. *Бородин М. А., Чижов И. В.* Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида — Маллера // Дискретная математика. 2014. Т. 26. № 1. С. 10–20.

Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.75 DOI 10.17223/2226308X/9/30

ПРОТОКОЛ БЕЗОТКАЗНОЙ ЛУКОВОЙ МАРШРУТИЗАЦИИ С ПОДТВЕРЖДЕНИЕМ ВРЕМЕНИ СОЗДАНИЯ СООБЩЕНИЯ

Н. И. Анисеня

Рассматривается задача маршрутизации сообщений в конкурентной среде децентрализованной сети на примере проведения соревнований CTF, основанных на решении заданий. К протоколу маршрутизации сообщений предъявляется дополнительное требование — подтверждение времени создания сообщения. Предложено улучшение протокола безотказной луковой маршрутизации, позволяющее участникам сети получать подтверждения времени создания передаваемых сообщений, описан улучшенный протокол и его возможная модификация.

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

В [1] автором предложен распределённый протокол проведения соревнований CTF, основанных на решении заданий. Описанный протокол обладает серьёзным недостатком, а именно — полагается на рассылку меток времени добросовестными участниками. Недобросовестный участник, который не рассылает свои разрешения, все ещё имеет доступ к сети и может получать сообщения, если участвует в передаче сообщений других команд.

Цель улучшения протокола безотказной луковой маршрутизации — сделать невозможным участие в соревновании команд, которые не ставят метки времени либо ставят некорректные метки под ответами других участников.

Будем полагать, что каждый участник сети постоянно ожидает получения сообщений. Сформулируем требования к улучшенному протоколу:

1) каждый участник сети должен иметь возможность получать сообщения только в том случае, если участвует в качестве посредника при передаче сообщений других участников;
2) каждый участник сети должен иметь возможность получать сообщения только в том случае, если устанавливает корректные метки времени на все передаваемые им сообщения;
3) в результате работы протокола отправитель сообщения должен иметь временные метки от различных участников сети, подтверждающие время отправки исходного сообщения;
4) никто из участников, кроме отправителя и получателя, не должен иметь возможность прочитать или изменить передаваемое сообщение;
5) никто из участников не должен иметь возможность подделать чужую метку времени под передаваемым сообщением;

6) протокол должен делать крайне сложной и маловероятной атаку сговора с целью установки некорректных меток времени под сообщением;
7) протокол должен допускать особый режим работы, если нет гарантий, что получатель сообщения в данный момент подключён к сети, но при этом необходимо здесь и сейчас зафиксировать время создания сообщения. В свою очередь, получатель должен иметь возможность убедиться в подлинности временной метки под сообщением, которое он получит, когда восстановит доступ в сеть.

Требования 1 и 2 необходимы для того, чтобы участники распределённой сети были заинтересованы в поддержании её работы. Требования 4 и 5 необходимы для защиты передаваемых сообщений и устанавливаемых под ними меток времени. Требование 6 служит для защиты от атаки сговора участников распределённой сети. Требование 7 необходимо, если данный протокол используется для проведения соревнований CTF, как в [1]. В этом случае необходимо уменьшить зависимость протокола от активного участия команды организаторов.

Пусть E_A — шифрование на открытом ключе участника с идентификатором A; S_A — подписание на закрытом ключе участника с идентификатором A; h — некоторая криптографическая хеш-функция. В случае, если y является конкатенацией байтового представления параметров $x_1, \ldots, x_t$, будем допускать следующую запись для функций E_A, S_A, h:

$$\begin{aligned} E_A(y) &= E_A(x_1, \ldots, x_t), \\ S_A(y) &= S_A(x_1, \ldots, x_t), \\ h(y) &= h(x_1, \ldots, x_t). \end{aligned}$$

Будем проводить сравнение значений времени с учётом временного окна w. Обозначим множество идентификаторов участников как U, $|U| = n$, где идентификаторы $id \in U$ — попарно различные числа. Функцию $G(y)$ определим как в [1]:

$$G(y) : \mathbb{N} \to U', \quad U' = \{u : u \subset U, |u| = t < n\}.$$

Введём функцию $H(y)$ следующим образом:

$$\begin{gathered} H(y) = [r_0, (id_1, r_1), \ldots, (id_t, r_t)], \\ id_i \in G(y),\ id_i < id_{i+1},\ i = 1, \ldots, t-1, \\ r_0 = h(y),\ r_i = h(y, id_i),\ i = 1, \ldots, t. \end{gathered}$$

Для удобства обозначим так же векторы идентификаторов участников и соответствующих им чисел:

$$M = (id_1, \ldots, id_t),\ R = (r_0, r_1, \ldots, r_t).$$

Будем говорить, что участник отключен от сети, если он не участвует в передаче сообщений либо искажает передаваемые им сообщения. Если все участники с идентификаторами $id_1, \ldots, id_t$ выступают в роли посредников при передаче сообщения, будем обозначать эти идентификаторы $M_1, \ldots, M_t$. Соответственно вектор M в этом случае запишется следующим образом: $M = (M_1, \ldots, M_t)$.

Пусть Алиса хочет послать сообщение m Бобу. При этом Алиса заинтересована в следующем:

1) она хочет убедиться в том, что все посредники, участвовавшие в передаче сообщения m, и получатель Боб честно выставляют метку времени (не завышают и не занижают время), когда выступают в роли посредника;

2) она хочет получить подтверждение времени создания сообщения m от других участников и предоставить его Бобу.

Боб, в свою очередь, хочет быть уверенным, что Алиса его не обманывает и указанное время создания сообщения m верно с точностью до некоторого временного окна w. Будем предполагать, что все участники сети постоянно ожидают сообщений и не могут предсказать время, в которое они должны им прийти.

Описание протокола:

1) Алиса считает $H(m) = [r_0, (M_1, r_1), \ldots, (M_t, r_t)]$.
2) Алиса конструирует «луковицу», шифруя сообщение m следующим образом:

$$E_B(E_{M_1}(\ldots E_{M_k}(E_A E_B(m), r_k), \ldots, r_1), r_0).$$

3) Алиса отправляет Бобу

$$E_B(E_{M_1}(\ldots E_{M_k}(E_A E_B(m), r_k), \ldots, r_1), r_0), \quad S_A(m, t_A), t_A,$$

где t_A — текущее время Алисы.

4) Боб расшифровывает внешний слой луковицы: получает r_0 и сообщение для первого посредника M_1. Боб отправляет посреднику M_1

$$E_{M_1}(\ldots E_{M_k}(E_A E_B(m), r_k), \ldots, r_1), \quad S_A(m, t_A), t_A, S_B(r_0, t_B), t_B.$$

5) Для $i \in \{1, \ldots, k-1\}$ i-й посредник отсылает $(i+1)$-му следующее сообщение:

$$E_{M_i}(E_{M_{i+1}}(\ldots E_{M_k}(E_A E_B(m), r_k), \ldots, r_{i+1}), r_i),$$
$$S_A(m, t_A), t_A, S_B(r_0, t_B), t_B, S_{M_1}(r_1, t_1), t_1, \ldots, S_{M_i}(r_i, t_i), t_i.$$

6) Последний посредник M_k отправляет Алисе

$$E_A E_B(m), \quad S_A(m, t_A), t_A, S_B(r_0, t_B), t_B, S_{M_1}(r_1, t_1), t_1, \ldots, S_{M_k}(r_k, t_k), t_k.$$

7) Алиса проверяет, что все метки времени $S_B(r_0, t_B)$, $S_{M_i}(r_i, t_i)$, t_i, $i = 1, \ldots, k-1$, имеют корректную подпись и указывают на адекватное время. Если проверки пройдены, Алиса посылает Бобу

$$E_B(m), \quad S_A(m, t_A), t_A, S_B(r_0, t_B), t_B, S_{M_1}(r_1, t_1), t_1, \ldots, S_{M_k}(r_k, t_k), t_k.$$

Боб проводит проверку следующим образом.

1) Посчитать $H(m) = [r_0, (M_1, r_1), \ldots, (M_k, r_k)]$.
2) Проверить подписи временных меток $S_A, S_B, S_{M_i}, i = 1, \ldots, k$.
3) Проверить, что для значений времени в метках времени верны следующие равенства:

$$t_{M_i} =_w t_{M_{i+1}}, \ i \in \{1, \ldots, k-1\}, \quad t_{M_1} =_w t_B, \quad t_B =_w t_A.$$

4) Если проверки пройдены, то считать, что сообщение m создано в момент времени t_A.

В случае, если Боб в данный момент не подключен к сети, а Алиса хочет засвидетельствовать факт создания сообщения m немедленно, можно внести следующие модификации в протокол. На шаге 2 внешний слой шифрования для Боба не включается.

Последний шаг 7 протокола не зависит от времени, поэтому может быть выполнен, когда Боб снова подключится к сети. Проверка выполняется аналогично с учётом того, что временная метка $S_B(r_0, t_B), t_B$ отсутствует.

Некоторые комментарии к протоколу. Функция $H(m)$, аналогично функции $G(m)$, имеет параметры n, t, k. В случе, если хотя бы один из первых k посредников из M отключен от сети, получение меток времени от этой цепочки посредников невозможно. Для того чтобы получить метку времени, необходимо выбрать k подключенных участников и сформировать луковицу согласно порядку в M. Таким образом, $H(m)$ также имеет запас в $(t-k)$ участников.

Функция $G(m)$ в составе функции $H(m)$ нужна для того, чтобы случайным образом выбирать участников для выставления метки времени под сообщением m, тем самым сильно затрудняя возможность их предварительного сговора с целью установки ложной метки времени.

Вектор R, получаемый функцией $H(m)$, является вектором чисел, которые невозможно предсказать, не зная сообщения m. Это нужно для того, чтобы посредники имели возможность поставить временную метку на $r_i = h(m, id_i)$, не зная самого сообщения m. Числа r_i также используются в качестве *Nonce*, чтобы следующие посредники не могли определить предыдущих посредников, которые уже поставили свою метку времени на сообщение.

Рассмотрим пример. Имеется множество участников $U = \{A, B, M_1, M_2\}$, $|U| = n = 4$, $t = k = 2$. Они подключены к сети, как показано на рис. 1.

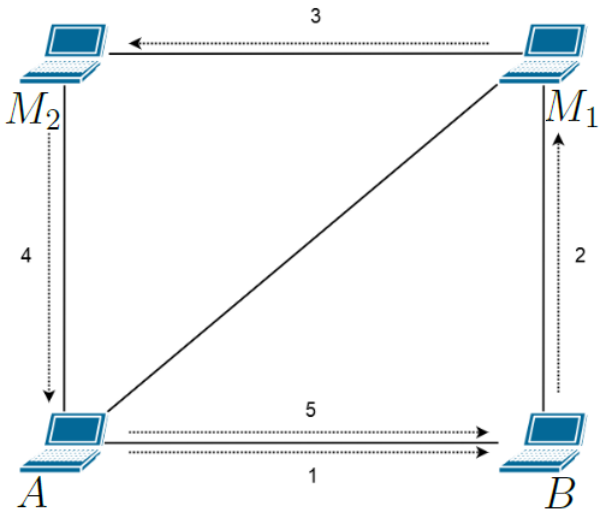


Рис. 1. Пример работы протокола безотказной луковой маршрутизации с подтверждением времени создания сообщения

Пусть участник A хочет послать сообщение m участнику B. Для этого ему необходимо вычислить $H(m) = [r_0, (M_1, r_1), (M_2, r_2)]$. Имеем следующую луковицу $E_B(E_{M_1}(E_{M_2}(E_A E_B(m), r_2), r_1), r_0)$. Подробно рассмотрим процесс передачи луковицы и выставления меток времени:

1) $A \to B$: $E_B(E_{M_1}(E_{M_2}(E_A E_B(m), r_2), r_1), r_0)$, $S_A(m, t_A), t_A$.
2) $B \to M_1$: $E_{M_1}(E_{M_2}(E_A E_B(m), r_2), r_1)$, $S_A(m, t_A), t_A, S_B(r_0, t_b), t_B$.

3) $M_1 \to M_2$: $E_{M_2}(E_A E_B(m), r_2)$,
$S_A(m, t_A), t_A, S_B(r_0, t_b), t_B, S_{M_1}(r_1, t_{M_1}), t_{M_1}$.

4) $M_2 \to A$: $E_A E_B(m)$,
$S_A(m, t_A), t_A, S_B(r_0, t_b), t_B, S_{M_1}(r_1, t_{M_1}), t_{M_1}, S_{M_2}(r_2, t_{M_2}), t_{M_2}$.

5) Проверка: $t_{M_2} =_w t_{M_1}$, $t_{M_1} =_w t_B$, $t_B =_w t_A$. Если проверки пройдены:
$A \to B$: $E_B(m)$,
$S_A(m, t_A), t_A, S_B(r_0, t_b), t_B, S_{M_1}(r_1, t_{M_1}), t_{M_1}, S_{M_2}(r_2, t_{M_2}), t_{M_2}$.

Описанный протокол может использоваться как протокол транспортного уровня в распределённой сети соревнования CTF следующим образом. Команда организаторов, согласно протоколу, осуществляет новостную рассылку во время соревнования. Если участник хочет получать новостную рассылку от организаторов, ему необходимо выступать в качестве посредника при передаче сообщений других участников, выставляя на них корректную метку времени. В противном случае участник не сможет получать новостную рассылку, что равносильно отключению от соревнования и техническому поражению.

Каждый участник при получении ответа на задание должен доказать этот факт, отправив сообщение организаторам. Засвидетельствовать факт получения ответа в текущий момент времени можно с помощью модифицированного протокола, т. е. предполагая, что команда организаторов в данный момент может быть недоступна. Команды-соперники, выбранные в качестве посредников с помощью функции $H(m)$, подтвердят факт создания сообщения в текущий момент времени. Итоговое сообщение вместе с метками времени может быть отправлено организаторам позже. По окончании соревнования организаторы смогут сформировать таблицу результатов с учётом времени получения ответов.

ЛИТЕРАТУРА

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

УДК 519.7 DOI 10.17223/2226308X/9/31

О ДИСКРЕТНО-АВТОМАТНЫХ МОДЕЛЯХ АТАК В КОМПЬЮТЕРНЫХ СЕТЯХ[1]

Д. Е. Горбатенко, С. Е. Кочемазов, А. А. Семёнов

Предлагается новая модель развития атак в компьютерных сетях. Основу модели составляет дискретный автомат синхронного действия, задаваемый графом сети. Рассматриваются переходы между состояниями данного автомата, совершаемые в дискретные моменты времени. Вершинам графа (интерпретирующим хосты сети) в каждый момент времени приписываются двоичные векторы, называемые состояниями хостов. В каждый следующий момент все состояния хостов синхронно пересчитываются по фиксированным правилам. В рамках предложенной модели проанализировано развитие некоторых известных типов атак. Изучены возможности атак с нескольких хостов, а также описана техника предотвращения атак посредством решения комбинаторной задачи расстановки патчей. В вычислительных экспериментах рассматривались сети, сгенерированные случайным образом. Перечисленные выше задачи для этих сетей решались за счёт их сведения к проблеме булевой выполнимости.

[1]Работа выполнена при частичной поддержке РФФИ, проекты № 14-07-00403а и 15-07-07891а.

Ключевые слова: *дискретный автомат, граф атак, задача булевой выполнимости, SAT.*

Исследование атак в компьютерных сетях и способов защиты от них является актуальной и интенсивно развивающейся областью компьютерной безопасности. Для анализа сети на предмет возможности реализации в ней той или иной атаки, а также для определения способов защиты от атак используются формальные модели компьютерных сетей [1]. Обычно основой такой модели является ориентированный помеченный граф $G = (V, A)$, в котором V — множество вершин, A — множество дуг. Вершины графа G соответствуют хостам рассматриваемой сети, а дуги интерпретируют связи между хостами. В последние 10 лет весьма широкое распространение получил подход к анализу атак в сетях, базирующийся на графах атак [2 – 4]. Есть большое число различных подходов к построению графов атак, описание некоторых способов может быть найдено в [4]. В настоящей работе предлагается рассматривать развитие атаки в компьютерной сети как эволюцию некоторого дискретного автомата, происходящую в моменты времени $t \in \{0, 1, \ldots\}$. Этот подход имеет в сравнении с известными по меньшей мере два преимущества. Во-первых, он позволяет в простой и естественной форме ставить комбинаторные задачи, связанные с развитием и блокированием атак. Во-вторых, эти задачи допускают применение современных эффективных комбинаторных алгоритмов. Для получения представленных в работе результатов в роли таковых использованы алгоритмы решения проблемы булевой выполнимости (SAT). Далее кратко остановимся на основных полученных к настоящему моменту результатах.

Итак, рассматриваем граф $G = (V, A)$, интерпретирующий компьютерную сеть. Пусть $Q = \{q_1, \ldots, q_l\}$ — множество уязвимостей хостов, возможных в рамках рассматриваемой сети. Процесс развития атаки в сети — это процесс эксплуатации злоумышленником доступных уязвимостей, результатом чего в следующий момент времени является возможность эксплуатировать другие уязвимости. Соответственно можно рассмотреть сеть G как дискретный автомат, функционирующий в моменты времени $t \in \{0, 1, \ldots\}$, момент $t = 0$ назовём начальным. Для каждого t свяжем с произвольным хостом $v \in V$ булев вектор

$$\alpha^v(t) = \left(\alpha_1^v, \ldots, \alpha_l^v, \alpha_{l+1}^v(t), \ldots, \alpha_r^v(t)\right), r \geqslant l,$$

называемый состоянием хоста v в момент t. Первые l координат вектора $\alpha^v(t)$ образуют вектор, называемый вектором уязвимостей. Он интерпретируется в следующем смысле: $\alpha_j^v = 1$ тогда и только тогда, когда на хосте v имеется уязвимость q_j, $j \in \{1, \ldots, l\}$. Вектор уязвимостей хоста во все моменты времени остаётся неизменным. В координатах $\alpha^v(t)$ с номерами $l + 1, \ldots, r$ находится информация, которая может меняться с течением времени. В частности, в этих координатах отображается доступ с рассматриваемого узла на другие узлы сети. Вектор $\left(\alpha_{l+1}^v(t), \ldots, \alpha_r^v(t)\right)$ будем называть вектором возможностей хоста v в момент t.

Полагая, что в начальный момент для всех хостов сети заданы их состояния (например, все векторы возможностей при $t = 0$ могут быть нулевыми), можем рассматривать переходы сети в последующие состояния, изменяя векторы возможностей хостов в каждый момент в соответствии с фиксированными правилами. В качестве правил использованы пары вида (предусловие, постусловие), посредством которых в работе [5] определяются элементарные атаки. В рамках предлагаемой модели состояния для всех хостов пересчитываются синхронно. В этом случае по аналогии с синхронными булевыми сетями (SBN, они же сети Кауффмана [6]) функционирование автомата,

задаваемого графом G, порождает граф переходов (STG, State Transition Graph), обозначаемый через Γ_G. Каждой вершине графа Γ_G соответствует набор состояний всех хостов сети в рассматриваемый момент времени.

Поясним сказанное на ставшем хрестоматийным примере, впервые рассмотренном в работе [2]. Рассматривается сеть, состоящая из трёх хостов H_1, H_2, H_3. Состояние каждого хоста в момент времени $t \in \{0, 1, \ldots\}$ — это булев вектор из 9 координат. Первые четыре координаты соответствуют уязвимостям «write-noauth», «trust-login», «pe-noauth», «pe-local». Смысл этих уязвимостей описан в [5] (например, уязвимость «pe-noauth» на хосте v дает получившему доступ на v права суперпользователя на данном хосте). Пятая координата отвечает за активность опции «trust between the host and all». Активность данной опции на конкретном хосте H означает, что этот хост доверяет любому другому хосту сети. Если нарушитель может активировать данную опцию на H, то на следующем шаге он может подключиться к H без использования логина и пароля. Остальные координаты определяют права, которые по умолчанию имеет рассматриваемый хост на остальные узлы сети. На рис. 1 приведён фрагмент графа состояний дискретного автомата, задаваемого (в указанном выше смысле) сетью из работы [2]. Данный фрагмент соответствует одной атаке на сеть, рассмотренной в [5].

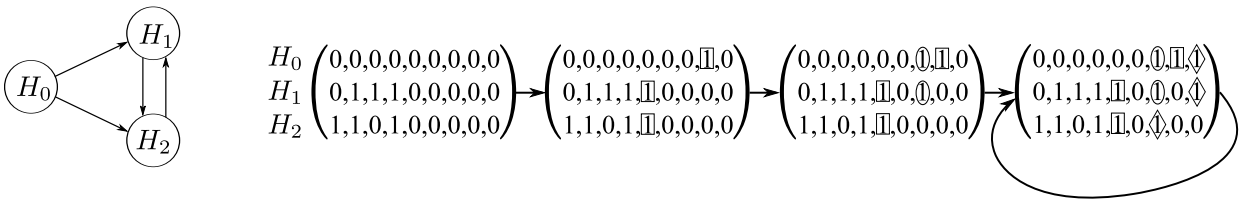


Рис. 1. Сеть из трёх хостов (слева) и фрагмент графа состояний автомата (STG), заданного этой сетью, интерпретирующий атаку, рассмотренную в [5]

Фрагмент графа состояний, приведённый на рис. 1, показывает два возможных пути развития атаки. В первом случае злоумышленник непосредственно со своего компьютера (хост H_0) проводит элементарную атаку, эксплуатирующую уязвимость «write-noauth» на хосте H_2, тем самым активируя на этом хосте опцию «trust between the host and all». Данная опция устанавливает доверительные отношения хоста H_2 со всеми остальными хостами в сети (на STG биты, отвечающие за включение данной опции, выделены квадратами). На следующем шаге, пользуясь полученной возможностью, злоумышленник получает права доступа пользователя на хосте H_2, эксплуатируя уязвимость «trust-login» (биты, соответствующие появлению прав пользователя у злоумышленника, выделены кругами). Далее, эксплуатируя уязвимость «pe-local» на хосте H_2, злоумышленник повышает свои права доступа до прав доступа суперпользователя (соответствующие биты выделены ромбами).

На фрагменте STG на рис. 1 виден также второй вариант получения злоумышленником прав суперпользователя на хосте 2. На первом шаге эксплуатируются уязвимости «write-noauth» и «pe-noauth» на хосте H_1, результат: доверие хоста H_1 всем остальным хостам сети и права суперпользователя у злоумышленника на хосте H_1. Далее злоумышленник проводит атаку на хост H_2 с хоста H_1, используя действия, аналогичные первому сценарию: последовательно эксплуатируются уязвимости «trust-login» и «pe-local» хостом H_1 на хосте H_2 в моменты времени $t = 2$ и 3 соответственно, благодаря чему хост H_1 получает права доступа суперпользователя на хосте H_2.

В рамках описанной модели мы рассмотрели ряд задач, связанных с анализом и блокированием атак в компьютерных сетях. В частности, рассмотрены задачи выбора злоумышленником нескольких хостов для атаки. При этом на возможности злоумышленника накладывались различные ограничения: например, требовалось получить root-право на некотором компьютере сети не более чем за фиксированное число моментов времени. Дополнительно предполагалось, что в процессе атаки злоумышленник не может в каждый момент времени иметь root-права более чем на заданном числе хостов сети. Такого рода задачи «подбора множеств хостов» являются комбинаторными из-за значительного в общем случае числа различных альтернатив, требующих проверки. Задачи описанного типа решались за счёт их сведения к задаче о булевой выполнимости (SAT). При этом использованы кодировки и общие идеи, представленные в работе [7], в которой методами SAT исследована активационная динамика в сетях. Если удавалось подобрать множество хостов, с которого злоумышленник успешно атаковал рассматриваемую систему, то для этой ситуации рассматривалась обратная задача: запретить те или иные уязвимости на некоторых хостах сети, чтобы в результате найденная атака стала невозможной. Эту задачу М. Данфорт называет задачей расстановки патчей. В рамках развитого вычислительного аппарата можно накладывать ограничения на число расставляемых патчей и их вид (например, предполагать, что блокирование некоторых уязвимостей невозможно). Все вычислительные эксперименты проводились на сетях, сгенерированных случайным образом в соответствии с моделью Барабаши — Альберт [8]. Перечисленные комбинаторные задачи удалось успешно решить для сетей с несколькими сотнями хостов.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Модели безопасности компьютерных систем: учеб. пособие для вузов. М.: Издательский центр «Академия», 2005.
2. *Jha S., Sheyner O., and Wing J.* Two formal analysis of attack graphs // Proc. 15th IEEE Workshop on Computer Security Foundations (CSFW '02). 2002. P. 49–63.
3. *Sheyner O., Haines J. W., Jha S., et al.* Automated generation and analysis of attack graphs // Proc. 2002 IEEE Symposium on Security and Privacy. 2002. P. 273–284.
4. *Колегов Д. Н.* Проблемы синтеза и анализа графов атак. `http://www.securitylab.ru/contest/299868.php`. 2009.
5. *Danforth M.* Models for Threat Assessment in Networks. PhD Thesis, University of California-Davis, 2006.
6. *Kauffman S.* Metabolic stability and epigenesis in randomly constructed genetic nets // J. Theoretical Biology. 1969. No. 22. P. 437–467.
7. *Kochemazov S. and Semenov A.* Using synchronous Boolean networks to model several phenomena of collective behavior // PLoS ONE. 2014. No. 9: e115156. P. 1–28.
8. *Barabasi A-L. and Albert R.* Emergence of scaling in random networks // Science. 1999. No. 286. P. 509–512.

УДК 004.94 DOI 10.17223/2226308X/9/32

О РЕЗУЛЬТАТАХ ФОРМИРОВАНИЯ ИЕРАРХИЧЕСКОГО ПРЕДСТАВЛЕНИЯ МРОСЛ ДП-МОДЕЛИ

П. Н. Девянин

«Монолитное» представление мандатной сущностно-ролевой ДП-модели, являющееся основой механизма управления доступом в отечественной защищённой опе-

рационной системе специального назначения (ОССН) *Astra Linux Special Edition*, ввиду своего значительного объёма и сложности стало неудобно как для научного анализа, верификации и дальнейшего развития самой модели, так и для непосредственного применения в ОССН. По этой причине предлагается полностью переработанное иерархическое представление модели, описывающее её по уровням. В текущем таком представлении заданы четыре иерархически упорядоченных уровня, соответствующих: 1) ролевому управлению доступом; 2) мандатному контролю целостности; 3) мандатному управлению доступом с информационными потоками по памяти и 4) по времени. В дальнейшем возможно добавление новых, в том числе «боковых» уровней, например 3') для модели гипервизора.

Ключевые слова: *компьютерная безопасность, формальная модель, иерархическое представление, Linux.*

Разработанная автором мандатная сущностно-ролевая ДП-модель (МРОСЛ ДП-модель) [1, 2] является частью комплексного научно-обоснованного решения [3] по разработке отечественной защищенной ОССН *Astra Linux Special Edition* [4, 5]. Для получения гарантий адекватности реализации МРОСЛ ДП-модели в ОССН Институтом системного программирования РАН [6, 7] она была сначала переведена в формализованную нотацию *Event-B* (*Rodin Platform*), которая позволила верифицировать описание модели и осуществить дедуктивные доказательства её свойств. Затем на основе формализованного представления модели с использованием инструмента дедуктивной верификации кода *Why* (в среде разработки *Frama-C*) были заданы и проверено выполнение спецификаций (предусловий и постусловий) функций механизма управления доступом ОССН, что позволило обосновать адекватность реализации модели в программном коде.

В то же время существующее описание МРОСЛ ДП-модели имеет значительный объём и является «монолитным», т. е. в нём элементы модели приводятся в порядке, принятом несколько лет назад в начале формирования модели. Первыми делаются предположения о базовых свойствах задаваемой в рамках модели абстрактной системы, потом даются определения элементов состояний системы, далее описываются требования к реализации в системе мандатного и ролевого управления доступом и мандатного контроля целостности, затем приводятся правила преобразования состояний системы, и в заключение формулируются и обосновываются условия безопасности системы, а также рассматриваются подходы к применению модели в ОССН.

В итоге по мере получения новых теоретических результатов и всё большей адаптации модели к условиям функционирования ОССН модель становится всё труднее корректировать, так как каждое изменение в каком-либо её элементе требует учёта во всех других связанных с ним элементах модели, а также проверки справедливости большинства обоснованных в модели утверждений. Кроме того, из-за большого объёма и «монолитности» модели, невозможности в таком виде её поэтапной реализации затрудняется использование модели разработчиками ОССН, а также создание на её основе новых моделей (например, модели гипервизора для ОССН).

В связи с этим автором реализуется переход от «монолитного» описания модели к иерархическому, позволяющему представить модель по уровням (слоям). При этом каждый нижний уровень модели представляет абстрактную систему, элементы которой не зависят от новых элементов, принадлежащих более высокому уровню, который, в свою очередь, наследует, а при необходимости корректирует или дополняет элементы нижнего уровня.

Таким образом, при иерархическом описании МРОСЛ ДП-модели в настоящее время задаются следующие уровни (рис. 1):

— первый уровень — модель системы ролевого управление доступом;
— второй уровень — модель системы ролевого управление доступом и мандатного контроля целостности;
— третий уровень — модель системы ролевого управление доступом, мандатного контроля целостности и мандатного управления доступом только с информационными потоками по памяти;
— четвёртый уровень — модель системы ролевого управление доступом, мандатного контроля целостности и мандатного управления доступом с информационными потоками по памяти и по времени.

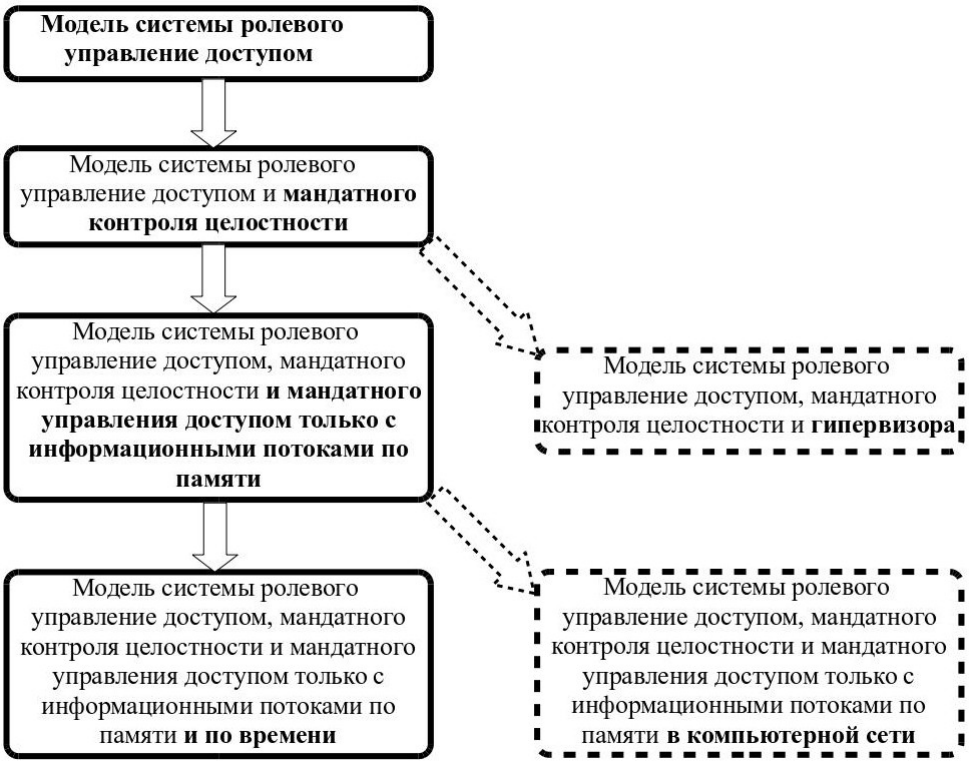


Рис. 1. Иерархическое представление МРОСЛ ДП-модели и его возможные расширения

Этот подход позволяет постепенно усложнять формулировки определений и утверждений модели по мере включения в неё соответствующих очередному рассматриваемому уровню элементов. Например, на третьем уровне (мандатного управления доступом с информационными потоками по памяти) с использованием обозначений из [1] даётся следующая формулировка определения безопасного начального состояния системы. При этом идентификаторы определения и его условий дополнительно показывают последовательность их формирования при переходе от уровня к уровню (Ц — второй уровень, КП — третий уровень).

Определение о.Ц.06.КП. Начальное состояние G_0 системы $\Sigma(G^*, OP, G_0)$ назовём безопасным, если оно удовлетворяет следующим условиям.

Условие Ц.1.КП. Для каждых субъект-сессий $x, y \in S_0$, таких, что $y \in de_facto_own_0(x)$, верно $f_{s_0}(y) = f_{s_0}(x)$ и $i_{s_0}(y) \leqslant i_{s_0}(x)$ (по сравнению со вторым уровнем добавляется требование равенства текущих уровней доступа субъект-сессий x и y, одна из которых де-факто владеет другой).

Условие Ц.2.КП. Для каждых недоверенной субъект-сессии $x \in N_{S_0}$, субъект-сессии $y \in S_0$ и сущности $e \in E_0$, таких, что либо $(e \in [y]$ и $(x, e, write_m) \in F_0)$, либо $(e \in]y[$ и либо $(e, x, write_m) \in F_0$, либо $(x, e, read_a) \in A_0)$, верно $f_{s_0}(y) \leqslant f_{s_0}(x)$ и $i_{s_0}(y) \leqslant i_{s_0}(x)$ (по сравнению со вторым уровнем добавляется требование, чтобы текущий уровень доступа к сущностям, параметрически или функционально ассоциированным с сущностью y, недоверенной субъект-сессии x был не ниже текущего уровня доступа этой субъект-сессии y и субъект-сессия x либо имела информационные потоки по памяти, либо обладала доступом на чтение).

Условие Ц.3. (На третьем уровне в это условие не дополняется новых требований.)

Условие Ц.4.КП. Для каждого информационного потока $(x, y, write_m) \in F_0$ справедливо $f_{x_0}(x) \leqslant f_{y_0}(y)$**, где** f_{x_0} **и** f_{y_0} **— соответствующие функции** f_{e_0} **или** f_{s_0}, и справедливо $i_{x_0}(x) \leqslant i_{y_0}(y)$, где i_{x_0} и i_{y_0} — соответствующие функции i_{e_0} или i_{s_0} (по сравнению со вторым уровнем добавляется требование, чтобы при наличии информационного потока по памяти уровень конфиденциальности источника x был не выше уровня конфиденциальности приемника y).

Условие КП.5. **Для доверенных субъект-сессий** $x, y \leqslant L_{S_0}$**, таких, что** $y \in de_facto_own_0(x)$**,** $(y, downgrade_admin_role, read_a) \in AA_0$**, верно** $(x, downgrade_admin_role, read_a) \in AA_0$ (новое условие, добавленное на третьем уровне, заключающееся в запрете получения через де-факто владение специальной административной роли $downgrade_admin_role$, позволяющей нарушать правила мандатного управления доступом).

Аналогично задаются 34 де-юре и 10 де-факто правил преобразования состояний, когда на каждом очередном уровне добавляются, корректируются или остаются без изменений условия и результаты их применения.

При таком иерархическом описании модель гипервизора для ОССН (рис. 1) рассматривается как альтернативный (дополнительный) третий уровень (модель системы ролевого управления доступом, мандатного контроля целостности и гипервизора), так как можно предположить, что гипервизор для ОССН должен обеспечивать корректность функционирования её мандатного контроля целостности, а мандатное управление доступом в ОССН не должно реализовываться средствами гипервизора. Аналогично модель ролевого управления доступом в компьютерной сети целесообразно считать альтернативной четвёртому уровню представления МРОСЛ ДП-модели, так как в этой модели существенным является мандатный контроль целостности и мандатное управление доступом только с информационными потоками по памяти.

Таким образом, переход от «монолитного» к иерархическому представлению МРОСЛ ДП-модели за счёт более ясного, структурированного её изложения способствует развитию самой модели, улучшению результатов её верификации при переводе модели в формализованную нотацию *Event-B*, а также позволяет повысить качество реализации модели непосредственно в ОССН.

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.* Необходимые условия нарушения безопасности информационных потоков по времени в рамках МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2015. № 8. С. 81–83.

3. *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.
4. Операционные системы Astra Linux. `http://www.astra-linux.ru/`
5. Astra Linux. `https://ru.wikipedia.org/wiki/Astra\_Linux`
6. *Девянин П. Н., Кулямин В. В., Петренко А. К. и др.* О представлении МРОСЛ ДП-модели в формализованной нотации Event-B // Проблемы информационной безопасности. Компьютерные системы. 2014. № 3. С. 7–15.
7. *Devyanin P., Khoroshilov A., Kuliamin V., et al.* Formal verification of OS security model with Alloy and Event-B // LNCS. 2014. V. 8477. P. 309–313.

УДК 517.19 DOI 10.17223/2226308X/9/33

СХЕМА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ В АЛГОРИТМЕ RAID-PIR

М. Р. Кащеев, Ю. В. Косолапов

Рассматривается задача обеспечения конфиденциальности информационной базы данных в схеме анонимного получения информации (private information retrieval) с удалённых серверов. Предполагается, что для хранения базы используются r серверов (r — нечётное), а для анонимного доступа к информации используется алгоритм RAID-PIR. Построен способ шифрования и распределения базы данных таким образом, чтобы, во-первых, по зашифрованным данным, хранящимся на каждом из серверов, нельзя было нарушить конфиденциальность базы данных, и, во-вторых, чтобы при чтении или перезаписи блока данных ни один из серверов не мог узнать, какой блок соответственно считывался или перезаписывался.

Ключевые слова: *анонимность данных, PIR, распределение данных.*

Под анонимностью в сетях передачи данных, как правило, понимается либо невозможность идентификации сервером пользователей, отправивших запрос (анонимность пользователя), либо невозможность идентификации сервером запрашиваемой пользователями информации (анонимность запроса) [1]. В настоящей работе рассматривается обеспечение второго варианта анонимности. Предполагается, что для хранения информационной базы данных используется несколько серверов. Пользователь заинтересован в получении некоторой части базы данных таким образом, чтобы серверы, участвующие в хранении, по отдельности не смогли идентифицировать, какая именно часть базы была запрошена пользователем. В подобных схемах серверы могут рассматриваться как недобросовестные наблюдатели, цель которых заключается в выяснении, в получении какой информации из базы данных заинтересован пользователь. Простейшим случаем обеспечения анонимности является схема с одним сервером, когда пользователь с сервера запрашивает всю базу полностью [2]. Обычно в системах обеспечения анонимности запроса предполагается, что серверу может быть известно (частично или полностью) информационное содержимое базы. В работе рассматривается ситуация, когда знание сервером базы нежелательно, при этом необходимо также защититься от получения сервером информации о расположении или доле запрашиваемой информации в базе. Таким образом, ставится задача построения схемы защиты

конфиденциальности информационной базы данных, позволяющей анонимно считывать данные из базы и перезаписывать их.

Пусть $\mathrm{DB} \in \mathbb{F}_2^n$ — информационная база данных, представленная в виде конкатенации b блоков длины k бит каждый: $\mathrm{DB} = (d_1, \ldots, d_b)$, $d_i \in \mathbb{F}_2^k$, а для хранения базы DB используются r серверов хранения $\mathrm{S}_1, \ldots, \mathrm{S}_r$, где r — нечётное число. Целью пользователей этой системы хранения является получение j-го ($j \in \{1, \ldots, b\}$) блока базы DB таким образом, чтобы каждый из серверов не узнал j. Для этого пользователь отправляет специальные вектор-запросы всем серверам, а серверы вычисляют побитовые суммы блоков, соответствующих вектор-запросу пользователя, и отправляют пользователю результаты суммирования. Вектор-запрос к серверу — это бинарный вектор, в котором единицы находятся на позициях с номерами блоков базы, которые сервер должен просуммировать в ответ. Отметим, что способ построения запросов и соответствующих ответов, при котором отдельный сервер может знать информационное содержимое базы, но не может по запросу понять, какой именно блок запрошен пользователем, предложен в [3]. Далее схему из [3] назовём RAID-PIR.

В настоящей работе на базе варианта RAID-PIR, когда каждый сервер отвечает несколькими блоками, строится решение задачи обеспечения конфиденциальности информации в базе относительно серверов. Для этого используется шифрование методом модульного гаммирования с $r-1$ случайными (псевдослучайными) ключами длины n. Предполагается, что для генерации ключевой последовательности (гаммы) используется генератор непредсказуемой последовательности чисел, который обозначим `rnd_gen`. Построены четыре протокола: распределения базы по серверам (**DistribDB**), чтения i-го блока из базы (**GetBlock**), перешифрования данных на серверах (**NewKey**) и перезаписи i-го блока в базе (**SetBlock**). Параметром протоколов является число p ($1 < p < r$) — число зашифрованных на разных ключах копий базы DB, хранимых на каждом сервере.

Алгоритм 1. DistribDB — распределение базы $\mathrm{DB} \in \mathbb{F}_2^n$ по серверам $\mathrm{S}_1, \ldots, \mathrm{S}_r$

1: Владелец базы строит набор $\Gamma = \{\Gamma^1, \ldots, \Gamma^r\}$, где для $j = 1, \ldots, r-1$ вектор $\Gamma^j = (\gamma_1^j, \ldots, \gamma_b^j)$, $\gamma_i^j \in \mathbb{F}_2^k$, генерируется с помощью генератора `rnd_gen`; $\Gamma^r := \bigoplus\limits_{i=1}^{r-1} \Gamma^i$.

2: По DB и Γ вычисляются векторы: $\mathrm{DB}_\Gamma^j = \mathrm{DB} \oplus \Gamma^j = (d_1^j, \ldots, d_b^j)$, $j = 1, \ldots, r$.

3: Серверу S_j передаются $\mathrm{DB}_\Gamma^{j \bmod (r+1) + \lfloor j/(r+1) \rfloor}, \ldots, \mathrm{DB}_\Gamma^{(j+p-1) \bmod (r+1) + \lfloor (j+p-1)/(r+1) \rfloor}$, $j = 1, \ldots, r$.

Алгоритм 2. GetBlock — получение i-го блока (блока d_i) из базы DB

1: Пользователь с помощью алгоритма RAID-PIR получает i-й блок d_i^j с каждого вектора DB_Γ^j, $j = 1, \ldots, r$.

2: Пользователь вычисляет: $\bigoplus\limits_{j=1}^{r} d_i^j = \bigoplus\limits_{j=1}^{r} (\gamma_i^j \oplus d_i) = \left(\bigoplus\limits_{j=1}^{r} \gamma_i^j \right) \oplus \left(\bigoplus\limits_{j=1}^{r} d_i \right)$. Так как $\bigoplus\limits_{j=1}^{r} \gamma_i^j = \mathbf{0} (\in \mathbb{F}_2^k)$ и r — нечётное число, то $\bigoplus\limits_{j=1}^{r} d_i^j = d_i$.

Алгоритм 3. NewKey — перешифрование данных на серверах с помощью набора $\widetilde{\Gamma} = \{\widetilde{\Gamma}^1, \ldots, \widetilde{\Gamma}^r\}$

1: Пользователь передаёт на сервер S_j, $j = 1, \ldots, r$, соответствующие этому серверу p векторов: $\widetilde{\Gamma}^{j \bmod (r+1)+\lfloor j/(r+1)\rfloor}, \ldots, \widetilde{\Gamma}^{(j+p-1) \bmod (r+1)+\lfloor (j+p-1)/(r+1)\rfloor}$.

2: Сервер S_j обновляет хранящиеся у него части: $\mathrm{DB}_\Gamma^l := \mathrm{DB}_\Gamma^l \oplus \widetilde{\Gamma}^l$, где $l \in \{j \bmod (r+1) + \lfloor j/(r+1)\rfloor, \ldots, (j+p-1) \bmod (r+1) + \lfloor (j+p-1)/(r+1)\rfloor\}$, $j = 1, \ldots, r$.

Алгоритм 4. SetBlock — перезапись i-го блока в базе DB новым значением $\widetilde{d}_i$

1: Пользователь получает i-й блок базы ($d_i = \mathbf{GetBlock}(i)$), генерирует новый набор $\widetilde{\Gamma} = \{\widetilde{\Gamma}^1, \ldots, \widetilde{\Gamma}^r\}$ ($\widetilde{\Gamma} \leftarrow$ `rnd_gen`) и для каждого $\widetilde{\Gamma}^j = (\widetilde{\gamma}_1^j, \ldots, \widetilde{\gamma}_b^j)$ из $\widetilde{\Gamma}$ переопределяет $\widetilde{\gamma}_i^j$: $\widetilde{\gamma}_i^j := \widetilde{\gamma}_i^j \oplus (\widetilde{d}_i \oplus d_i)$.

2: Пользователь выполняет протокол перешифрования $\mathbf{NewKey}(\widetilde{\Gamma})$.

Показано, что

1) протоколы **GetBlock** и **SetBlock** обеспечивают анонимность соответственно запрашиваемых и записываемых данных;
2) протоколы **DistribDB**, **NewKey** и **SetBlock** обеспечивают конфиденциальность хранимых на серверах данных;
3) любая коалиция мощности $t < \lceil r/p \rceil$ не может нарушить конфиденциальность базы данных, а любая коалиция мощности $t \geqslant r - p + 1$ однозначно дешифрует базу данных.

ЛИТЕРАТУРА

1. *Pfitzmann A. and Hansen M.* A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. `https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.18.pdf`. Дата обращения 30.03.2016.
2. *Chor B., Goldreich O., Kushilevitz E., and Sudan M.* Private information retrieval // J. ACM. 1998. V. 45(6). P. 965–981.
3. *Demmler D., Herzberg A., and Schneider T.* RAID-PIR: Practical Multi-Server PIR // Proc. 6th edition of the ACM Workshop on Cloud Computing Security. N. Y., USA: 2014. P. 45–56.

УДК 004.94 DOI 10.17223/2226308X/9/34

МЕТОД ЗАПУТЫВАНИЯ ПРОГРАММНОЙ РЕАЛИЗАЦИИ СХЕМЫ HMAC ДЛЯ НЕДОВЕРЕННОЙ СРЕДЫ

Д. Н. Колегов, О. В. Брославский, Н. Е. Олексов

Предлагается метод обфускации схемы аутентификации сообщений HMAC для реализации в недоверенных средах.

Ключевые слова: *white-box cryptography, коды аутентификации сообщений, HMAC, обфускация, защита приложений.*

При разработке защищённых веб-приложений часто необходимо реализовывать алгоритмы выработки кодов аутентификации сообщений (MAC) на языке JavaScript

в браузере пользователя. При этом нарушитель имеет не только доступ к исходному коду криптографических алгоритмов и ключевой информации, но и возможность отладки и изменения программы, что позволяет рассматривать браузер как недоверенную среду. В данном контексте возможность вычисления кодов аутентификации, в отличие от обладания ключевой информацией, может не представлять существенного интереса для нарушителя.

В качестве примера рассмотрим веб-приложение, в котором для уменьшения поверхности атаки используется аутентификация HTTP-запросов на стороне клиента. Для осуществления подобной аутентификации возникает необходимость использования MAC для контролируемых параметров HTTP-запроса. В данном случае возможность вычислять MAC представляет для нарушителя существенно меньший интерес, чем сама ключевая информация. Зная ключ и алгоритм выработки MAC, нарушитель способен использовать эффективные автоматизированные средства для анализа веб-приложения. Обладая же лишь возможностью вычисления MAC при помощи исходного алгоритма, нарушитель вынужден генерировать все запросы через веб-браузер, используя стандартную функциональность веб-приложения, что существенно затрудняет и замедляет анализ приложения.

С целью затруднения извлечения нарушителем ключевой информации из приложения принято использовать положения модели «White-box Cryptography» [1]. В настоящее время для недоверенных сред известны лишь примеры реализации симметричных алгоритмов шифрования [2, 3] и неизвестно ни одного метода для схемы HMAC.

Одним из способов выработки MAC являются ключевые хэш-функции. Известны два основных способа построения ключевых хэш-функций. Первый — использование блочных шифров в режиме генерации имитовставки. Однако полученные таким образом MAC, как правило, имеют недостаточную длину, а алгоритм их вычисления может быть неэффективен. Кроме того, проблема получения реализации блочных шифров для недоверенных сред частично изучена, и на данный момент существует ряд таких реализаций шифров DES [2] и AES [3].

Второй способ — получение ключевых хэш-функций на основе бесключевых. Данный подход позволяет строить эффективно вычислимые ключевые хэш-функции и более гибко выбирать длину получаемого MAC. Для описания этого алгоритма рассмотрим классическую схему вычисления хэш-функций на основе одношагового сжимающего отображения.

В качестве сжимающего отображения выбирается функция двух переменных $f(x, y)$, где x и y — двоичные слова длины m и n соответственно. Важно отметить, что отображение f в данном построении полностью определяет свойства получаемой хэш-функции, а потому f должна быть односторонней и устойчивой к коллизиям. Далее для вычисления $h(M)$ сообщение M разбивается на блоки $M_1, \ldots, M_N$ длины m, которые последовательно передаются на вход сжимающему отображению следующим образом:

$$b_0 = \nu, \quad b_i = f(M_i, b_{i-1}), \quad i = 1, \ldots, N, \quad h(M) = b_N, \tag{1}$$

где ν — некоторое фиксированное начальное значение.

В случае, если длина сообщения M не кратна m, последний блок сообщения дополняется некоторым специальным образом до полного. Обозначим операцию дополнения $pad(x, p)$, результат её вычисления — сообщение x, дополненное до длины m при помощи p. Помимо непосредственно дописывания дополнения, для операции $pad(x, p)$ допустима также модификация сообщения x, например сложение x и p по модулю 2^m, как это происходит в алгоритме [4].

Очевидно, для построения ключевой хэш-функции на основе бесключевой ключ MAC должен быть некоторым образом добавлен к исходному сообщению. Ввиду того, что непосредственно приписывание ключа к началу или концу сообщения может существенно ослабить получаемую ключевую хэш-функцию, в [5] предлагается следующая схема построения:

$$H(k, x) = h(k, p_1, h(k, p_2, x)),$$

где p_1 и p_2 — дополнения ключа k до длины, кратной m, используемые при выполнении операций $pad(k, p_1)$ и $pad(k, p_2)$, а h — бесключевая хэш-функция, вычисляемая по схеме (1) .

Обратим внимание, что значение k, в соответствии с требованиями схемы, целиком попадает в первые блоки вычисления обоих хеш-значений. Данное наблюдение позволяет предвычислить значение h на данных блоках и тем самым избежать использования k в реализации алгоритма в открытом (или легко вычислимом) виде.

Разобьём ключ k на блоки $K_1, K_2, \ldots, K_l$ длины m. Положим

$$epad(k, p) = K_1||K_2|| \ldots ||pad(K_l, p),$$

где «||» — конкатенация строк.

Обозначим h_1 и h_2 хэш-функции, в которых b_0 равно $h(epad(k, p_1))$ и $h(epad(k, p_2))$ соответственно, а дальнейшее вычисление производится по схеме (1). Тогда нетрудно заметить, что

$$H(k, x) = h(k, p_1, h(k, p_2, x)) = h_1(h_2(x)).$$

То есть ключ k не используется в алгоритме в открытом виде, а только в составе свёрток $h(epad(k, p_1))$ и $h(epad(k, p_2))$. Извлечение ключа из данных свёрток является вычислительно трудной задачей ввиду требований к сжимающим отображениям, указанным выше.

Полученный алгоритм вычисления H удовлетворяет всем условиям модели «White-box Cryptography» [1]. Предложенный метод реализован для общепринятого алгоритма HMAC [4] на языке JavaScript в рамках экспериментального проекта jCrypto [6].

ЛИТЕРАТУРА

1. White-Box Cryptography: Protecting Cryptographic Keys in Software Applications. `http://www.whiteboxcrypto.com/`
2. *Chow W. S., Eisen P., Johnson H., and Van Oorschot P. C.* A White-box DES Implementation for DRM Applications // LNCS. 2003. V. 2696. P. 1–15.
3. *Chow W. S., Eisen P., Johnson H., and Van Oorschot P. C.* White-Box Cryptography and an AES Implementation // LNCS. 2003. V. 2595. P. 250–270.
4. RFC 2104. HMAC: Keyed-Hashing for Message Authentication. `https://tools.ietf.org/html/rfc2104`
5. *Menezes A. J., Van Oorschot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. N. Y.: CRC Press, 1997.
6. jCrypto: White-Box Cryptography Tools for ECMAScript Language. `https://github.com/tsu-iscd/jcrypto`

УДК 004.416.6 DOI 10.17223/2226308X/9/35

ОБ ИДЕНТИФИКАЦИИ ЗАЩИТНЫХ ЭКРАНОВ ВЕБ-ПРИЛОЖЕНИЙ В МОДЕЛИ MitB

Д. Н. Колегов, П. А. Линейцев

Рассматриваются существующие способы идентификации защитных экранов веб-приложений и их программная реализация в рамках модели нарушителя «Man in the Browser».

Ключевые слова: *безопасность приложений, защитные экраны веб-приложений, идентификация.*

Защитные экраны уровня приложения (Web Application Firewalls, WAF) применяются для обнаружения и предотвращения атак на веб-приложения. Применение защитных экранов не гарантирует безопасность веб-приложения, так как они сами могут содержать уязвимости реализации и конфигурирования. Одной из актуальных задач анализа защищённости веб-приложений является разработка программных средств идентификации защитных экранов на клиентской стороне веб-приложений в рамках модели «Man in the Browser» (MitB) [1]. В данной работе исследованы возможности идентификации экранов приложений в рамках модели MitB и реализован программный модуль для фрэймворка BeEF [2], реализующий данную функциональность.

Идентификация защитных экранов, как правило, реализуется на основе сигнатурного анализа следующих веб-сущностей: идентификаторы сессий, HTTP-заголовки, cookie, коды ответов и т. д. Известными средствами идентификации защитных экранов являются WAFW00F [3] и sqlmap [4]. Приведём пример модуля, идентифицирующего экран «Wallarm» в sqlmap на основе сигнатуры HTTP-заголовка «Server»:

```
retval = False
for vector in WAF_ATTACK_VECTORS:
    _, headers, _ = get_page(get=vector)
    retval = re.search(r"nginx-wallarm",
                       headers.get(HTTP_HEADER.SERVER, ""),
                       re.I) is not None
    if retval:
        break
```

Вместе с тем данные средства ограничены в применении и не могут быть использованы в модели MitB, являющейся основной с точки зрения анализа клиентской части веб-приложения. Для обеспечения возможности идентификации защитных экранов в модели MitB реализован программный модуль для фрэймворка BeEF (Browser Explotation Framework) с использованием известных баз сигнатур.

Разработанный модуль функционирует следующим образом: он отправляет стандартный HTTP-запрос, затем анализирует ответ, полученный от веб-приложения. Если это не дало никаких результатов в части идентификации экрана, то отправляется серия HTTP-запросов с различными векторами атак, что приводит к реакции защитного экрана при его наличии. Экран может добавить специальный заголовок с сигнатурой или выставить идентификатор сессии. Если защитный экран не удалось идентифицировать с помощью HTTP-запросов, то анализируются коды ответов веб-приложения.

Для проведения сигнатурного анализа необходима коллекция сигнатур защитных экранов. Для её составления использовались базы сигнатур средств WAFW00F [3] и

sqlmap [4], некоторые сигнатуры добавлены авторами. Сигнатуры хранятся в формате JSON. Пример сигнатуры рализованного модуля BeEF:

```
1 {
2   "name":"F5 BIG-IP ASM",
3   "cookie": ["TS[a-zA-Z0-9]{3,8}"],
4   "headers": []
5 }
```

ЛИТЕРАТУРА

1. *Alkorn W., Frichot C., and Orru M.* The Browser Hacker's Handbook. Indianapolis, John & Wiley Sons, 2014. 648 p.
2. The Browser Exploitation Framework Project. `http://beefproject.com/`
3. The WAFW00F project. `https://github.com/EnableSecurity/wafw00f`
4. The sqlmap project. `http://sqlmap.org/`

УДК 004.94 DOI 10.17223/2226308X/9/36

ЛЕГКОВЕСНАЯ РЕАЛИЗАЦИЯ МЕХАНИЗМА АТРИБУТНОГО УПРАВЛЕНИЯ ДОСТУПОМ ДЛЯ СУБД НА УРОВНЕ ЗАЩИТНОГО ЭКРАНА

Д. Н. Колегов, Н. О. Ткаченко

Рассматривается легковесная реализация механизмов атрибутного управления доступом для систем управления базами данных на уровне защитных экранов приложений (*Web Application Firewall*, *Database Firewall*), функционирующих в режиме прокси-сервера. Предлагается механизм проекции ролей для добавления элементов ролевого управления доступом.

Ключевые слова: *управление доступом, ABAC, RBAC, защитный экран, СУБД.*

В настоящее время политики безопасности для приложений являются, как правило, ролевыми (*RBAC*), атрибутными (*ABAC*) или гибридными, сочетающими в себе как ролевое, так и атрибутное управление доступом. Для каждого управления доступом в отдельности имеются или создаются детально проработанные стандарты [1, 2], но они ориентированы на реализацию в конечных системах, а не в защитных экранах приложений, а потому не могут быть использованы без существенной адаптации как к условиям функционирования защитных экранов в режиме прокси-сервера, так и к самим защищаемым системам управления базами данных (СУБД).

Задача ставится следующим образом. Имеется СУБД и заданная политика безопасности, которая не может быть реализована встроенными механизмами управления доступом этой СУБД. Необходимо реализовать эту политику безопасности без изменения конфигурации, исходного кода и данных на СУБД. Такая реализация называется неинвазивной и была предложена авторами в работах [3, 4]. Для решения поставленной задачи строится легковесный механизм атрибутно-ролевого управления доступом — *ABAC-lite*.

Реализуемый механизм состоит из следующих структурных элементов в терминологии *NIST ABAC* [1]. *Policy Enforcement Point* (*PEP*) отвечает за получение и парсинг *SQL*-запросов от клиента к серверу СУБД и формирование запросов средствами

протокола HTTP к *PDP*. *Policy Decision Point* (*PDP*) вычисляет решение о возможности получения доступа субъекта к сущности. *Policy Information Point* (*PIP*) реализует получение всех атрибутов субъектов и сущностей для принятия решения *PDP*. *Policy Administration Point* (*PAP*) отвечает за администрирование, представлления и хранения политики безопасности. В рамках реализации получены и используются следующие новые результаты.

Для связи атрибутного и ролевого управления доступом впервые используется механизм проекций. Пусть $e_1, \ldots, e_M$ — сущности, $r_1, \ldots, r_N$ — права доступа, $role_1, \ldots, role_K$ — роли, где $role_k = \{(e_i, r_j)\}$ для некоторых $i \in \{1, \ldots, M\}$, $j \in \{1, \ldots, N\}$, $k \in \{1, \ldots, K\}$. Проекцией ролей на сущность e_i будем называть набор вида $pr(e_i) = \{(role_k, r_j) : (e_i, r_j) \in role_k\}$. Данный механизм позволяет более легко реализовать гибридное атрибутное и ролевое управление доступом.

Политика безопасности представляет собой набор правил, составленных на специальном языке *AF Rules*, ориентированном на применение в графических пользовательских интерфейсах и представленном в нотации *JSON*. Правило состоит из условия и решения, которое применяется при выполненном условии. Правила проверяются в порядке их записи в политике. Условие правила может содержать атрибуты объектов Сессии (*session*), Пользователя (*user*), Ресурса (*resource*) и Окружения (*env*), логичесие операторы, операторы сравнения. Возможны два вида решения: разрешить или запретить. Последнее правило является правилом по умолчанию, условие данного правила всегда выполняется. Существует также возможность сконфигурировать способ выбора решения в политике [5]:

1) *firstApplicable* — будет выбрано первое решение из правила, условия которого выполнены;
2) *permitOverrides* — будет выбрано первое «разрешающее» правило. В отсутствие «разрешающих» правил или в случае невыполнения их условий возвращается решение по умолчанию;
3) *denyOverrides* — будет выбрано первое «запрещающее» правило. В отсутствие «запрещающих» правил или в случае невыполнения их условий возвращается решение по умолчанию.

В примере, приведённом ниже, проверяется наличие группы у пользователя, и если такая задана, то группа пользователя сравнивается с группой ресурса. При этом сравнение предполагает использование иерархии групп, которая описывается отдельно в виде дерева. Если группы не сравнимы с точки зрения заданной иерархии, то условие не выполняется. Если группа пользователя ниже по иерархии группы ресурса, то условие не выполняется. В остальных случаях последняя часть условия будет выполнена.

```
1 {
2  "and": [
3   {"session.groups>isSet": true},
4   {"session.groups>any": {"in":"resource.groups>rbac.hge"}}
5  ],
6     "decision":"permit"
7 }
```

В множество атрибутов, помимо атрибутов, свойственных сущностям СУБД (базы данных, таблицы, столбцы и т. д.), входят: уровень доступа, уровень конфиденциальности, роли, группы, тэги. Уровни доступа и конфиденциальности задаются числами.

В правиле может быть описан способ сравнения уровней, что позволяет реализовать управление доступом на основе меток. Группы — иерархическая структура, которая позволяет отразить внутреннюю структуру организации. Тэги позволяют определить принадлежность субъекта к какому-либо отделу внутри организации. С точки зрения ролевого механизма наиболее интересен способ задания ролей.

Для создания и назначения роли необходимо конфигурируемой сущности присвоить имя роли и привилегии. Пример конфигурации для таблицы *test* из базы данных *test_db* приведён ниже; здесь роль с именем *gen_dir* разрешает доступы типа *select*,*insert*,*delete* и *update* к сущности *test_dbtest*.

```
{
    "id":{
        "database":"test_db",
        "table":"test"
    },
    "level": 3,
    "tags": ["accounting"],
    "privileges":[
        {
           "name":"gen_dir",
           "rights":["select","insert", "delete", "update"]
        }
    ]
}
```

Для использования политики *PAP* в механизме управления доступом правила транслируются из формата *JSON* в код на языке *Python* с помощью разработанного транслятора. Сгенерированный модуль содержит функцию *checkAccess*, которая применяет все проверки, описанные в правилах политики, и в случае выполнения условий возвращает решение о предоставлении доступа.

Таким образом, в работе представлены результаты очередного этапа разработки легковесной системы ролевого и атрибутного управления доступом, ориентированной на применение в защитных экранах приложений. В системе разработаны новые механизмы: 1) проекции ролей, 2) проверки доступа по иерархии разрешающих и запрещающих ролей генерации, 3) генерации кода на основе политики безопасности.

ЛИТЕРАТУРА

1. *Hu V. C., Ferraiolo D., Kuhn R., et al.* Guide to Attribute Based Access Control (ABAC) Definition and Considerations [Электронный ресурс]. http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf
2. Role Based Access Control. American National Standarts Institute, Inc., 2004. http://profsandhu.com/journals/tissec/ANSI+INCITS+359-2004.pdf
3. *Колегов Д. Н., Ткаченко Н. О.* Неинвазивная реализация мандатного управления доступом в веб-приложениях на уровне СУБД //Прикладная дискретная математика. Приложение. 2015. № 8. С. 89–92.
4. *Колегов Д. Н., Ткаченко Н. О.* Неинвазивное устранение уязвимостей логического управления доступом в веб-приложениях [Электронный ресурс]. https://www.youtube.com/watch?v=SPiY6D3M0yE
5. *Brossard D.* Understanding XACML combining algorithms [Электронный ресурс]. https://www.axiomatics.com/blog/entry/understanding-xacml-combining-algorithms.html

Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНЫХ И УПРАВЛЯЮЩИХ СИСТЕМ

УДК 519.718 DOI 10.17223/2226308X/9/37

О НАДЁЖНОСТИ СХЕМ В БАЗИСЕ РОССЕРА — ТУРКЕТТА (В P_k)[1]

М. А. Алехина, О. Ю. Барсукова

Рассматривается реализация функций k-значной логики схемами из ненадёжных функциональных элементов в базисе Россера — Туркетта. Предполагается, что все элементы схемы независимо друг от друга подвержены инверсным неисправностям на выходах. Найдены верхняя и нижняя оценки ненадёжности схем, а также класс функций, для которых нижние оценки справедливы.

Ключевые слова: *функции k-значной логики, ненадёжные функциональные элементы, надёжность и ненадёжность схемы, инверсные неисправности на выходах элементов.*

Пусть $k, n \in \mathbb{N}$, $k \geqslant 3$, $E_k = \{0, 1, \ldots, k-1\}$, P_k — множество всех функций k-значной логики, т. е. функций $f(x_1, \ldots, x_n) : (E_k)^n \to E_k$. Рассмотрим реализацию функций из множества P_k схемами из ненадёжных функциональных элементов в базисе Россера — Туркетта $\{0, 1, \ldots, k-1, J_0(x_1), J_1(x_1), \ldots, J_{k-1}(x_1), \min\{x_1, x_2\}, \max\{x_1, x_2\}\}$.

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 $i \in E_k$ 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 $P_{f(\tilde{a}^n)\neq\tau}(S, \tilde{a}^n) = P_{\tau+1}(S, \tilde{a}^n) + P_{\tau+2}(S, \tilde{a}^n) + \ldots + P_{\tau+k-1}(S, \tilde{a}^n)$. В выражениях $\tau + 1$, $\tau + 2$,…, $\tau + k - 1$ сложение осуществляется по mod k. Например, если входной набор $\tilde{a}^n$ схемы S такой, что $f(\tilde{a}^n) = 0$, то вероятность появления ошибки на этом наборе равна

$$P_{f(\tilde{a}^n)\neq 0}(S, \tilde{a}^n) = P_1(S, \tilde{a}^n) + P_2(S, \tilde{a}^n) + \ldots + P_{k-1}(S, \tilde{a}^n) = \sum_{i=1}^{k-1} P_i(S, \tilde{a}^n).$$

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 ε, $0 < \varepsilon < 1/(2(k-1))$, подвержены инверсным неисправностям на выходах, т. е. каждый базисный элемент с функцией $\varphi(\tilde{x}^m)$, $m \in \mathbb{N}$, на любом входном наборе $\tilde{a}^m$, таком, что $\varphi(\tilde{a}^m) = \tau$, с вероятностью ε выдаёт любое из значений α, $\alpha \neq \tau \pmod k$. Поэтому вероятность ошибки на выходе любого базисного элемента равна $(k-1)\varepsilon$. Очевидно, что ненадёжность любого базисного элемента также равна $(k-1)\varepsilon$, а надёжность — $1 - (k-1)\varepsilon$.

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

Пусть $P_\varepsilon(f) = \inf P(S)$, где инфимум берется по всем схемам S из ненадёжных элементов, реализующим функцию $f(\tilde{x}^n)$. Схему A, реализующую f, назовем асимптотически оптимальной по надёжности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

Справедливы теоремы об оценках ненадёжности схем и классе функций, для схем которых нижняя оценка ненадёжности верна.

Теорема 1. Любую функцию $f \in P_k$ можно реализовать такой схемой S, что $P(S) \leqslant 3(k-1)\varepsilon + 90k^2\varepsilon^2$ при всех $\varepsilon \in (0, 1/(288k^4)]$.

Обозначим через $K(n)$ множество таких k-значных функций, зависящих от переменных $x_1, \ldots, x_n$ $(n \geqslant 3)$, что каждая из этих функций принимает все k значений 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 k-значной логики). Пусть $K = \bigcup\limits_{n=3}^{\infty} K(n)$.

Теорема 2. $|K(n)| \geqslant k^{k^n} - 2nk^{(k-1)k^{n-1}} - k(k-1)^{k^n}$.

Теорема 3. Пусть функция $f \in K$. Тогда для любой схемы S, реализующей f, при $\varepsilon \in (0, 1/(288k^4)]$ верно неравенство $P(S) \geqslant 3(k-1)\varepsilon - (k-1)(3k-1)\varepsilon^2 + k(k-1)^2\varepsilon^3$.

В заключение можно сделать следующие выводы:

1) Любую функцию из P_k можно реализовать схемой, функционирующей с ненадёжностью, асимптотически (при $\varepsilon \to 0$) не больше $3(k-1)\varepsilon$ (теорема 1).

2) Любую функцию из класса K (содержащего почти все функции из P_k) нельзя реализовать схемой с ненадёжностью, асимптотически (при $\varepsilon \to 0$) меньше $3(k-1)\varepsilon$ (теорема 3).

3) Схема, реализующая функцию $f \in K$ и удовлетворяющая условиям теоремы 1, является асимптотически оптимальной по надёжности и функционирует с ненадёжностью, асимптотически равной $3(k-1)\varepsilon$ при $\varepsilon \to 0$.

Таким образом, в базисе Россера — Туркетта: 1) любую функцию k-значной логики можно реализовать схемой, ненадёжность которой асимптотически (при $\varepsilon \to 0$) не больше $3(k-1)\varepsilon$; 2) для почти любой функции такая схема является асимптотически оптимальной по надёжности и функционирует с ненадёжностью, асимптотически равной $3(k-1)\varepsilon$ при $\varepsilon \to 0$.

В списке литературы приведены работы, в которых получены результаты по надёжности и ненадёжности схем в базисе Россера — Туркетта при $k = 3$ [1–4] и $k = 4$ [5–8]. Результаты для произвольного k получены впервые.

ЛИТЕРАТУРА

1. *Алехина М. А., Барсукова О. Ю.* О надежности схем, реализующих функции из P_3 // Известия высших учебных заведений. Поволжский регион. Физ.-мат. науки. 2012. № 1(21). С. 57–65.
2. *Алехина М. А., Барсукова О. Ю.* Оценки ненадежности схем в базисе Россера — Туркетта // Известия высших учебных заведений. Поволжский регион. Физ.-мат. науки. 2014. № 1(29). С. 5–19.
3. *Алехина М. А., Барсукова О. Ю.* Ненадёжность схем в базисе Россера — Туркетта // Прикладная дискретная математика. Приложение. 2014. № 7. С. 109–110.
4. *Барсукова О. Ю.* Синтез надежных схем, реализующих функции двузначной и трехзначной логик: дис. ... канд. физ.-мат. наук. Пенза, 2014. 87 с.
5. *Алехина М. А., Каргин С. П.* Асимптотически оптимальные по надежности схемы в базисе Россера — Туркетта в P_4 // Известия высших учебных заведений. Поволжский регион. Физ.-мат. науки. 2015. № 1. С. 38–54.

6. *Алехина М. А., Каргин С. П.* Об одном методе повышения надежности схем в базисе Россера — Туркетта // Труды IX Междунар. конф. «Дискретные модели в теории управляющих систем» (Москва и Подмосковье, 20–22 мая 2015 г.), посвященной 90-летию со дня рождения С. В. Яблонского. М.: МГУ, МАКС Пресс, 2015. С. 17–19.
7. *Алехина М. А., Каргин С. П.* Верхняя оценка ненадежности схем в базисе Россера — Туркетта (в P_4) // Сб. статей Междунар. науч.-технич. конф. «Проблемы автоматизации и управления в технических системах — 2015», посвященной 70-летию Победы в Великой Отечественной войне (г. Пенза, 19–21 мая 2015 г.) Пенза: Изд-во Пенз. ун-та, 2015. С. 315–317.
8. *Алехина М. А., Каргин С. П.* Нижние оценки ненадёжности схем в базисе Россера — Туркетта (в P_4) // Прикладная дискретная математика. Приложение. 2015. № 8. С. 104–105.

УДК 519.718 DOI 10.17223/2226308X/9/38

НЕНАДЁЖНОСТЬ СХЕМ ПРИ СЛИПАНИЯХ ВХОДОВ ЭЛЕМЕНТОВ[1]

М. А. Алехина, О. А. Логвина

Рассматривается реализация булевых функций схемами из ненадёжных функциональных элементов в некоторых полных конечных базисах. Предполагается, что каждый из элементов схемы независимо от других элементов подвержен дизъюнктивным (конъюнктивным) слипаниям входов. Показано, что в некоторых базисах любую булеву функцию можно реализовать схемой сколь угодно высокой надёжности, а в некоторых — схемой, ненадёжность которой равна нулю.

Ключевые слова: *ненадёжные функциональные элементы, надёжность схемы, ненадёжность схемы, слипание входов элементов.*

Задача синтеза надёжных схем, реализующих булевы функции, при константных неисправностях одного типа (например, только типа 0 на входах элементов) решена в полных неприводимых базисах из двухвходовых элементов [1], при константных неисправностях двух типов [2 – 4], при константных неисправностях четырёх типов на входах и выходах [5, 6].

В этой работе рассмотрим реализацию булевых функций схемами из ненадёжных элементов в полном конечном базисе B и исследуем модель неисправностей, в которой каждый элемент схемы подвержен дизъюнктивным (конъюнктивным) слипаниям входов, когда на оба входа базисного элемента при наличии неисправности подается дизъюнкция (конъюнкция) входных значений. Различные слипания переменных исследовались, например, в работах [7 – 10] при построении тестов.

Считаем, что 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 неисправные состояния элементы схемы переходят независимо друг от друга с вероятностью $\varepsilon \in (0, 1/2)$. 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 равна максимальному 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 $1 - P(S)$.

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

1. Дизъюнктивные слипания входов элементов

1.1. Пусть базис $B = \{x|y\}$ (где $x|y = \overline{x\&y}$ — штрих Шеффера) и на входах базисных элементов с вероятностью ε появляются дизъюнктивные слипания. Учитывая характер этих неисправностей, вычислим вероятности появления ошибок на выходе базисного элемента E при всех входных наборах этого элемента: $P_0(E,(00)) = 0$, $P_0(E,(01)) = P_0(E,(10)) = \varepsilon$, $P_1(E,(11)) = 0$. В этом случае [11] любую булеву функцию можно реализовать схемой сколь угодно высокой надёжности, т. е. схемой ненадёжность которой стремится к нулю. Построение такой схемы можно сделать так же, как в [2 – 7], причём для повышения надёжности используется одна и та же схема.

1.2. Пусть базис B содержит $x\&y$, $\bar{x}$ и на входах базисных элементов с вероятностью ε появляются дизъюнктивные слипания. Заметим, что инвертор при такой неисправности работает абсолютно надёжно. Возьмём конъюнктор и инвертор и соединим выход конъюнктора со входом инвертора. Построенная схема D реализует штрих Шеффера, а вероятности появления ошибок на выходе схемы D таковы: $P_0(D,(00)) = 0$, $P_0(D,(01)) = P_0(D,(10)) = \varepsilon$, $P_1(D,(11)) = 0$. В этом случае [11] любую булеву функцию можно реализовать схемой сколь угодно высокой надёжности, т. е. схемой, ненадёжность которой стремится к нулю.

1.3. Пусть базис $B = \{x \downarrow y\}$ (где $x \downarrow y = \overline{x \vee y}$ — стрелка Пирса) и на входах базисных элементов с вероятностью ε появляются дизъюнктивные слипания. Поскольку в неисправном состоянии базисный элемент также реализует стрелку Пирса, вероятность появления ошибки на выходе базисного элемента на каждом входном наборе равна нулю. Поэтому любую булеву функцию можно реализовать схемой, ненадёжность которой равна нулю.

1.4. Пусть базис B содержит $x \vee y$, $\bar{x}$ и на входах базисных элементов с вероятностью ε появляются дизъюнктивные слипания. Заметим, что инвертор при такой неисправности работает абсолютно надёжно. Возьмем дизъюнктор и инвертор и соединим выход дизъюнктора со входом инвертора. Построенная схема реализует стрелку Пирса, причём вероятность появления ошибки на выходе этой схемы на каждом входном наборе равна нулю. Поэтому любую булеву функцию можно реализовать схемой, ненадёжность которой равна нулю.

2. Конъюнктивные слипания входов элементов

2.1. Пусть базис $B = \{x|y\}$ и на входах базисных элементов с вероятностью ε появляются конъюнктивные слипания. Учитывая характер этих неисправностей, нетрудно проверить, что вероятность появления ошибки на каждом входном наборе равна нулю. Поэтому любую булеву функцию можно реализовать схемой, ненадёжность которой равна нулю.

2.2. Пусть базис B содержит $x\&y$, $\bar{x}$ и на входах базисных элементов с вероятностью ε появляются конъюнктивные слипания. Заметим, что инвертор при такой неисправности работает абсолютно надёжно. Возьмем конъюнктор и инвертор и соединим выход конъюнктора со входом инвертора. Построенная схема реализует штрих Шеффера, причём вероятность появления ошибки равна нулю на каждом из входных наборов. Поэтому любую булеву функцию можно реализовать схемой, ненадёжность которой равна нулю.

2.3. Пусть базис $B = \{x \downarrow y\}$ и на входах базисных элементов с вероятностью ε появляются конъюнктивные слипания. Учитывая характер этих неисправностей, вычислим вероятности появления ошибок на выходе базисного элемента E при всех входных наборах этого элемента: $P_0(E,(00)) = 0$, $P_1(E,(01)) = P_1(E,(10)) = \varepsilon$, $P_1(E,(11)) = 0$.

В этом случае [11] любую булеву функцию можно реализовать схемой сколь угодно высокой надёжности, т. е. схемой, ненадёжность которой стремится к нулю. Построение такой схемы можно сделать так же, как в [2 – 7], причём для повышения надёжности используется одна и та же схема.

2.4. Пусть базис B содержит $x \vee y$, $\bar{x}$ и на входах базисных элементов с вероятностью ε появляются конъюнктивные слипания. Заметим, что инвертор при такой неисправности работает абсолютно надёжно. Возьмем конъюнктор и инвертор и соединим выход конъюнктора со входом инвертора. Построенная схема C реализует стрелку Пирса, причём вероятности появления ошибок на выходе схемы C равны $P_0(C, (00)) = 0$, $P_1(C, (01)) = P_1(C, (10)) = \varepsilon$, $P_1(C, (11)) = 0$. В этом случае [11] любую булеву функцию можно реализовать схемой сколь угодно высокой надёжности, т. е. схемой, ненадёжность которой стремится к нулю.

Вывод: при дизъюнктивных (конъюнктивных) слипаниях входов элементов в некоторых базисах любую булеву функцию можно реализовать схемой сколь угодно высокой надёжности, а в некоторых — схемой, ненадёжность которой равна нулю.

ЛИТЕРАТУРА

1. *Алехина М. А.* Синтез, надежность и сложность схем из ненадежных функциональных элементов: дис. . . . докт. физ.-мат. наук. Пенза, 2004. 169 с.
2. *Алехина М. А., Барсукова О. Ю.* О ненадежности схем из функциональных элементов, подверженных двум типам неисправностей // Известия высших учебных заведений. Поволжский регион. Физ.-мат. науки. 2013. № 3. С. 33–50.
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.
4. *Alekhina M. A. and Barsukova O. Yu.* The reliability of circuits in the basis anticonjuction with constant faults of gates // Comput. Sci. Inform. Technol. 2014. V. 2(1). P. 51–54.
5. *Алехина М. А.* Синтез надежных схем при константных неисправностях на входах и выходах элементов // Известия высших учебных заведений. Поволжский регион. Физ.-мат. науки. 2015. № 2. С. 3–15.
6. *Алехина М. А.* Ненадёжность схем при константных неисправностях на входах и выходах элементов // Прикладная дискретная математика. Приложение. 2015. № 8. С. 100–102.
7. *Романов Д. С.* О диагностических тестах относительно локальных слипаний переменных в булевых функциях // Прикладная математика и информатика. 2010. Т. 36. С. 91.
8. *Romanov D. S.* Diagnostic tests for local coalescences of variables in Boolean functions // Computat. Math. Modeling. 2012. V. 23. P. 72–78.
9. *Морозов Е. В., Романов Д. С.* Проверяющие тесты для булевых функций при линейных локальных неисправностях входов схем // Дискретный анализ и исследование операций. 2015. Т. 22. № 1. С. 49–61.
10. *Морозов Е. В., Романов Д. С.* О проверяющих тестах относительно множественных линейных слипаний переменных // Материалы XI Междунар. семинара «Дискретная математика и ее приложения», посвященного 80-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2012 г.). М.: Изд-во механико-математического фак-та МГУ, 2012. С. 144–147.
11. *Тарасов В. В.* К синтезу надежных схем из ненадежных элементов // Математические заметки. 1976. Т. 20. № 3. С. 391–400.

Секция 6

ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ И ГРАФОВ

УДК 519.17 DOI 10.17223/2226308X/9/39

УТОЧНЕНИЕ НИЖНЕЙ ОЦЕНКИ ЧИСЛА ДОПОЛНИТЕЛЬНЫХ ДУГ МИНИМАЛЬНОГО ВЕРШИННОГО 1-РАСШИРЕНИЯ ОРИЕНТАЦИИ ЦЕПИ

М. Б. Абросимов, О. В. Моденова

Ранее был получен следующий результат: минимальное вершинное 1-расширение любой отличной от гамильтоновой ориентации цепи с числом вершин больше 4 содержит по крайней мере четыре дополнительные дуги. В данной работе удалось значительно уточнить эту оценку, а также получить верхнюю оценку на число дополнительных дуг.

Ключевые слова: *минимальное вершинное 1-расширение, ориентация цепи, отказоустойчивость.*

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным вершинным k-расширением* (МВ-kР) n-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1) граф G^* является вершинным k-расширением графа G, т. е. граф G вкладывается в каждый подграф графа G^*, получающийся удалением любых его k вершин;
2) граф G^* содержит $n + k$ вершин, т. е. $|V^*| = |V| + k$;
3) α^* имеет минимальную мощность при выполнении условий 1 и 2.

Понятие минимального вершинного k-расширения появилось в работе [1] как модель для исследования отказоустойчивости дискретных систем, здесь же доказывается, что минимальным вершинным 1-расширением n-вершинной цепи является $(n+1)$-вершинный цикл. В работе [2] доказывается, что это минимальное вершинное 1-расширение единственно с точностью до изоморфизма. Задача поиска минимального вершинного k-расширения для произвольного графа является вычислительно сложной [3], и в общем виде решение удалось получить лишь для некоторых классов графов.

Рассмотрим ориентации цепи. Очевидно, что ориентация цепи, являющаяся гамильтоновым графом, имеет единственное с точностью до изоморфизма минимальное вершинное 1-расширение — контур с одной дополнительной вершиной. В работах [4, 5] доказаны следующие результаты относительно ориентаций цепей.

Теорема 1. Среди всех ориентаций цепей только гамильтонова цепь имеет МВ-1Р с двумя дополнительными дугами.

Теорема 2. Любая ориентация цепи с числом вершин $n > 4$, отличная от гамильтоновой цепи, имеет минимальное вершинное 1-расширение с не менее чем 4 дополнительными дугами.

Общих схем, которые бы позволили построить минимальные вершинные 1-расширения для каких-либо ориентаций цепей, отличных от гамильтоновой, пока получить не удается. В связи с этим большой интерес представляет оценка на число дополнительных дуг минимальных вершинных 1-расширений. Обозначим эту величину $\mathrm{ec}(G)$.

Тогда оценка из последней теоремы может быть записана следующим образом: при $n > 4$

$$4 \leqslant \mathrm{ec}(P_n).$$

Полученный ранее результат удалось улучшить. Очевидно, что концевая вершина ориентации цепи может быть или источником, или стоком. Будем говорить, что концевые вершины цепи имеют один тип, если они одновременно являются источниками или стоками. В противном случае будем говорить, что концевые вершины имеют разный тип.

Заметим достаточно очевидный факт, который можно использовать для получения верхней оценки числа дополнительных дуг.

Теорема 3. Неориентированный цикл C_{n+1} при $n > 1$ является вершинным 1-расширением для любой ориентации цепи P_n.

В неориентированном цикле подразумевается, что ребро представляет собой пару встречных дуг. Из теоремы получается оценка $\mathrm{ec}(P_n) \leqslant n + 3$.

Теорема 4. Число дополнительных дуг негамильтоновой ориентации цепи P_n, имеющей концы разного типа:

$$\left\lceil \frac{n+1}{6} \right\rceil + 2 \leqslant \mathrm{ec}(P_n) \leqslant n + 3.$$

Теорема 5. Число дополнительных дуг MB-1P ориентации цепи P_n, имеющей концы одинакового типа:

$$\left\lceil \frac{n+1}{4} \right\rceil + 2 \leqslant \mathrm{ec}(P_n) \leqslant n + 3.$$

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.* О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2010. Т. 88. Вып. 5. С. 643–650.
4. *Абросимов М. Б., Моденова О. В.* Характеризация орграфов с малым числом дополнительных дуг минимального вершинного 1-расширения // Изв. Сарат. ун-та. Нов. сер. 2013. Т. 13. Сер. Математика. Механика. Информатика. Вып. 2. Ч. 2. С. 3–9.
5. *Абросимов М. Б., Моденова О. В.* Характеризация орграфов с тремя дополнительными дугами в минимальном вершинном 1-расширении // Прикладная дискретная математика. 2013. № 3. С. 68–75.

УДК 519.17 DOI 10.17223/2226308X/9/40

О КОЛИЧЕСТВЕ ОПТИМАЛЬНЫХ 1-ГАМИЛЬТОНОВЫХ ГРАФОВ С ЧИСЛОМ ВЕРШИН ДО 26 И 28

М. Б. Абросимов, С. А. Сухов

Граф называется 1-вершинно(рёберно)-гамильтоновым, если после удаления любой его вершины (ребра) получившийся граф является гамильтоновым; 1-вершинно(рёберно)-гамильтонов граф называется оптимальным, если он имеет минимально возможное число рёбер среди всех 1-вершинно(рёберно)-гамильтоновых графов с тем же числом вершин. В работе перепроверены полученные ранее данные для оптимальных 1-вершинно- и 1-рёберно-гамильтоновых графов, а также удалось вычислить новые значения для 28 вершин.

Ключевые слова: *оптимальный 1-гамильтонов граф, минимальное 1-расширение цикла, отказоустойчивость.*

J. P. Hayes в работе [1], а затем совместно с F. Harary в работах [2, 3] предложил графовую модель для исследования отказоустойчивости дискретных систем. Особое внимание было уделено системам, представимым циклами. В [1 – 3] предложены схемы построения одной оптимальной 1-отказоустойчивой реализации (минимального 1-расширения) цикла. Предложены и другие схемы [4 – 8].

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным вершинным k-расширением* (k — натуральное) n-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1) граф G^* является вершинным k-расширением графа G, т. е. граф G вкладывается в каждый подграф графа G^*, получающийся удалением любых его k вершин;
2) граф G^* содержит $n + k$ вершин, т. е. $|V^*| = |V| + k$;
3) α^* имеет минимальную мощность при выполнении условий 1 и 2.

Граф $G^* = (V^*, \alpha^*)$ называется *минимальным рёберным k-расширением* (MP-kP) n-вершинного графа $G = (V, \alpha)$, если выполняются следующие условия:

1) граф G^* является рёберным k-расширением G, т. е. граф G вкладывается в каждый граф, получающийся из G^* удалением любых его k рёбер;
2) граф G^* содержит n вершин, т. е. $|V^*| = |V|$;
3) α^* имеет минимальную мощность при выполнении условий 1 и 2.

Для минимальных вершинных и рёберных k-расширений циклов можно встретить эквивалентные определения.

Граф называется *k-вершинно-гамильтоновым*, если после удаления любых его k вершин и инцидентных им рёбер получившийся граф является гамильтоновым. Граф называется *k-рёберно-гамильтоновым*, если после удаления любых k рёбер получившийся граф является гамильтоновым; k-вершинно(рёберно)-гамильтонов граф называется *оптимальным*, если он имеет минимально возможное число рёбер среди всех k-вершинно(рёберно)-гамильтоновых графов с тем же числом вершин.

Известно, что задачи проверки вершинных (рёберных) k-расширений произвольных графов, так же как и задачи проверки k-вершинно(рёберно)-гамильтоновых графов, являются NP-полными [9]. Интересной представляется задача вычисления числа неизоморфных минимальных вершинных и рёберных k-расширений для различных графов. Рассмотрим случай $k = 1$.

Минимальные вершинные и рёберные 1-расширения циклов — это либо кубические графы, если число вершин чётно, либо графы с вектором степеней $(4, 3, \ldots, 3)$, если

число вершин нечётно [1 – 3]. Это позволяет использовать более эффективные способы для поиска всех расширений циклов. В 2000 г. проведён вычислительный эксперимент [6, 7, 10], в рамках которого удалось построить все минимальные вершинные и рёберные 1-расширения циклов с числом вершин до 14. В 2011 г. удалось дойти до 17 вершин [11]. В 2013 г. проведены следующие вычислительные эксперименты [12] с использованием наиболее эффективных из известных на сегодня способов генерации кубических графов [13, 14] и графов с вектором степеней $(4, 3, \ldots, 3)$ [15]. Удалось построить все минимальные вершинные и рёберные 1-расширения циклов с числом вершин до 26. Вычисления проводились на кластере Гентского университета.

В рамках данной работы удалось перепроверить полученные ранее результаты, а также получить новые значения для 28-вершинных графов. Для проведения вычислений разработана программа на языке C++ [16], в основе которой лежит параллельный алгоритм генерации всех неизоморфных реализаций вектора степеней [15]. Расчёты проводились на кластере высокопроизводительных вычислений ПРЦ НИТ СГУ. Полученные результаты представлены в таблице. В первом столбце приводится вектор степеней графа, во втором и третьем столбцах указывается число реализаций этого вектора степеней, являющихся оптимальными 1-рёберно-гамильтоновыми (О1-РГ) и 1-вершинно-гамильтоновыми (О1-ВГ) графами соответственно, в последнем столбце — число реализаций вектора степеней, являющихся О1-РГ- и О1-ВГ-графами.

Вектор степеней	Число О1-РГ	Число О1-ВГ	Общее число
(3^4)	1	1	1
$(4, 3^4)$	1	1	1
(3^6)	2	1	1
$(4, 3^6)$	2	2	2
(3^8)	4	2	2
$(4, 3^8)$	13	10	10
(3^{10})	13	7	6
$(4, 3^{10})$	87	63	63
(3^{12})	53	27	26
$(4, 3^{12})$	885	602	598
(3^{14})	320	158	154
$(4, 3^{14})$	10933	7203	7129
(3^{16})	2641	1396	1370
$(4, 3^{16})$	160145	104212	102786
(3^{18})	28643	16069	15843
$(4, 3^{18})$	2636205	1739987	1717103
(3^{20})	375906	227734	225312
$(4, 3^{20})$	47500069	32545889	32214688
(3^{22})	5672841	3740297	3713170
$(4, 3^{22})$	921357310	664225667	659673074
(3^{24})	95206332	68237411	67921892
$(4, 3^{24})$	19072278349	14515830380	14454468790
(3^{26})	1745426880	1346345125	1342594673
$(4, 3^{26})$	—	—	—
(3^{28})	34590425317	28311172759	28265410940

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. *Harary F. and Hayes J. P.* Edge fault tolerance in graphs // Networks. 1993. V. 23. P. 135–142.

3. *Harary F. and Hayes J. P.* Node fault tolerance in graphs // Networks. 1996. V. 27. P. 19–23.
4. *Mukhopadhyaya K. and Sinha B. P.* Hamiltonian graphs with minimum number of edges for fault-tolerant topologies // Inform. Process. Lett. 1992. V. 44. P. 95–99.
5. *Hsu L. H. and Lin C. K.* Graph Theory and Interconnection Networks. CRC Press, 2009.
6. *Абросимов М. Б.* О неизоморфных оптимальных 1-отказоустойчивых реализациях некоторых графов // Теоретические проблемы информатики и её приложений. Саратов: СГУ, 2000. Вып. 3. С. 3–10.
7. *Абросимов М. Б.* О неизоморфных минимальных реберных 1-расширениях графов // Теоретические проблемы информатики и её приложений. Саратов: СГУ, 2004. Вып. 6. С. 3–9.
8. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012.
9. *Абросимов М. Б.* О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2010. № 5(88). С. 643–650.
10. *Абросимов М. Б.* Минимальные вершинные расширения циклов с числом вершин не более одиннадцати. Саратов: СГУ, 2001. 17 с. Деп. в ВИНИТИ 14.08.2001, № 1869-В2001.
11. *Абросимов М. Б., Кузнецов Н. А.* О количестве минимальных вершинных и рёберных 1-расширений циклов с числом вершин до 17 // Прикладная дискретная математика. Приложение. 2012. № 5. С. 84–86.
12. *Бринкман Г., Абросимов М. Б.* О количестве минимальных расширений циклов с числом вершин до 26 и 28 // Дискретная математика, теория графов и их приложения: Тез. докл. Междунар. науч. конф. Минск, 11–14 ноября 2013 г. Мн.: Институт математики НАН Беларуси, 2013. С. 7–9.
13. *Brinkmann G.* Fast generation of cubic graphs // J. Graph Theory. 1996. V. 23. P. 139–140.
14. *Brinkmann G., Goedgebeur J., and McKay B. D.* Generation of cubic graphs // Discr. Math. Theor. Comp. Sci. 2011. V. 13(2). P. 69–80.
15. *Grund R.* Konstruktion schlichter Graphen mit gegebener Gradpartition // Bayreuther Mathematische Schriften. 1993. B. 44. S. 73–104.
16. *Сухов С. А.* DSR Generator. Свид. о гос. регистрации программы для ЭВМ № 2016610073. Зарегистрирована в Реестре программ для ЭВМ 11 января 2016 г.

УДК 519.1 DOI 10.17223/2226308X/9/41

ОБ ОДНОМ НАСЛЕДСТВЕННОМ ПРИЗНАКЕ В ЦИКЛИЧЕСКИХ ПОЛУГРУППАХ ГРАФОВ

Я. Э. Авезова, В. М. Фомичев

В циклической полугруппе орграфов исследован признак наличия петель в вершинах из заданного множества. Для показателя этого признака через длины контуров орграфа (образующего элемента циклической полугруппы) получены достижимые оценки и формулы для подсчёта точного значения. Применение формул показано на примере. Результаты позволяют оценить экспоненты широкого класса примитивных систем орграфов.

Ключевые слова: *признак, показатель признака, экспонент системы графов.*

Введение

Важной задачей в криптографических приложениях является определение экспонента системы орграфов $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_m\}$, обозначаемого $\exp \hat{\Gamma}$ (равносильное определение экспонента системы матриц дано в [1, с. 202]). Один из способов получения

оценки $\exp\hat{\Gamma}$ основан на построении примитивного орграфа Γ', являющегося словом в алфавите $\hat{\Gamma}$, то есть элементом полугруппы $\langle\hat{\Gamma}\rangle$, и оценке $\exp\Gamma'$, где, согласно универсальному критерию примитивности [2], орграф Γ' примитивный, если и только если он сильносвязный и имеет простые контуры взаимно простых длин.

Примитивный орграф Γ' может быть получен как произведение непримитивных орграфов, составляющих некоторую систему. Одно из условий примитивности орграфа Γ' связано, в частности, с наличием петель в определённом подмножестве вершин орграфа Γ_j^t при некотором $j \in \{1,\ldots,m\}$ и некотором натуральном t. В частности, пример такой системы $\hat{\Gamma}$ из двух графов рассмотрен в [3]. Настоящая работа посвящена исследованию свойства орграфа, связанного с наличием петель в определённом подмножестве вершин.

1. Полугрупповой признак наличия петель в заданном подмножестве вершин орграфов

Подмножество H полугруппы G, состоящее из всех элементов G, обладающих определённым свойством, называется признаком H (H-признаком) в полугруппе G. Если $H \leqslant G$ — подполугруппа, то H называется полугрупповым признаком в G [1, с. 178].

Пусть G — полугруппа орграфов с множеством вершин $V = \{1,\ldots,n\}$, $\varnothing \neq P \subseteq V$. В полугруппе G полугрупповым признаком (обозначим его P_{loop}) является, в частности, множество всех орграфов, имеющих петли в каждой вершине множества P.

Пусть $\Gamma \in G$. Обозначим $\langle\Gamma\rangle$ циклическую полугруппу, порождённую орграфом Γ. Показателем P_{loop}-признака в полугруппе $\langle\Gamma\rangle$ называется наименьшее натуральное t, при котором $\Gamma^t \in P_{\text{loop}}$ (обозначается $\operatorname{pok} P_{\text{loop}}$ или кратко l_P). Заметим, что $l_V = \operatorname{ord} g$, если Γ — граф подстановки g множества V.

Утверждение 1. Признак P_{loop} в полугруппе $\langle\Gamma\rangle$ не пуст, если и только если каждая вершина из P является циклической.

2. Оценки показателя признака наличия петель в заданном подмножестве вершин орграфов

Рассмотрим орграф Γ, все вершины которого из множества P являются циклическими. Обозначим в Γ: $\hat{C} = \{C_1,\ldots,C_k\}$ — множество k простых контуров; $l(C)$ — длина контура C; $V(C)$ — множество вершин контура C; $L(i)$ — множество длин контуров, проходящих через вершину i; $L^{[m]}(i)$ — множество не превосходящих натурального числа m длин контуров, проходящих через вершину i; $\Lambda(i)$ — множество длин простых контуров, проходящих через вершину i; $C_{\min,i}$ — кратчайший простой контур, проходящий через вершину i, $i \in V$.

Утверждение 2. Показатель признака P_{loop} равен

$$l_P = \min \bigcap_{i\in P} L(i). \tag{1}$$

Поскольку через каждую вершину $i \in P$ проходит бесконечно много контуров, применение (1) для вычисления точного значения показателя признака P_{loop} затруднительно. Для уточнения формулы получим ряд оценок l_P.

Запишем, что система контуров $\hat{C} = \{C_1,\ldots,C_k\}$ содержит множество P, если $P \subseteq V(C_1) \cup \ldots \cup V(C_k)$. Систему контуров $\hat{C} = \{C_1,\ldots,C_k\}$ назовём связной, если связной является часть графа Γ, совпадающая с $C_1 \cup \ldots \cup C_k$. Связную систему контуров, содержащую множество P, назовём P-сокращённой, если после удаления любого контура оставшаяся подсистема либо не является связной, либо не содержит

множество P. P-сокращённую систему $\hat{C} = \{C_1, \ldots, C_k\}$ назовём минимальной в Γ, если сумма длин её контуров принимает наименьшее значение. Заметим, что P-сокращённых и минимальных систем в орграфе Γ может быть несколько.

Далее полагаем $P = \{1, \ldots, p\}$.

Лемма 1. Пусть орграф Γ содержит связную систему контуров $\hat{C} = \{C_1, \ldots, C_k\}$, $k \geqslant 1$. Тогда в Γ имеется контур длины $l(\hat{C}) = l(C_1) + \ldots + l(C_k)$, обходящий однократно каждый контур системы $\hat{C}$.

Теорема 1. Если в орграфе Γ связная система контуров $\hat{C} = \{C_1, \ldots, C_k\}$ содержит множество P, то верны оценки

$$\max\{l(C_{\min,i}) \colon i \in P\} \leqslant l_P \leqslant l(\hat{C}). \tag{2}$$

Верхняя оценка (2) принимает наименьшее значение, если система $\hat{C}$ P-сокращённая и минимальная.

Теорема 2. Для любого разбиения множества $P = P_1 \cup \ldots \cup P_r$ выполнено

$$l_P \leqslant \mathrm{HOK}(l_{P_1}, \ldots, l_{P_r}). \tag{3}$$

Следствие 1 (для минимального разбиения множества P). Верна оценка

$$l_P \leqslant \min\{\mathrm{HOK}\{(\lambda_1, \ldots, \lambda_p) \in \Lambda(1) \times \ldots \times \Lambda(p)\}\}. \tag{4}$$

Оценка (4) позволяет уточнить (1), заменив бесконечные множества конечными.

Следствие 2. При $m = \mathrm{HOK}\{(\lambda_1, \ldots, \lambda_p) \in \Lambda(1) \times \ldots \times \Lambda(p)\}$ выполнено

$$l_P = \min \bigcap_{i \in P} L^{[m]}(i). \tag{5}$$

Уточним равенство (5) с использованием верхней оценки (2).

Следствие 3. Если в Γ связная система контуров $\hat{C}$ содержит множество P, то формула (5) верна при $m = \min\{l(\hat{C}), \min\{\mathrm{HOK}\{(\lambda_1, \ldots, \lambda_p) \in \Lambda(1) \times \ldots \times \Lambda(p)\}\}\}$.

Следствие 4. Пусть орграф Γ содержит компоненты сильной связности $\Gamma_1, \ldots, \Gamma_r$ с множествами вершин $V_1, \ldots, V_r$ соответственно и $P_i = P \cap V_i$, $i = 1, \ldots, r$. Тогда верна оценка (3).

Проиллюстрируем примером полученные результаты для показателя P_{loop}.

Пример 1. Граф Γ (рис. 1) состоит из компонент сильной связности Γ_1 и Γ_2. Компонента сильной связности Γ_1 представляет собой связную систему простых контуров $C_1 = (1, 2, 3)$, $C_2 = (3, 4)$ и $C_3 = (4, 5, 6, 7, 8)$ длин 3, 2 и 5 соответственно. Компонента сильной связности Γ_2 есть связная система простых контуров $C_4 = (9, 10)$, $C_5 = (10, 11)$ и $C_6 = (10, 11, 12)$ длин 2, 2 и 3 соответственно. Для орграфа Γ при некоторых P посчитаны оценки показателя l_P с помощью оценок (2) и (4) (табл. 1 и 2), а также точное значение показателя l_P (табл. 3) с помощью (5) или следствия 3.

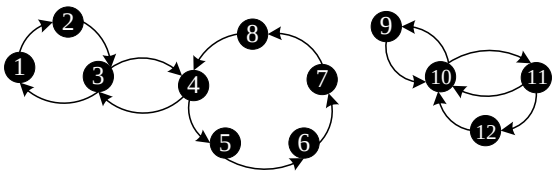


Рис. 1. Орграф Γ

Таблица 1

Верхняя оценка (2) показателя l_P для различных P

P	Минимальная связная система, содержащая P	Оценка (2)
$\{1,5\}$	$\{C_1, C_2, C_3\}$	$l_P \leqslant 3+2+5=10$
$\{1,4\}$	$\{C_1, C_2\}$	$l_P \leqslant 3+2=5$
$\{9,11\}$	$\{C_4, C_5\}$	$l_P \leqslant 2+2=4$

Таблица 2

Верхняя оценка (4) показателя l_P для различных P

P	$\Lambda(i)$, $i \in P$	Оценка (4)
$\{1,5\}$	$\Lambda(1)=\{3\}$, $\Lambda(5)=\{5\}$	$l_P \leqslant \mathrm{HOK}(3,5)=15$
$\{1,4\}$	$\Lambda(1)=\{3\}$, $\Lambda(4)=\{2,5\}$	$l_P \leqslant \min\{\mathrm{HOK}(3,2), \mathrm{HOK}(3,5)\}=6$
$\{9,11\}$	$\Lambda(9)=\{2\}$, $\Lambda(11)=\{2,3\}$	$l_P \leqslant \min\{\mathrm{HOK}(2,2), \mathrm{HOK}(2,3)\}=2$
$\{1,4,9,11\}$	$\Lambda(1)=\{3\}$, $\Lambda(4)=\{2,5\}$, $\Lambda(9)=\{2\}$, $\Lambda(11)=\{2,3\}$	$l_P \leqslant \min\{\mathrm{HOK}(3,2,2,2), \mathrm{HOK}(3,5,2,2)\}$, $\mathrm{HOK}(3,2,2,3), \mathrm{HOK}(3,5,2,3)\}=6$

Таблица 3

Показатель l_P для различных P, посчитанный с помощью (5)

P	m	$L^{[m]}(i)$, $i \in P$	l_P (5)
$\{1,5\}$	10	$L^{[10]}(1)=\{3,5,6,7,8,9,10\}$, $L^{[10]}(5)=\{5,7,9,10\}$	$l_P=\min L^{[10]}(1) \cap L^{[10]}(5)=5$
$\{1,4\}$	5	$L^{[5]}(1)=\{3,5\}$, $L^{[5]}(4)=\{2,4,5\}$	$l_P=\min L^{[5]}(1) \cap L^{[5]}(4)=5$
$\{9,11\}$	2	$L^{[2]}(9)=L^{[2]}(11)=\{2\}$	$l_P=2$
$\{1,4,9,11\}$	6	$L^{[6]}(1)=\{3,5,6\}$, $L^{[6]}(4)=\{2,4,5,6\}$, $L^{[6]}(9)=\{2,4,5,6\}$, $L^{[6]}(11)=\{2,3,4,5,6\}$	$l_P=\min\{5,6\}=5$

Из табл. 1 следует, что для $P=\{1,5\}$ и $\{1,4\}$ оценка (2) точнее оценки (4), а для $P=\{9,11\}$ соотношение обратное. Для $P=\{1,4,9,11\}$ с помощью следствия 3 получаем оценку $l_P \leqslant \mathrm{HOK}(2,5)=10$; величина оценки (4) более точная (см. табл. 2), но превышает точное значение, посчитанное в табл. 3.

Результаты показывают, что в некоторых случаях оценки (2) и (4) достижимы. Для многих орграфов с большим числом вершин сложность вычисления оценок показателя l_P по предварительным оценкам меньше, чем сложность определения точного значения. Однако для вычисления по формуле (5) точного значения l_P необходимо вычислить параметр m, являющийся верхней оценкой l_P, и затем построить пересечение множеств $L^{[m]}(1), \ldots, L^{[m]}(p)$.

Перспективное направление дальнейших исследований связано с алгоритмическими вопросами вычисления показателя P_{loop}-признака в полугруппе $\langle\Gamma\rangle$.

Выводы

Доказанные оценки показателя P_{loop}-признака могут быть использованы для оценки экспонентов некоторых примитивных систем орграфов. Полученные условия существенно расширяют область систем орграфов, для которой удаётся получить оценки экспонентов.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.

2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 116–121.
3. *Авезова Я. Э., Фомичев В. М.* Условия примитивности системы двух графов // Прикладная дискретная математика. Приложение. 2015. № 8. С. 113–114.

УДК 519.175.3 DOI 10.17223/2226308X/9/42

ПЕРЕЧИСЛЕНИЕ ПОМЕЧЕННЫХ ЦВЕТОЧНО-КОЛЁСНЫХ ГРАФОВ

В. А. Воблый, А. К. Мелешко

Получена точная формула для числа помеченных цветочно-колёсных графов с заданным количеством вершин и лепестков.

Ключевые слова: *корневой граф, граф колесо, цветочно-колёсный граф.*

Точкой сочленения связного графа называется его вершина, после удаления которой вместе с инцидентными ей рёбрами граф становится несвязным. Блок — это связный граф без точек сочленения, а также максимальный связный нетривиальный подграф, не имеющий точек сочленения. Корневой граф имеет одну выделенную вершину, называемую корнем. Колесо W_n — граф с $n \geqslant 4$ вершинами, который образован соединением единственной вершины со всеми вершинами $(n-1)$-цикла [1, с. 63]. Граф W_4 изоморфен полному графу K_4.

Цветочно-колёсный граф с m лепестками — это связный граф с одной точкой сочленения, у которого все m блоков (лепестков) — колёса, причём вершина, являющаяся осью колеса, не может быть точкой сочленения. Цветочно-колёсные графы представляют топологию коммуникационных, компьютерных и других сложных сетей [2]. Кроме того, перечисление графов тесно связано с теорией случайных графов; рандомизация колёсных подграфов сети может использоваться для защиты данных пользователей социальных сетей [3].

Теорема 1. Число $FW(n,m)$ помеченных цветочно-колесных графов с n вершинами и m лепестками при $n \geqslant 7$ и $m \geqslant 2$ равно

$$FW(n,m) = \frac{n!}{m!6^m}\sum_{i=0}^{r}\binom{m}{i}\binom{n-2m-i-2}{m-1}2^i,$$

где $r = \min(m, n-3m-1)$.

Доказательство. Пусть $C_m(z) = \sum\limits_{n=4}^{\infty} FW(n,m)\dfrac{z^n}{n!}$, NW_n — число помеченных колёс с n вершинами, RW_n — число помеченных корневых колёс с n вершинами, $R(z) = \sum\limits_{n=4}^{\infty} RW_n\dfrac{z^n}{n!}$.

Так как метку для оси колеса W_n можно выбрать n способами и число циклов с $n-1$ помеченными вершинами равно $(n-2)!/2$, то $NW_n = n(n-2)!/2$ при $n \geqslant 5$, $NW_4 = 1$.

Поскольку корень колеса W_n не должен быть вершиной-осью колеса, то метку для него можно выбрать $n-1$ способами и при $n \geqslant 5$ имеем $RW_n = (n-1)NW_n = n!/2$. Однако в случае W_4 (полный граф) осью может быть любая вершина и $RW_4 = nNW_4 = 4$. Поэтому имеем

$$R(z) = \frac{z^4}{6} + \frac{1}{2}\sum_{n=5}^{\infty} z^n = \frac{z^4}{6} + \frac{z^5}{2(1-z)}.$$

Граф с одной точкой сочленения может рассматриваться как корневой граф с корнем в точке сочленения. Такой граф можно получить склейкой в одну вершину непомеченных корней блоков. После склейки для непомеченной вершины вводится новая метка. Снятию метки с корня соответствует операция деления соответствующей производящей функции на z, а введению метки — операция умножения производящей функции на z [4, 5]. С учётом перестановок блоков вокруг точки сочленения получим

$$C_m(z) = \frac{z}{m!}\Big(\frac{R(z)}{z}\Big)^m = \frac{z}{m!}\Big(\frac{z^3}{6} + \frac{z^4}{2(1-z)}\Big)^m = \frac{z^{3m+1}(1+2z)^m}{m!6^m(1-z)^m}.$$

С помощью бинома Ньютона и ряда $(1-z)^{-m} = \sum\limits_{k=0}^{\infty}\binom{k+m-1}{m-1}z^k$ найдём

$$C_m(z) = \frac{z^{3m+1}}{m!6^m}\sum_{i=0}^{m}\binom{m}{i}2^i z^i \sum_{k=0}^{\infty}\binom{k+m-1}{m-1}z^k.$$

Следовательно, имеем $FW(n,m) = n![z^{-1}]C_m(z)z^{-n-1}$, где $[z^{-1}]$ — оператор формального вычета:

$$FW(n,m) = \frac{n!}{m!6^m}[z^{-1}]\sum_{i=0}^{m}\sum_{k=0}^{\infty}\binom{m}{i}\binom{k+m-1}{m-1}2^i z^{i+k+3m-n} =$$
$$= \frac{n!}{m!6^m}\sum_{i=0}^{m}\binom{m}{i}\binom{n-2m-i-2}{m-1}2^i.$$

Поскольку биномиальный коэффициент обращается в ноль при $m < i$ и $n-2m-i-2 < m-1$, верхний предел суммы равен $r = \min(m, n-3m-1)$. ■

ЛИТЕРАТУРА

1. *Харари Ф., Палмер Э.* Перечисление графов. М.: Мир, 1977.
2. *Bhatti A A., Nisar A., and Kanwal M.* Radio number of wheel like graphs // Int. J. Graph Theory in Wireless ad hoc Networks and Sensor Networks. 2011. No. 4. P. 39–57.
3. *Brankovic L., Lopez N., Miller M., and Sebe F.* Triangle randomization for social network data anonymization // Ars Math. Contemporanea. 2014. V. 7. No. 2. P. 461–477.
4. *Jin Y.-L.* Enumeration of labelled connected graphs and Euler graphs with only one cut vertex // Yokohama Math. J. 1977. No. 45. P. 125–134.
5. *Selkow S M.* The enumeration of labeled graphs by number of cutpoints // Discr. Math. 1998. No. 185. P. 183–191.

УДК 519.1+519.173 DOI 10.17223/2226308X/9/43

О ГРАФАХ ПОЛНОГО РАЗНООБРАЗИЯ ШАРОВ[1]

А. А. Евдокимов, Е. П. Куценогая, Т. И. Федоряева

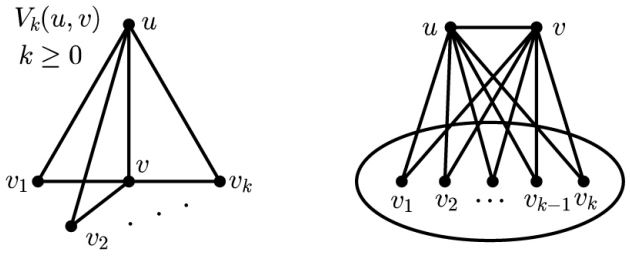
Изучается разнообразие шаров в конечных связных обыкновенных графах. Получен ряд свойств графов с полным разнообразием шаров. Как следствие, описаны кактусы с таким разнообразием шаров.

Ключевые слова: *граф, метрический шар, радиус шара, число шаров, вектор разнообразия шаров.*

[1]Работа поддержана грантом РФФИ, проект № 14-01-00507.

В случае дискретных метрических пространств шары заданного радиуса с центрами в различных вершинах не всегда различны, а могут совпадать. Данный эффект, когда шар имеет несколько центров, наблюдается в графах. О проблеме характеризации графов с заданным вектором числа различных шаров можно посмотреть в [1], а о связи свойств структуры шаров в графах и вложениями дискретных метрических пространств — в [2, 3]. Заметим также, что наличие в графе шаров с несколькими центрами позволяет, например, передавать управление с одного центра на другой, оставаясь при этом в зоне контроля или достижимости, определяемой шаром, в случае, например, «отказа» некоторого центра. Постановка подобных вопросов надёжности информационного взаимодействия и обмена данными в пределах заданных областей (окрестностях центров) приводит к задачам исследования взаимосвязей свойств структур или сетей с наличием в них окрестностей с «множественным центром», их числе, возможностей покрытия такими областями всего пространства и т. п. Далее связный конечный граф рассматривается как дискретное метрическое пространство с обычной метрикой пути [4]. Простейший пример графа с отмеченным эффектом даёт так называемый волан.

Определение 1 [5]. Граф $V_k(u, v)$, изображённый на рис. 1, *а*, называется *воланом на вершинах* u, v. Граф G *имеет волан*, если в G есть подграф $V_k(u, v)$ и $\deg_G u = \deg_G v = k + 1$ (рис. 1, *б*).



а *б*

Рис. 1. Волан

Если граф G имеет волан (рис. 1, *б*), то все шары с различными центрами $u, v \in V(G)$ совпадают для любого радиуса $i \geqslant 1$ [5].

Пусть $\tau_i(G)$ — число всех различных шаров радиуса i в метрическом пространстве конечного связного графа G.

Определение 2 [6]. Вектор $\tau(G) = (\tau_0(G), \tau_1(G), \ldots, \tau_d(G))$, где $d = \mathrm{d}(G)$ — диаметр графа G, называется *вектором разнообразия шаров* графа G.

Определение 3 [7]. Граф G обладает *локальным t-разнообразием шаров*, если $|V(G)| = \tau_0(G) = \tau_1(G) = \ldots = \tau_t(G)$, $0 \leqslant t < \mathrm{d}(G)$. Граф G с локальным t-разнообразием шаров при $t = \mathrm{d}(G) - 1$ 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 настоящей работе изучаются свойства конечных связных обыкновенных (т. е. не имеющих кратных рёбер и петель) графов с полным разнообразием шаров.

Теорема 1. Пусть G — граф диаметра $\mathrm{d}(G) \geqslant 3$ с полным разнообразием шаров. Тогда в графе G либо нет мостов, либо имеется единственный мост, один из концов которого является висячей вершиной.

Теорема 2. В классе n-вершинных графов диаметра d существует граф с полным разнообразием шаров тогда и только тогда, когда $n \geqslant 2d > 0$ или $n = d + 1 = 3$.

Как следствие из найденных свойств получено описание графов с полным разнообразием шаров для *кактусов* — связных графов, в которых нет рёбер, принадлежащих более чем одному простому циклу.

Теорема 3. Цикл и звезда — все с точностью до изоморфизма кактусы с полным разнообразием шаров.

ЛИТЕРАТУРА

1. *Евдокимов А. А., Федоряева Т. И.* О проблеме характеризации векторов разнообразия шаров // Дискрет. анализ и исслед. операций. 2014. Т. 21. № 1. С. 44–52.
2. *Евдокимов А. А.* Кодирование структурированной информации и вложения дискретных пространств // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7. № 4. С. 48–58.
3. *Евдокимов А. А.* Вложения графов в n-мерный булев куб и интервальное кодирование таблo // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 15–19.
4. *Харари Ф.* Теория графов. М.: Мир, 1973.
5. *Федоряева Т. И.* Операции и изометрические вложения графов, связанные со свойством продолжения метрики // Дискрет. анализ и исслед. операций. 1995. Т. 2. № 3. С. 49–67.
6. *Федоряева Т. И.* Разнообразие шаров в метрических пространствах деревьев // Дискрет. анализ и исслед. операций. Сер. 1. 2005. Т. 12. № 3. С. 74–84.
7. *Евдокимов А. А.* Локально изометрические вложения графов и свойство продолжения метрики // Сиб. журн. исслед. операций. 1994. Т. 1. № 1. С. 5–12.

УДК 519.1 DOI 10.17223/2226308X/9/44

ОБ АТТРАКТОРАХ В КОНЕЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ ОРИЕНТАЦИЙ ПОЛНЫХ ГРАФОВ

А. В. Жаркова

Рассматриваются конечные динамические системы ориентаций полных графов. Состояниями системы являются все возможные ориентации данного полного графа, а эволюционная функция задаётся следующим образом: динамическим образом данного орграфа является орграф, полученный из исходного путём переориентации всех дуг, входящих в стоки, других отличий между исходным орграфом и его образом нет. Приводится критерий принадлежности состояний системы аттракторам, описывается формирование аттракторов системы, их вид, длина.

Ключевые слова: *аттрактор, граф, конечная динамическая система, ориентация графа, полный граф, эволюционная функция.*

Под *ориентированным графом* (или, для краткости, *орграфом*) понимается пара $\overrightarrow{G} = (V, \beta)$, где V — конечное непустое множество (*вершины* орграфа), а $\beta \subseteq V \times V$ — отношение на множестве V (пара $(u, v) \in \beta$ называется *дугой* орграфа с *началом* u и *концом* v). Отношение β называют *отношением смежности*. *Неориентированным графом* (или, для краткости, *графом*) называется пара $G = (V, \beta)$, где β — симметричное и антирефлексивное отношение на множестве вершин V. Дуги неориентирован-

ного графа называют *рёбрами*. Орграф $\overrightarrow{G} = (V, \beta)$ называется *направленным графом* (или *диграфом*), если отношение α антисимметрично. Пусть $\overrightarrow{G} = (V, \beta)$ — некоторый орграф, $v \in V$ — одна из его вершин. *Степенью исхода* вершины $v \in V$ называется число $d^+(v)$ дуг орграфа $\overrightarrow{G} = (V, \beta)$, имеющих своим началом v; *степень захода* вершины v — это количество $d^-(v)$ дуг, имеющих v своим концом. Граф $G = (V, \beta)$ называется *полным*, если любые две его вершины соединены ребром. Полный граф с n вершинами обозначается K_n. Простой циклический путь в орграфе называется *контуром* [1].

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*. Таким образом, 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*. Получается, что каждый бассейн представляет собой контур с входящими в него деревьями. Контуры, в свою очередь, называются предельными циклами или *аттракторами*.

Основными проблемами теории конечных динамических систем являются задачи отыскания эволюционных параметров системы без проведения динамики. К их числу относятся свойства принадлежности состояния аттрактору, описание самих аттракторов системы. Написаны программы для ЭВМ, позволяющие вычислять различные параметры конечных динамических систем, ассоциированных с некоторыми типами графов [2]. Описаны аттракторы конечных динамических систем двоичных векторов, ассоциированных с ориентациями таких графов, как цепи, циклы, пальмы [3–5]. В данной работе приводится критерий принадлежности состояний аттракторам в конечных динамических системах ориентаций полных графов, описывается формирование аттракторов в данных системах, их вид, длина.

Пусть дан полный граф $G = (V, \beta)$, $V = \{v_1, v_2, \ldots, v_n\}$, $n > 1$, $m = n(n-1)/2$, где m — число рёбер. Придадим его рёбрам произвольную ориентацию, тем самым получив направленный граф $\overrightarrow{G} = (V, \beta)$, где отношение смежности β антирефлексивно и антисимметрично. Применим к полученному орграфу эволюционную функцию α, которая у данного орграфа одновременно переориентирует все дуги, входящие в *стоки* (вершины с нулевой степенью исхода), а остальные дуги оставляет без изменения, в результате чего получаем орграф $\alpha(\overrightarrow{G})$. Если проделать указанные действия со всеми возможными ориентациями данного графа, то получим карту данной динамической системы, состоящую из одного или нескольких бассейнов.

Таким образом, будем рассматривать конечную динамическую систему (Γ_{K_n}, α), $n > 1$, где через Γ_{K_n} обозначим множество всех возможных ориентаций полного графа K_n, $|\Gamma_{K_n}| = 2^m$, а эволюционная функция α задаётся следующим образом: если дан некоторый орграф $\overrightarrow{G} \in \Gamma_{K_n}$, то его динамическим образом $\alpha(\overrightarrow{G})$ является орграф, полученный из $\overrightarrow{G}$ одновременной переориентацией всех дуг, входящих в стоки, других отличий между $\overrightarrow{G}$ и $\alpha(\overrightarrow{G})$ нет.

В [6] рассматривается конечная динамическая система (Ω, α), где Ω — множество всех бесконтурных ориентаций данного графа, и замечается, что для полного графа существует $n!$ бесконтурных ориентаций, где $n!$ — количество перестановок его вершин, при этом система имеет $(n-1)!$ бассейнов, каждый из которых состоит исключительно из аттрактора длины n.

Определение 1. Под *вектором степеней захода* ориентированного графа $\overrightarrow{G} = (V, \beta)$ будем понимать вектор, компонентами которого являются степени захода всех его вершин, то есть $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$.

Очевидно, что в полном графе может быть не более одного стока.

Теорема 1 (критерий принадлежности состояния аттрактору). В конечной динамической системе (Γ_{K_n}, α), $n > 1$, состояние $\overrightarrow{G} \in \Gamma_{K_n}$ тогда и только тогда принадлежит аттрактору, когда в орграфе $\overrightarrow{G}$

1) нет стока
   или
2) вектор степеней захода представляет собой некоторую перестановку чисел $\{0, 1, \ldots, n-1\}$.

Теорема 2. В конечной динамической системе (Γ_{K_n}, α), $n > 1$, существуют аттракторы

1) длины 1, каждый из которых образован таким состоянием $\overrightarrow{G} \in \Gamma_{K_n}$, у которого нет стока;
2) длины n, каждый из которых состоит из состояний $\overrightarrow{G} \in \Gamma_{K_n}$, вектор степеней захода которых представляет собой некоторую перестановку чисел $\{0, 1, \ldots, n-1\}$, при этом каждый такой аттрактор представляет собой контур, в котором следующее состояние получается из предыдущего так: если $\overrightarrow{G}$ имеет вектор степеней захода $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$, то $\alpha(\overrightarrow{G}) \in \Gamma_{K_n}$ имеет вектор степеней захода $(d^-(v_1)+1, d^-(v_2)+1, \ldots, d^-(v_n)+1)$, где сложение осуществляется по модулю n,

и только они.

Заметим, что в конечной динамической системе (Γ_{K_n}, α), $n > 1$, количество аттракторов длины n равно $(n-1)!$, при этом количество состояний, принадлежащих данным аттракторам, равно $n!$. Например, карта конечной динамической системы (Γ_{K_6}, α), $|\Gamma_{K_6}| = 32768$, состоит из 26 744 бассейнов, при этом 27 344 состояния принадлежат аттракторам (что составляет $\approx 83\,\%$ от общего числа состояний); всего 26 624 аттрактора длины 1 и 120 аттракторов длины 6.

ЛИТЕРАТУРА

1. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, Физматлит, 1997.
2. *Власова А. В.* Исследование эволюционных параметров в динамических системах двоичных векторов // Свидетельство о государственной регистрации программы для ЭВМ № 2009614409, выданное Роспатентом. Заявка № 2009613140. Дата поступления 22 июня 2009 г. Зарегистрировано в Реестре программ для ЭВМ 20 августа 2009 г.
3. *Власова А. В.* Аттракторы конечных динамических систем, ассоциированных с цепями и циклами // Сб. тез. докл. конф. молодых ученых. Вып. 1. СПб.: СПбГУ ИТМО, 2011. С. 70–71.
4. *Жаркова А. В.* Количество аттракторов в динамических системах, ассоциированных с циклами // Матем. заметки. 2014. Т. 95. Вып. 4. С. 529–537.
5. *Жаркова А. В.* Аттракторы в конечных динамических системах двоичных векторов, ассоциированных с ориентациями пальм // Прикладная дискретная математика. 2014. № 3(25). С. 58–67.
6. *Barbosa V. C.* An atlas of edge-reversal dynamics. London: Chapman & Hall/CRC, 2001.

УДК 519.713.4 DOI 10.17223/2226308X/9/45

О ПРОСТЫХ УСЛОВНЫХ ЭКСПЕРИМЕНТАХ ИДЕНТИФИКАЦИИ ОБРАТИМЫХ АВТОМАТОВ НЕКОТОРОГО КЛАССА

А. О. Жуковская, В. Н. Тренькаев

Рассматривается класс сильносвязных автоматов, получаемых из некоторого инициального обратимого автомата с m состояниями, n входными и n выходными символами путём изменения его функции переходов в зависимости от ключа. Показывается существование простого условного эксперимента, идентифицирующего автоматы в этом классе и имеющего длину не более $mn(m+3)/2$.

Ключевые слова: *инициальный автомат, перестраиваемый автомат, обратимый автомат, сильносвязный автомат, идентификация автоматов, простые условные эксперименты.*

Следуя [1], назовём *перестраиваемым автоматом* набор из восьми объектов $R = (X, S, Y, K, \psi, \varphi, \delta_0, \delta_1)$, где $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_n\}$, $S = \{s_1, s_2, \ldots, s_m\}$ — множества входных символов, выходных символов и состояний соответственно; $K = \{k : k = ||k_{ij}||, k_{ij} \in \{0,1\}, i = 1, \ldots, n, j = 1, \ldots, m\}$ — множество ключей; $\varphi : X \times S \to Y$ — функция выходов; $\psi : X \times S \times K \to S$ — функция переходов, такая, что $\psi(x_i, s_j, k) = \psi_k(x_i, s_j) = \delta_{k_{ij}}(x_i, s_j)$ для некоторых функций $\delta_p : X \times S \to S$, $p \in \{0,1\}$.

Автомат R называется *обратимым*, если функция $\varphi_s(x) = \varphi(x, s)$ является биекцией для любого $s \in S$.

Обозначим через $A_{n,m}$ множество всех инициальных обратимых перестраиваемых автоматов R с фиксированными множествами X, S, Y, K и следующими свойствами:

1) среди $\varphi_s(x)$, $s \in S$, нет одинаковых биекций; 2) при любом $k \in K$ автомат $R_k = (X, S, Y, \psi_k, \varphi)$ сильносвязен.

Теорема 1. Для любого автомата $R \in A_{n,m}$ существует простой условный эксперимент длины не более $nm(m+3)/2$, идентифицирующий автоматы в классе $\{R_k : k \in K\}$.

ЛИТЕРАТУРА

1. *Тренькаев В. Н.* Реализация шифра Закревского на основе перестраиваемого автомата // Прикладная дискретная математика. 2010. № 3. С. 69–77.

УДК 519.7 DOI 10.17223/2226308X/9/46

О ТРАНЗИТИВНОСТИ ОТОБРАЖЕНИЙ, АССОЦИИРОВАННЫХ С КОНЕЧНЫМИ АВТОМАТАМИ ИЗ ГРУПП AS_p

М. В. Карандашов

Рассматривается вопрос определения свойства транзитивности автоматных отображений. Приводится общий критерий транзитивности автоматного отображения на словах длины $k \in \mathbb{N}$. Для автоматов из групп AS_p предложен алгоритм проверки транзитивности. Сложность представленного алгоритма зависит от числа состояний автомата и не зависит от длины входного слова; приведена верхняя граница сложности алгоритма.

Ключевые слова: *конечные автоматны, автоматные отображения группы AS_p, транзитивность.*

Под *детерминированным автоматом* будем понимать пятёрку объектов $A = (S, X, Y, \delta, \lambda)$, где S — множество состояний; X — входной алфавит; Y — выходной алфавит; $\delta : S \times X \to S$ — функция переходов; $\lambda : S \times X \to Y$ — функция выходов. Для всех рассматриваемых в работе автоматов $|S|, |X|, |Y| \in \mathbb{N}$ и $X = Y = \{0, 1, \ldots, p-1\}$, p — простое.

Пусть X^* обозначает множество всех конечных слов над алфавитом X. Действие функций δ и λ можно расширить на множество слов X^* следующими рекуррентными правилами: $\delta(s, x \cdot w) = \delta(\delta(s, x), w)$, $\lambda(s, x \cdot w) = \lambda(s, x) \cdot \lambda(\delta(s, x), w)$, $x \in X$, $w \in X^*$.

Автомат с выделенным начальным состоянием называют *инициальным*. Инициальный автомат будем обозначать через A_s, где s — начальное состояние автомата. Каждый инициальный автомат A_s определяет отображение $f_{A_s} : X^* \to Y^*$, называемое *автоматным*, такое, что $f_{A_s}(w) = \lambda(s, w)$.

Автоматное отображение f называют *транзитивным на словах длины* k, если оно порождает одноцикловую перестановку на X^k. Отображение f *транзитивно*, если оно транзитивно на X^k для любого натурального k. Транзитивные отображения представляют значительный интерес в силу того, что применяются для решения как теоретических, так и практических задач. В частности, описаны семейства транзитивных автоматных отображений [1].

Будем называть *состоянием с потерей* [2] такое состояние s, что $\lambda(s, x_1) = \lambda(s, x_2)$ для некоторых $x_1, x_2 \in X$, $x_1 \neq x_2$.

Теорема 1 [3]. Автоматное отображение $f_{A_s} : X^* \to X^*$ биективно на X^k тогда и только тогда, когда автомат A_s не содержит состояний с потерей, достижимых из s за k шагов.

Далее будем рассматривать только инициальные автоматы, порождающие биективные отображения. Следовательно, отображение f_{A_s} осуществляет перестановку множества X, которую будем обозначать σ_s.

Действие инициального конечного автомата на входные последовательности можно описать с помощью бесконечного сбалансированного дерева [4]. Обозначим дерево, ассоциированное с действием автомата A_s, символом $T(A_s)$. Обозначим через $T(A_s, k)$ мультимножество состояний автомата A, где состояние s' входит в $T(A_s, k)$ ровно столько раз, со сколькими вершинами k-го яруса $T(A_s)$ ассоциировано состояние s'.

Рассмотрим итерацию слова $w \in X^k$ автоматным отображением f_{A_s}. Пусть $f_{A_s}(w) = w_1$, $f_{A_s}(f_{A_s}(w)) = w_2$, $\ldots$, $f^m_{A_s}(w) = w$ и m — наименьшее из возможных. Составим кортеж из перестановок $\sigma_{\delta(s,w)}, \ldots \sigma_{\delta(s,w_{m-1})}$ и обозначим через $Ar(T(A_s), w)$.

Лемма 1. Автоматное отображение f_{A_s} действует транзитивно на словах длины $(k+1)$, где $k \in \mathbb{N}$, тогда и только тогда, когда одновременно выполняются следующие условия:

1) f_{A_s} действует транзитивно на словах длины k;
2) для всех $w \in X^k$ композиция $\sigma_{\delta(s,w)} \circ \sigma_{\delta(s,w_1)} \circ \ldots \circ \sigma_{\delta(s,w_{p^k-1})}$ элементов $Ar(T(A_s), w)$ является одноцикловой перестановкой.

Заметим, что для каждого простого p существует циклическая группа перестановок $\langle \sigma_+(p) \rangle$, где $\sigma_+(p) = (0\ 1\ \ldots\ (p-1))$ — образующий элемент группы [5]. Инициальные автоматы, где с каждым состоянием связана перестановка из $\langle \sigma_+(p) \rangle$, образуют группу AS_p [6]. Важным является тот факт, что $\langle \sigma_+(p) \rangle$ — абелева группа.

Тут и далее под автоматом будем понимать автомат из группы AS_p.

Пусть автомат A_s действует транзитивно на словах длины k. Следовательно, $Ar(T(A_s), w)$ является некоторым упорядочиванием мультимножества перестановок, ассоциированных с состояниями из $T(A_s, k)$. Более того, в силу коммутативности перестановок из $\langle\sigma_+(p)\rangle$, композиции элементов из $Ar(T(A_s), w)$ совпадают для всех возможных w, т. е. композиция элементов $Ar(T(A_s), w)$ однозначно определяется мультимножеством $T(A_s, k)$ и не зависит от выбора w. Следовательно, достаточно проверить, что композиция перестановок (в произвольном порядке), ассоциированных с состояниями из $T(A_s, k)$, является одноцикловой.

Введём матрицы M и $\widehat{M}$, а также векторы V_σ и R. По таблице переходов конечного автомата A построим матрицу смежности M размера $n \times n$. Значения элементов матрицы M вычисляются как мощности множеств $\{x : x \in X, \delta(s_i, x) = s_j\}$, где i, j — номера строки и столбца матрицы. Таким образом, i-я строка матрицы M^k описывает $T(A_{s_i}, k)$.

Построим вектор V_σ следующим образом. Как отмечено выше, с состоянием s_i автомата связана некоторая перестановка τ_i из $\langle\sigma_+(p)\rangle$. Следовательно, в силу цикличности группы $\langle\sigma_+(p)\rangle$, $\tau_i = \sigma_+(p)^{h_i}$, $h_i = 0, \ldots, (p-1)$. Сопоставим i-му элементу вектора V_σ число h_i. Положим $R_k = M^k \cdot V_\sigma^{\mathrm{T}}$, где i-й элемент есть степень перестановки $\sigma_+(p)$, получаемой при композиции перестановок, ассоциированных с $T(A_{s_i}, k)$. Таким образом, задача проверки транзитивности сводится к последовательному сравнению с нулём значений i-х ячеек R_k, $k \geqslant 1$.

Основной проблемой использования матрицы M является то, что количество попарно различных матриц M^k, $k \in \mathbb{N}$, бесконечно. Построим матрицу $\widehat{M}$ из M следующим образом. Каждому элементу m_{ij} матрицы M сопоставим элемент $\widehat{m}_{ij} = m_{ij} \bmod p$ матрицы $\widehat{M}$.

Лемма 2. Пусть $\widehat{R}_k = \widehat{M}^k \cdot V_\sigma^{\mathrm{T}}$. Тогда $r_i^k = \widehat{r}_i^k \pmod p$.

Заметим, что количество различных матриц $\widehat{M}$ для фиксированных p и n конечно и равно p^{n^2}. Составим на основе представленных результатов алгоритм проверки транзитивности автомата A_{s_i} (алгоритм 1). Можно показать, что строки матрицы $\widehat{M}^k$ не могут быть произвольными, а лишь такими, где сумма элементов строки кратна p.

Алгоритм 1. Алгоритм проверки транзитивности автомата

Вход: Конечный автомат $A_{s_i} \in AS_p$
Выход: `true`, если A_{s_i} транзитивен, `false` иначе

1: Построить матрицу $\widehat{M}$ и вектор V_σ по автомату A_{s_i}.
2: **Если** i-й элемент V_σ равен нулю, **то**
3: вернуть `false`.
4: Положить $k := 1$, $L := \varnothing$.
5: **Пока** $\widehat{M}^k \notin L$
6: $\widehat{R}^k := \widehat{M}^k \cdot V_\sigma^{\mathrm{T}}$.
7: **Если** i-й элемент $\widehat{R}^k$ сравним с 0 по модулю p, **то**
8: вернуть `false`.
9: Добавить $\widehat{M}^k$ в L, увеличить k на 1.
10: Вернуть `true`.

Теорема 2. Максимальное число умножений матриц, требуемое для остановки алгоритма, ограничено сверху числом $(p^{(n-1)} - 1)$.

Полученная в теореме 2 оценка сложности является достижимой, что было подтверждено численными экспериментами.

ЛИТЕРАТУРА

1. *Тяпаев Л. Б.* Транзитивные семейства автоматных отображений // Дискретные модели в теории управляющих систем: IX Междунар. конф., Москва и Подмосковье, 20–22 мая 2015. Труды / отв. ред. В. Б. Алексеев, Д. С. Романов, Б. Р. Данилов. М.: МАКС Пресс, 2015. С. 244–247.
2. *Гилл А.* Введение в теорию конечных автоматов. М.: Наука, 1966. 272 с.
3. *Карандашов М. В.* Исследование биективных автоматных отображений на кольце вычетов по модулю 2^k // Компьютерные науки и информационные технологии: Материалы Междунар. науч. конф. Саратов: Издат. центр «Наука», 2014. С. 148–152.
4. *Яблонский С. В.* Введение в дискретную математику: учеб. пособие для вузов. 2-е изд., перераб. и доп. М.: Наука, 1986. 384 с.
5. *Калужнин Л. А., Сущанский В. И.* Преобразования и перестановки: пер. с укр. 2-е изд., перераб. и доп. М.: Наука, 1985. 160 с.
6. *Алешин С. В.* Конечные автоматы и проблема Бернсайда о периодических группах // Матем. заметки. 1972. Т. 11. № 3. С. 319–328.

Секция 7

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

УДК 519.682 DOI 10.17223/2226308X/9/47

О СОВМЕСТНОСТИ СИСТЕМ СИМВОЛЬНЫХ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ И ИХ ПРИЛОЖЕНИИ

О. И. Егорушкин, И. В. Колбасина, К. В. Сафонов

Разрабатываются подходы к решению систем некоммутативных полиномиальных уравнений, возникающих в математической теории языков и грамматик; системы решаются в виде формальных степенных рядов (ФСР), которые выражают символьные неизвестные через символьные параметры. Всякому ФСР поставлен в соответствие его коммутативный образ — степенной ряд, который получается в предположении, что все символы обозначают коммутативные переменные, принимающие значения из поля комплексных чисел. Изучаются вопросы совместности системы некоммутативных символьных уравнений на основе исследования коммутативного образа этой системы.

Ключевые слова: *некоммутативные переменные, полиномиальные уравнения, формальный степенной ряд, коммутативный образ.*

Рассмотрим систему полиномиальных уравнений

$$P_j(z, x) = 0, \quad j = 1, \ldots, n, \tag{1}$$

$P_j(0, 0) = 0$, $j = 1, \ldots, n$, которая решается относительно символов $z = (z_1, \ldots, z_n)$ в виде формальных степенных рядов, зависящих от символов $x = (x_1, \ldots, x_m)$.

В математической теории языков и грамматик символы $z_1, \ldots, z_n, x_1, \ldots, x_m$ интерпретируют как алфавит, над которым определена некоммутативная операция умножения (конкатенации) и коммутативная операция формальной суммы, кроме того, определена коммутативная операция умножения на комплексные числа, и потому можно рассматривать символьные многочлены и ФСР с числовыми (комплексными) коэффициентами. В теории формальных языков приложение систем уравнений (1) состоит в том, что они являются грамматиками, порождающими определённые классы контекстно-свободных языков, языков непосредственно составляющих, языков в нормальной форме Грейбах и др. [1, 2]. При этом символы $x_1, \ldots, x_m$ называются терминальными и образуют словарь (алфавит) данного языка, а символы $z_1, \ldots, z_n$ называются нетерминальными и необходимы для задания грамматических правил; мономы являются предложениями (словами) языка, а ФСР, который является решением системы (1), рассматривают как порождённый грамматикой формальный язык, представляющий собой формальную сумму всех «правильных» предложений [1, 2].

Вопросы, связанные с решением символьных систем (1), изучены мало: основные трудности связаны с некоммутативностью умножения и отсутствием деления, препятствующих исключению неизвестных.

Целью данной работы является получение условий разрешимости системы (1) в терминах коммутативного образа этой системы, который получается в предположении, что все переменные, входящие в систему, принимают значения из поля комплексных чисел.

Предположим, что все мономы от $x_1, \ldots, x_m$ занумерованы в лексикографическом порядке по возрастанию степеней в последовательность $\{u_i : i = 0, 1, \ldots\}$, играющую роль универсального базиса. Тогда каждый ряд s можно однозначно записать в виде разложения по этому базису с числовыми коэффициентами $\langle s, u_i \rangle$ при мономах u_i:

$$s = \sum_{i=0}^{\infty} \langle s, u_i \rangle u_i. \tag{2}$$

Поставим в соответствие ФСР (2) его коммутативный образ $\mathrm{ci}(s)$ — степенной ряд, который получается из s в предположении, что символы $x_1, \ldots, x_m$ обозначают коммутативные переменные, принимающие значения из поля комплексных чисел [3].

Обозначим $z = z(x) = (z_1(x), \ldots, z_n(x))$ решение системы (1), представленное ФСР.

Теорема 1. Если $z = z(x)$ — решение некоммутативной системы уравнений (1) в виде символьных ФСР, то коммутативные ФСР $z = \mathrm{ci}(z(x))$ над полем комплексных чисел сходятся в окрестности нуля, определяя ростки голоморфных алгебраических функций, и являются решением коммутативной системы уравнений

$$\mathrm{ci}(P_1(z, x)) = \cdots = \mathrm{ci}(P_n(z, x)) = 0. \tag{3}$$

Обратное утверждение, вообще говоря, неверно. Так, система уравнений $z_1 - z_2 = = x_1 x_2$, $z_1 - z_2 = x_2 x_1$ несовместная, тогда как её коммутативный образ имеет бесконечно много решений: $z_1 = t + x_1 x_2$, $z_2 = t$, где t — произвольный ФСР.

Подчеркнём, что совместность, т. е. наличие решения, понимается для некоммутативной системы (1) и коммутативной системы (3) по-разному: в первом случае решением являются символьные ФСР, а во втором — точки в $\mathbb{C}^n$, параметризованные голоморфным в нуле алгебраическим отображением.

Теорему 1 можно сформулировать в эквивалентном виде.

Теорема 2. Если коммутативная система уравнений (3) несовместна, то и некоммутативная система (1) несовместна.

Таким образом, условия несовместности коммутативной системы уравнений также представляют интерес.

Известна теорема: если для якобиана системы голоморфных функций $\mathrm{ci}(P_1(z, x))$, $\ldots, \mathrm{ci}(P_n(z, x))$ имеет место тождество

$$\det \left(\frac{\partial(\mathrm{ci}(P_i(z, x)))}{\partial z_j} \right) \equiv 0,$$

то система уравнений (3) при каждом x либо не имеет решения в пространстве $\mathbb{C}_z^n$, либо все её решения в этом пространстве неизолированные [4, с. 39].

Покажем, что для некоммутативных систем уравнений (1) подобная альтернатива (решений нет либо решений бесконечно много) не имеет места.

Пример. Рассмотрим систему, состоящую из двух одинаковых уравнений:

$$x_1 z_1 + x_2 z_2 - x_1 x_2 - x_2 x_1 = 0.$$

Коммутативный образ этой системы имеет якобиан, тождественно равный нулю, и неизолированные решения.

Тем не менее исходная система некоммутативных уравнений имеет единственное решение. В самом деле, записав уравнение в виде $x_1(z_1 - x_2) - x_2(z_2 - x_1) = 0$, получим, что первое слагаемое принадлежит левостороннему идеалу, порождённому x_1, а второе — левостороннему идеалу, порождённому x_2. Очевидно, что сумма этих слагаемых может быть равна нулю только в случае, когда равны нулю оба слагаемых: $z_1 - x_2 = 0$, $z_2 - x_1 = 0$, следовательно, исходная система уравнений имеет единственное решение $z_1 = x_2$, $z_2 = x_1$.

Далее, можно показать, что одно символьное полиномиальное уравнение может 1) не иметь решений; 2) иметь конечное число решений; 3) иметь бесконечно много решений, что принципиально отличается от свойств уравнений с комплексными переменными.

Более подробно указанные вопросы изложены в работе [5].

ЛИТЕРАТУРА

1. *Глушков В. М., Цейтлин Г. Е., Ющенко Е. Л.* Алгебра. Языки. Программирование. Киев: Наукова думка, 1973.
2. *Salomaa A. and Soitolla M.* Automata-Theoretic Aspects of Formal Power Series. N.Y.: Springer Verlag, 1978.
3. *Семенов А. Л.* Алгоритмические проблемы для степенных рядов и контекстно-свободных грамматик // Доклады АН СССР. 1973. № 212. С. 50–52.
4. *Айзенберг Л. А., Южаков А. П.* Интегральные представления и вычеты в многомерном комплексном анализе. Новосибирск: Наука, 1979.
5. *Egorushkin O. I., Kolbasina I. V., and Safonov K. V.* On solvability of systems of symbolic polynomial equations // J. Siberian Federal University. Mathematics and Physics. 2016. No. 2(9). P. 166–172.

УДК 004.4’422 DOI 10.17223/2226308X/9/48

ТРАНСЛЯТОР ЯЗЫКА ЛЯПАС-Т НА ЯЗЫК АССЕМБЛЕРА ДЛЯ ОС WINDOWS И LINUX

В. Н. Князев, М. С. Князева

Представлены результаты по созданию транслятора с языка ЛЯПАС-Т на язык ассемблера fasm. Цель разработки — популяризация ЛЯПАСа как претендента на роль национального языка программирования для создания доверенных программ и построения защищённых компьютерных систем. Для написания транслятора использовались генераторы лексических и синтаксических анализаторов flex и Bison в целях приведения грамматики ЛЯПАСа к общепринятому виду и получения эффективного LALR-анализатора.

Ключевые слова: *ЛЯПАС-Т, транслятор, компьютерная безопасность, программирование.*

ЛЯПАС — русский язык программирования, возрождаемый Томским государственным университетом (ТГУ) в целях создания доверенного программного обеспечения и защищённых компьютерных систем [1, 2]. Учитывая масштабы этих целей, считаем важным создание и распространение свободного транслятора с ЛЯПАСа для современных операционных систем (ОС). Это необходимо для обучения программи-

стов на ЛЯПАСе, пока не разработана ОС, поддерживающая ЛЯПАС изначально. Для достижения этой цели поставлены и решены следующие задачи:

— **Описание грамматики ЛЯПАСа-Т**. Из источников [3 – 5], а также из личной переписки с сотрудниками ТГУ собраны и обобщены сведения о синтаксисе и семантике ЛЯПАСа-Т.
— **Создание программы для построения синтаксического дерева**. Написаны программы для flex и Bison, связка которых генерирует LALR-парсер, строящий синтаксическое дерево программы на ЛЯПАСе-Т [6].
— **Создание трансляторов для ОС Windows и Linux**. Реализованы соответствующие программы, генерирующие код на языке ассемблера по синтаксическому дереву.

Реализованы некоторые алгоритмы дискретной математики на ЛЯПАСе-Т, демонстрирующие возможности языка:

— Алгоритм быстрого перемножения многочленов и длинных чисел на основе алгоритма Кули — Тьюки быстрого преобразования Фурье. Примеры комбинации его с алгоритмом Винограда для поиска свёртки длины маленьких простых чисел [7].
— Алгоритмы факторизации: ρ-метод Полларда, метод квадратичного решета [7].
— Алгоритм Миллера — Рабина проверки простоты чисел [7].

ЛИТЕРАТУРА

1. *Агибалов Г. П.* К возрождению русского языка программирования // Прикладная дискретная математика. 2012. № 3. С. 77–84.
2. *Торопов Н. Р.* Язык программирования ЛЯПАС // Прикладная дискретная математика. 2009. № 2. С. 9–25.
3. *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.
4. *Broslavskiy O. V.* AES in LYaPAS // Прикладная дискретная математика. Приложение. 2013. № 6. С. 102–104.
5. *Гречнев С. Ю., Стефанцов Д. А.* Модификация ЛЯПАСа для разработки ОС // Прикладная дискретная математика. Приложение. 2015. № 8. С. 129–131.
6. *Ахо А. В., Лам М. С., Сети Р., Ульман Д. Д.* Компиляторы: принципы, технологии и инструментарий. М.: Вильямс, 2008.
7. *Крэндалл Р., Померанс К.* Простые числа. Криптографические и вычислительные аспекты. М.: УРСС, 2011.

УДК 004.43+004.4’42+004.451 DOI 10.17223/2226308X/9/49

МОДУЛЬНЫЙ ТРАНСЛЯТОР С ЯЗЫКА ЛЯПАС

Д. А. Стефанцов, В. О. Сафонов, В. В. Першин, С. Ю. Гречнев, П. А. Томских

Сообщается о разработке модульного транслятора с языка программирования ЛЯПАС. Цель разработки — упрощение создания транслятора с ЛЯПАСа, написанного на ЛЯПАСе. Процесс трансляции разделяется на этапы, за каждый из которых ответствен один из модулей транслятора. Модули выполнены в виде исполняемых программ и обмениваются данными с помощью файлов. Для представления промежуточных результатов работы модулей используются вспомогательные языки программирования.

Ключевые слова: *ЛЯПАС, язык программирования, операционная система.*

Язык программирования ЛЯПАС [1] возрождается в Томском государственном университете силами кафедры защиты информации и криптографии с целью иметь высокопроизводительную доверенную вычислительную систему для создания доверенного ПО, разработки и исследования криптографических алгоритмов, управления сетевым оборудованием. Главные компоненты создаваемой системы — транслятор с ЛЯПАСа [2] и ОС ЛЯПАС [3].

В [3] описаны этапы создания ОС ЛЯПАС, после завершения которых появляется возможность разработки и компиляции ОС ЛЯПАС и прикладных программ для неё в самой ОС ЛЯПАС. Для выполнения последних двух этапов требуется транслятор с ЛЯПАСа, написанный на ЛЯПАСе. Модульный транслятор с языка ЛЯПАС — вспомогательное средство для создания требуемого.

Создание транслятора с ЛЯПАСа на ЛЯПАСе — трудоёмкая задача, требующая решения множества отдельных небольших проблем. Предлагается реализация транслятора, разделённого на модули, каждый из которых может быть написан на любом языке программирования независимо от других модулей. Такой транслятор может быть создан изначально, например, на C++ и переписан по частям на ЛЯПАСе. В качестве способа связи модулей выбрана передача данных через файлы в формате, не зависящем от языка реализации модулей.

1. Архитектура транслятора

Транслятор $t : X_1 \to X_{n+1}$ состоит из модулей $m_i : X_i \to X_{i+1}$, таких, что $t = m_1 \circ \circ m_2 \circ \ldots \circ m_n$; X_i — входной язык модуля m_i и выходной язык модуля m_{i-1}. Входной язык X_1 транслятора t — ЛЯПАС, выходной язык X_{n+1} — язык ассемблера; языки X_i, $i \in \{2, \ldots, n\}$, используются для представления промежуточных результатов трансляции; $X_1, \ldots, X_{n+1}$ называются *языками транслятора* t; $X_2, \ldots, X_n$ называются *внутренними языками транслятора* t. Возможно $X_i = X_j$ при $i \neq j$, например, входной и выходной языки оптимизирующего модуля могут совпадать.

Модули реализованы в виде исполняемых программ, каждая из которых может быть написана на любом языке программирования, независимо от других модулей. Обмен данными между модулями осуществляется с помощью временных файлов, содержащих программы на внутренних языках транслятора. Поскольку программы на внутренних языках транслятора анализируются, в основном, модулями транслятора и их разработчиками, эти программы можно представить в виде, лёгком для разбора машиной, и только во вторую очередь — человеком. Дополнительное требование к такому способу представления программ — наличие библиотек для разбора и генерации данных этим способом для большинства существующих языков программирования. В качестве такого способа представления выбран JSON [4]; в качестве библиотек для работы с JSON на языках C и C++ выбраны [5] и [6] соответственно.

На этапе, когда модули транслятора переписываются на ЛЯПАСе, необходима библиотека, конвертирующая программы, представленные с помощью JSON, в программы, представленные с помощью типов данных ЛЯПАСа — логических и символьных комплексов и чисел. Эта библиотека для представления внутренних языков транслятора (ПВЯТ) реализуется как обёртка над библиотекой для формата JSON на C. Такая технология добавления библиотек C в ЛЯПАС уже опробована на работе с файлами и сокетами в ОС GNU/Linux. После того, как все модули будут переписаны на ЛЯПАСе, необходимость в формате JSON отпадёт и модули смогут обмениваться программами, представленными с помощью комплексов и чисел. Промежуточные результаты трансляции можно будет записывать во временные файлы в бинарном виде с помощью

вспомогательной библиотеки, подпрограммы которой имеют те же заголовки, что и подпрограммы библиотеки ПВЯТ.

Примером такой архитектуры модульного транслятора с ЛЯПАСа частично послужил транслятор CompCert [7] с C, обладающий формальным (проверяемым машиной) доказательством корректности своей работы. В будущем планируется разработка формально верифицированного транслятора с ЛЯПАСа по образцу CompCert. Одной из задач, необходимых для достижения этой цели, является создание модульного транслятора, так как формальное доказательство упрощается разбиением его на части, соответствующие модулям. Другая важная задача для достижения указанной цели — создание операционной семантики ЛЯПАСа [8].

2. Языки транслятора

В настоящий момент в модульном трансляторе предусмотрены одиннадцать языков. Первый (входной язык транслятора) — ЛЯПАС. Одиннадцатый (выходной язык транслятора) — язык ассемблера. Внутренние языки модульного транслятора не имеют собственных имён, они пронумерованы числами от 2 до 10.

Язык 2. Программы на языке 2 представляют собой программы на ЛЯПАСе с добавленным к ним именем файла, в котором хранится данная программа. Это необходимо для вывода сообщений об ошибках на следующих этапах трансляции.

Язык 3. Программы на языке 3 представляют собой результат лексического анализа программы на ЛЯПАСе — последовательность *токенов*. Помимо типа и значения лексемы, в токенах хранится информация о нахождении лексемы в исходной программе на ЛЯПАСе: имя файла, номер строки и символа в строке. Транслятор из языка 2 в язык 3 реализуется на языке C с использованием генератора flex [9].

Язык 4. Программы на языке 4 представляют собой результат синтаксического анализа программы — дерево разбора. Узлы дерева разбора, помимо символов грамматики, содержат информацию об их нахождении в исходной программе на ЛЯПАСе. Транслятор из языка 3 в язык 4 реализуется на языке C с использованием генератора bison [10].

Язык 5. Язык 5 представляет собой язык абстрактной одноадресной машины, каждый регистр общего назначения которой соответствует переменной ЛЯПАСа. Каждый вызов подпрограммы на ЛЯПАСе создаёт в машине новый набор регистров. Копирование входных и выходных параметров выполняется абстрактной машиной автоматически. Поскольку ЛЯПАС изначально создавался для компиляции в язык одноадресной машины Урал-1 [1], язык 5 является наиболее простым выходным языком для трансляции с ЛЯПАСа из всех следующих языков модульного транслятора. Транслятор с языка 4 в язык 5 реализуется на языке C++.

Язык 6. Язык 6 отличается от языка 5 тем, что представляет собой язык абстрактной двухадресной машины. Переход от одноадресной к двухадресной машине облегчает явную работу со стеком на следующих этапах трансляции и помогает более эффективно производить оптимизацию получаемой программы. Транслятор с языка 5 в язык 6 реализуется на языке C++.

Язык 7. Язык 7 отличается от языка 6 явной работой со стеком при вызове подпрограмм. Механизм композиции функций, описанный в [2], реализуется транслятором с языка 6 в язык 7.

Язык 8. Язык 8 отличается от языка 7 наличием ограниченного количества регистров общего назначения и неограниченным количеством пронумерованных областей памяти, с которыми регистры могут обмениваться значениями. Набор регистров соот-

ветствующей абстрактной машины — один для всех вызовов всех подпрограмм. Транслятор с языка 7 в язык 8 производит отображение переменных ЛЯПАСа, каждая из которых до сих пор хранилась в собственном регистре абстрактной машины, в ограниченный набор регистров новой абстрактной машины. В необходимых местах значения регистров сохраняются в памяти для последующего восстановления. Количество регистров абстрактной машины для языка 8 — параметр. Это необходимо для обеспечения независимости транслятора в язык 8 от конкретной аппаратной архитектуры.

Язык 9. Язык 9 отличается от языка 8 наличием операций захвата и освобождения памяти. Адресная арифметика в данном языке запрещена. Операции с комплексами производятся в явном виде, в отличие от предыдущих языков, в которых абстрактная машина имела элементарные операции для работы с комплексами.

Язык 10. Язык 10 отличается от языка 9 наличием адресной арифметики при работе с памятью. Из языка 10 происходит трансляция в язык ассемблера. Производится замена некоторых специальных операций абстрактной машины для языка 10 вызовами заранее подготовленных ассемблерных процедур.

3. Этапы разработки

Разработка модульного транслятора с ЛЯПАСа разделяется на три этапа.

1) На первом этапе языки реализации модулей — C и C++, формат представления внутренних языков программирования — JSON.
2) На втором этапе производится перенос модулей на язык ЛЯПАС. Языки реализации модулей — C, C++ и ЛЯПАС, формат представления промежуточных данных — JSON. На этом этапе требуется библиотека ПВЯТ для модулей на ЛЯПАСе.
3) На третьем этапе все модули переписаны на ЛЯПАСе. Формат JSON становится ненужным. Библиотека ПВЯТ модифицируется так, что она записывает в файлы данные не в формате JSON, а напрямую — комплексы и целые числа. На этом этапе производится оптимизация транслятора и его перекомпиляция с помощью предыдущей версии этого же транслятора.

Заключение

В настоящий момент разработка модульного транслятора находится на первом этапе. Создана цепочка модулей, транслирующая исходную программу на ЛЯПАСе в язык 5. Ведётся разработка модуля, переводящего программу с языка 5 в язык 6.

На втором этапе планируется использование существующего монолитного транслятора с ЛЯПАСа, разработанного в ТГУ, который используется в настоящий момент [3].

ЛИТЕРАТУРА

1. *Торопов Н. Р.* Язык программирования ЛЯПАС // Прикладная дискретная математика. 2009. № 2. С. 9–25.
2. *Гречнев С. Ю., Стефанцов Д. А.* Модификация ЛЯПАСа для разработки ОС // Прикладная дискретная математика. Приложение. 2015. № 8. С. 129–131.
3. *Стефанцов Д. А., Томских П. А.* Разработка операционной системы на языке ЛЯПАС // Прикладная дискретная математика. Приложение. 2015. № 8. С. 134–135.
4. JSON. ECMA-404 The JSON Data Interchange Standard. `http://www.json.org/`. 2016.
5. Jansson: C library for encoding, deconding and manipulating JSON data. `https://github.com/akheron/jansson`. 2016.

6. Jsoncpp: A C++ library for interacting with JSON. https://github.com/open-source-parsers/jsoncpp. 2016.
7. CompCert. Compilers you can formally trust. http://compcert.inria.fr/. 2016.
8. *Жуковская А. О., Стефанцов Д. А.* Операционная семантика ЛЯПАСа // Прикладная дискретная математика. Приложение. 2015. № 8. С. 131–132.
9. flex: The Fast Lexical Analyzer. http://flex.sourceforge.net/. 2016.
10. GNU Bison. A general-purpose parser generator. https://www.gnu.org/software/bison/. 2016.

УДК 519.714 DOI 10.17223/2226308X/9/50

МЕТОДЫ СИНТЕЗА ФРАГМЕНТОВ ПРЕДИКАТНЫХ ПРОГРАММ[1]

М. С. Чушкин, В. И. Шелехов

Рассматривается задача синтеза фрагментов предикатной программы. Синтезируемая программа определяется в форме композиции подпрограмм, полученных применением правил синтеза. Задача синтеза иллюстрируется на примере эффективной программы вычисления чисел Фибоначчи.

Ключевые слова: *формальная операционная семантика, программный синтез, дедуктивная верификация.*

1. Язык предикатного программирования

Программа на языке P_0 определяется следующей конструкцией:

$$<\textit{имя предиката}>\ (<\textit{аргументы}>:<\textit{результаты}>)\{<\textit{оператор}>\},$$

аргументы и результаты — непересекающиеся наборы имён переменных.

Предположим, что x, y и z обозначают разные непересекающиеся наборы переменных. Набор x может быть пустым, наборы y и z не пусты. Простейшим оператором является *вызов предиката* $A(x : y)$. *Операторами* языка P_0 являются следующие конструкции: $B(x : z); C(z : y)$ — последовательный оператор, $B(x : y)\ ||\ C(x : z)$ — параллельный оператор и $if\ (e)\ B(x : y)\ else\ C(x : y)$ — условный оператор.

Операционную семантику программы $H(x : y)$ определим в виде предиката: $R(H)(x, y) \equiv$ для значения набора x исполнение программы H всегда завершается и существует исполнение, при котором результатом вычисления является значение набора y [1].

Тотальная корректность (далее просто корректность) программы относительно *спецификации* в виде *предусловия* $P(x)$ и *постусловия* $Q(x, y)$ определяется формулой

$$\forall x\ (P(x) \Rightarrow [\forall y\ R(H)(x, y) \Rightarrow Q(x, y)]\ \&\ \exists y\ R(H)(x, y)).$$

2. Задача синтеза

Пусть $Q(x, y)$ — некоторая формула, связывающая между собой аргументы x и результаты y. Целью синтеза является получение (возможно, недетерминированным образом) программы $H(x : y)$, вычисляющей значение результатов y из аргументов x.

Будем говорить, что *синтезом формулы* $Q(x, y)$ является оператор $H(x : y)$ и предусловие $P(x)$ в виде формулы, и писать

$$\lceil Q(x, y) \rceil = H(x : y), \quad \lfloor Q(x, y) \rfloor = P(x),$$

[1]Работа поддержана грантом РФФИ, проект № 16-01-00498.

если существует программа $H(x : y)$, корректная относительно спецификации в виде предусловия $P(x)$ и постусловия $Q(x, y)$. Предусловие при этом описывает контекст, в рамках которого происходит вычисление.

Правила синтеза строятся на базе правил доказательства корректности в системе дедуктивной верификации [2].

Утверждение 1 (Condition Rule). Для некоторой формулы $Q(x, y)$ истинны следующие тождества:

$$\lceil Q(x,y)\rceil = if\ (e(x))\ \lceil e(x) \Rightarrow Q(x,y)\rceil\ else\ \lceil !e(x) \Rightarrow Q(x,y)\rceil,$$
$$\lfloor Q(x,y)\rfloor = e(x)?\lfloor e(x) \Rightarrow Q(x,y)\rfloor : \lfloor !e(x) \Rightarrow Q(x,y)\rfloor.$$

Утверждение 2 (Call Rule). Пусть $Q(x, y)$ — некоторая формула. Если существуют такие формулы $Q'(x, x')$ и $f(x', y)$, что $\forall x, y\ (Q(x, y) \Leftrightarrow \exists x'\ (Q'(x, x')\ \&\ f(x', y)))$, $F(x : y) = \lceil f(x, y)\rceil$ и истинно одно из следующих утверждений:

1) $f(x', y)$ — рекурсивный вызов и $Q'(x, x')\ \&\ m(x') < m(x)$, где m — некоторая функция меры, заданная на аргументах формулы f;
2) $f(x', y)$ — нерекурсивный вызов,

то истинны тождества $\lceil Q(x, y)\rceil = \lceil Q'(x, x')\rceil$; $F(x' : y)$, $\lfloor Q(x, y)\rfloor = \lfloor Q'(x, y)\rfloor$.

3. Пример

Рассмотрим формулу, описывающую числа Фибоначчи:

```
fib(i) := (i = 0 or i = 1) ? i : fib(i- 1) + fib(i - 2);
q(i, r) := r = fib(i);
```

Очевидной программой является реализация функции `fib` в виде условного оператора и двух рекурсивных вызовов. Такая программа будет неэффективна, так как рекурсия не является хвостовой. В предикатном программировании для приведения рекурсии к хвостовому виду используется метод обобщения исходной задачи.

Введём дополнительные параметры-накопители $current = fib(j)$ и $previous = fib(j - 1)$ для некоторого $j \leqslant i$. Формула для обобщённой задачи выглядит следующим образом:

```
g(i, j, current, previous, last) := 1 <= j & j <= i &
  current = fib(j) & previous = fib(j - 1) & last = fib(i);
```

Синтез формулы $q(i, r)$ начинается с применения правила *Condition Rule* с формулой $e(i) \equiv (i = 0 \text{ or } i = 1)$. Истинность посылки правила при этом проверяется с помощью SMT-решателя. Следом применяется правило *Call Rule* с вызовом $g(i, 1, 0, 1, r)$ в качестве вызова формулы. Посылки правила также проверяются с помощью решателя. Результатом синтеза является следующая предикатная программа:

```
main(i: r)
pre true
post q(i, n)
{
    if (i = 0 or i = 1)
        r = i
    else
        G(i, 1, 0, 1: r);
}
```

Синтез формулы $g(i, j, current, previous, last)$ также осуществляется с помощью правил *Condition Rule* и *Call Rule*, условия $i = j$ и формулы $g(i, j + 1, current + previous, current, last)$ для рекурсивного вызова генерируемой программы. Истинность посылок правил позволяет синтезировать следующую программу:

```
G(i, j, current, previous: last)
pre true
post g(i, j, current, previous, last)
{
    if (i = j)
        last = current
    else
        G(i, j + 1, current + previous, current: last);
}
```

Выбор правила на очередном шаге осуществляется методом перебора, указанным в работе [3]; выбор выражения в правилах *Condition Rule* и *Call Rule* — методом перебора, указанным в [4].

Предельная цель проекта — разработать алгоритмы и методы синтеза программы по её спецификации и спецификации обобщённой задачи. Предполагается интегрировать различные методы синтеза функциональных программ, предлагаемых, например, в работе [3].

ЛИТЕРАТУРА

1. *Шелехов В. И.* Семантика языка предикатного программирования // 5-я Всерос. конф. «Знания — Онтологии — Теории». ИМ СО РАН, Новосибирск, 2015. С. 15.
2. *Чушкин М. С.* Методы дедуктивной верификации предикатных программ // Труды 2-й Междунар. конф. «Инструменты и методы анализа программ». Кострома, 2014. С. 205–214.
3. *Jacobs S., Kuncak V., and Suter Ph.* Reductions for synthesis procedures // Verification, Model Checking, and Abstract Interpretation. 2013. LNCS. V. 7337. P. 88–107.
4. *Alur R., Bod'ik R., Juniwal G., et al.* Syntax-guided synthesis // FMCAD, 2013. P. 1–8.

Секция 8

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.7 DOI 10.17223/2226308X/9/51

ПРИМЕНЕНИЕ АЛГОРИТМОВ РЕШЕНИЯ ПРОБЛЕМЫ БУЛЕВОЙ ВЫПОЛНИМОСТИ К ПОСТРОЕНИЮ РАЗНОСТНЫХ ПУТЕЙ В ЗАДАЧАХ ПОИСКА КОЛЛИЗИЙ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ СЕМЕЙСТВА MD[1]

И. А. Грибанова

Представлен новый метод построения разностных путей в задаче поиска коллизий криптографических хеш-функций, основанный на использовании алгоритмов решения проблемы булевой выполнимости. На начальном этапе метода строится пропозициональная кодировка задачи поиска коллизий рассматриваемой хеш-функции. Затем в полученную кодировку добавляются (в виде КНФ) дополнительные ограничения. Как правило, это значения целочисленных разностей на сообщения, дающие коллизию, а также на отдельные фрагменты дифференциального пути. В качестве отправной точки поиска можно использовать некоторый известный либо случайный дифференциальный путь (во втором случае наличие коллизий, удовлетворяющих такому пути, не гарантируется). Задача варьирования значений разности переменных, кодирующих заполнение хеш-регистров, сводится к SAT. Для эффективного решения соответствующих серий SAT-задач написана MPI-программа, работающая на вычислительном кластере. Основным результатом стало построение дифференциального пути для задачи поиска коллизий криптографической хеш-функции MD4, отличного от известных.

Ключевые слова: *криптографическая хеш-функция, коллизия, разностные атаки, задача о булевой выполнимости (SAT), хеш-функции семейства MD.*

Криптографические хеш-функции являются важным примитивом, используемым в многочисленных приложениях современной криптографии. Хеш-функция — это всюду определённая алгоритмически вычислимая функция вида $\chi : \{0,1\}^* \mapsto \{0,1\}^C$, где C — некоторая константа, называемая длиной хеша. При $n > C$ в $\{0,1\}^*$ обязательно найдутся такие $x_1, x_2 \in \{0,1\}^n$, $x_1 \neq x_2$, что имеет место $\chi(x_1) = \chi(x_2)$. В этом случае говорят, что сообщения x_1, x_2 дают коллизию. К криптографическим хеш-функциям предъявляется ряд дополнительных требований, кратко суммировать которые можно так: задачи, так или иначе связанные с обращением хеш-функции, должны быть вычислительно трудными. В частности, высокую вычислительную трудность должна иметь и задача поиска коллизий.

Многие современные криптографические хеш-функции имеют в своей основе конструкцию Меркля — Дамгарда [1, 2], в соответствии с которой процесс построения хеш-образа исходного сообщения выглядит как последовательность итераций, на каждой из которых происходит обновление содержимого специальных регистров, далее назы-

[1]Работа выполнена при частичной финансовой поддержке РФФИ, проект № 14-07-00403а.

ваемых хеш-регистрами. На начальном шаге в хеш-регистры записываются константы, определённые в спецификации алгоритма. Затем содержимое хеш-регистров итеративно обновляется за счёт последовательного замешивания в них подписываемого сообщения. Длина хеш-регистра для различных алгоритмов может варьироваться от 128 до 512 битов, а число итераций, называемых далее шагами, от 48 до 80. Данные в хеш-регистрах разделены на слова длиной 32 или 64 бита. К наиболее популярным криптографическим хеш-функциям, основанным на конструкции Меркля — Дамгарда, относятся функции семейства SHA, а также функции семейства MD (MD4, MD5, RIPEMD).

В 2004–2005 гг. коллективом китайских криптографов, возглавляемым К. Ванг (X. Wang), был предложен подход к поиску коллизий криптографических хеш-функций семейства MD [3, 4]. Данная атака получила название разностной, или дифференциальной из-за сходства подхода, лежащего в её основе, с дифференциальным криптоанализом. Основная идея «атаки Ванг» заключается в попытке дополнить уравнения, задающие хеш-функцию, дополнительными ограничениями, которые резко сужают пространство поиска коллизий. Далее мы описываем основу метода Ванг, подразумевая, что рассматривается задача поиска коллизии хеш-функции MD4. Рассмотрим два процесса вычисления хеш-значений MD4 для двух 512-битных сообщений, традиционно обозначаемых через M, M'. Обозначим через H и H' хеш-регистры, заполняемые при вычислении хеш-значений M, M'. На шаге с фиксированным номером k в H и H' записаны некоторые 32-битные слова. На эти слова, рассматриваемые как целые числа, накладываются дополнительные ограничения, имеющие вид целочисленных разностей, обозначаемых через δ_k. Разность между значениями хеш-регистров на последнем шаге должна быть равна нулю, что означает условие равенства хешей: $\chi(M) = \chi(M')$, то есть сообщения M, M' дают коллизию. Множество значений δ_k для всех или части шагов (в MD4 число шагов равно 48) задаёт так называемый дифференциальный (разностный) путь. На сообщения M, M' также накладывается дополнительное ограничение, имеющее вид разности для соответствующих целых 512-битных чисел.

В [5] для задачи поиска коллизий хеш-функций семейства MD успешно применён SAT-подход; более точно, реализована SAT-версия разностной «атаки Ванг». Как результат, при помощи SAT-решателя `minisat` были найдены одноблоковые коллизии для хеш-функции MD4 и представлены реалистичные оценки времени поиска двухблоковых коллизий для MD5. Во всех случаях использовались разностные пути, представленные в [3, 4]. В [6] аналогичные задачи решены с более высокой эффективностью и построено семейство специального вида двухблоковых коллизий хеш-функции MD5; для сведения задач поиска коллизий MD4 и MD5 к SAT использован программный комплекс `Transalg` [7, 8].

В ряде последующих работ [9 – 11] представлены попытки построения новых дифференциальных путей, отличных от приведённых в [3, 4]. Наиболее успешными в этом плане можно считать результаты [11]. Особо отметим, что во всех этих случаях новые дифференциальные соотношения являлись результатом громоздких построений, фактически выполняемых авторами «вручную». Мы предлагаем автоматизировать данный процесс за счёт использования современных технологий решения SAT, имея в виду работу [5] как пример автоматизации «атаки Ванг» посредством SAT.

На данном этапе новые разностные соотношения для значений хеш-регистров, позволяющие быстро находить коллизии, построены для функции MD4. Остановимся кратко на основах разработанного метода. Начальным этапом является построение

пропозициональной кодировки алгоритма вычисления хеш-функции; для этой цели используется комплекс `Transalg`. Результатом является построение двух КНФ (так называемых «шаблонов» [8]) C и C' над множествами переменных X и X', $X \cap X' = \varnothing$. Возможности `Transalg` позволяют отслеживать связь между переменными, входящими в C, C', и содержимым хеш-регистров, получаемым в процессе вычисления хеш-образов сообщений M и M'. На переменные в C, C', кодирующие заполнение хеш-регистров на последнем шаге, накладывается условие их логической эквивалентности. Полученная в результате КНФ $\tilde{C}$ выполнима тогда и только тогда, когда существуют сообщения M и M', дающие коллизию. К КНФ C можно конъюнктивно приписывать различные дополнительные условия. В частности, к $\tilde{C}$ может быть приписана КНФ C_Δ, принимающая значение 1 тогда и только тогда, когда разность целых чисел, заданных 512-битными векторами M и M', равна некоторой константе Δ.

Пусть $C_{\delta_k=c}$ — КНФ, принимающая значение 1 тогда и только тогда, когда переменная δ_k принимает значение c. Поскольку c — 32-битная константа, не представляет труда перебрать все возможные её значения и рассмотреть проблемы выполнимости соответствующих КНФ вида $\tilde{C} \wedge C_\Delta \wedge C_{\delta_k=c}$. Экспериментально установлено, что для подавляющего большинства возможных значений c современные SAT-решатели доказывают невыполнимость $\tilde{C} \wedge C_\Delta \wedge C_{\delta_k=c}$ очень быстро (за доли секунды). Задачи о выполнимости КНФ вида $\tilde{C} \wedge C_\Delta \wedge C_{\delta_k=c}$, для которых не удаётся получить ответ за относительно небольшое время (несколько секунд), прерываются. Пусть c' — значение δ_k, при котором решение SAT-задачи для КНФ $\tilde{C} \wedge C_\Delta \wedge C_{\delta_k=c'}$ прервано, и при этом c' не совпадает с соответствующим значением в пути Ванг. Тогда c' можно рассматривать как кандидата на значение разности δ_k в новом дифференциальном пути. Описанный алгоритм реализован в виде параллельной MPI-программы и запускался на вычислительном кластере «Академик В. М. Матросов» ИНЦ СО РАН. В результате его работы построен новый дифференциальный путь для задачи поиска коллизий криптографической хеш-функции MD4. Данный путь отличается от пути Ванг [3] разностными соотношениями для шагов с номерами $k \in \{13, 17, 20, 21\}$. Введя в пропозициональную кодировку MD4 новый путь и используя значение разности между сообщениями M, M', взятое из [3], мы построили КНФ, к которой применили SAT-решатель `cryptominisat` [12], имеющий функцию перечисления множеств решений. Для построенной КНФ данный решатель нашел 1000 различных коллизий за 416 с. При применении к аналогичной КНФ, в которой записан оригинальный путь Ванг, `cryptominisat` находит 1000 коллизий за 520 с. На наш взгляд, полученные результаты убедительно демонстрируют применимость SAT-подхода к анализу стойкости криптографических хеш-функций к разностным атакам.

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. *Wang X., Lai X., Feng D., et al.* Cryptanalysis of the hash functions MD4 and RIPEMD // LNCS. 2005. V. 3494. P. 1–18.
4. *Wang X. and Yu H.* How to break MD5 and other hash functions // LNCS. 2005. V. 3494. P. 19–35.
5. *Mironov I. and Zhang L.* Applications of SAT solvers to cryptanalysis of hash functions // LNCS. 2006. V. 4121. P. 102–115.

6. *Богачкова И. А., Заикин О. С., Кочемазов С. Е. и др.* 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.
7. *Отпущенников И. В., Семёнов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
8. *Otpuschennikov I., Semenov A., and Kochemazov S.* Transalg: a tool for translating procedural descriptions of discrete functions to SAT // WCSE 2015-IPCE: Proc. 5th Intern. Workshop on Computer Science and Engineering: Information Processing and Control Engineering. 2015. P. 289–294.
9. *Hawkes P., Paddon M., and Rose G.* Musings on the Wang et al. MD5 Collision. IACR Eprint archive. `http://eprint.iacr.org/2004/264`. 2004.
10. *Hirshman G.* Further Musings on the Wang et al. MD5 Collision: Improvements and Corrections on the Work of Hawkes, Paddon, and Rose. Cryptology ePrint Archive, Report 2007/375. 2007.
11. *Stevens M.* Attacks on Hash Functions and Applications. PhD Thesis. Amsterdam: Ipskamp Drukkers, 2012. 258 p.

УДК 519.688 DOI 10.17223/2226308X/9/52

О ВЫЧИСЛЕНИИ ФУНКЦИЙ РОСТА КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ БЕРНСАЙДОВЫХ ГРУПП ПЕРИОДА 5[1]

А. А. Кузнецов, С. С. Карчевский

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — наибольшая конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34}. Для каждого элемента данной группы существует уникальное коммутаторное представление вида $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, где $\alpha_i \in \mathbb{Z}_5$, $i = 1, 2, \ldots, 34$. Здесь a_1 и a_2 — порождающие элементы $B_0(2,5)$; $a_3, \ldots, a_{34}$ — коммутаторы, которые вычисляются рекурсивно через a_1 и a_2. Определим фактор-группу группы $B_0(2,5)$ следующего вида: $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$. Очевидно, что $|B_k| = 5^k$. В настоящей работе вычислены функции роста B_k относительно порождающих множеств $\{a_1, a_2\}$ и $\{a_1, a_1^{-1}, a_2, a_2^{-1}\}$ для $k = 15$, 16, 17.

Ключевые слова: *функция роста группы, группа Бернсайда.*

Одним из важных инструментов для определения строения группы является изучение её роста относительно фиксированного порождающего множества. Пусть $G = \langle X \rangle$. *Шаром* K_s радиуса s группы G будем называть множество всех её элементов, которые могут быть представлены в виде групповых слов в алфавите X длиной не больше s. Для каждого целого неотрицательного s можно определить функцию роста группы $F(s)$, которая равна числу элементов группы G относительно X, представимых в виде несократимых групповых слов длиной s. Таким образом,

$$F(0) = |K_0| = 1,\ F(s) = |K_s| - |K_{s-1}| \text{ при } s \in \mathbb{N}.$$

Как правило, функцию роста конечной группы представляют в виде таблицы, в которую записывают ненулевые значения $F(s)$.

Пусть $F(s_0) > 0$, но $F(s_0 + 1) = 0$, тогда s_0 является диаметром графа Кэли группы G в алфавите порождающих X, который будем обозначать $D_X(G)$.

[1]Работа поддержана грантом Президента РФ (проект МД-3952.2015.9).

Вычисление функции роста произвольной конечной группы является хотя и разрешимой, но весьма сложной проблемой. Это связано с тем, что в общем случае задача по определению минимального слова элемента группы, как показали С. Ивен и О. Голдрейх [1], является NP-трудной.

Пусть $B_0(2,5) = \langle a_1, a_2 \rangle$ — максимальная конечная двупорождённая бернсайдова группа периода 5, порядок которой равен 5^{34} [2]. Используя систему компьютерной алгебры GAP, нетрудно получить pc-представление (*power commutator presentation*) данной группы [3, 4]. В этом случае каждый элемент $g \in B_0(2,5)$ записывается в виде уникального упорядоченного произведения базисных коммутаторов в определённых степенях:

$$\forall g \in B_0(2,5)\ (g = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}},\ \alpha_i \in \mathbb{Z}_5,\ i = 1, 2, \ldots, 34).$$

Здесь коммутаторы a_1 и a_2 являются порождающими элементами группы, а последующие — $a_3, \ldots, a_{34}$ — определяются рекурсивно через a_1 и a_2 [2].

Обозначим через B_k фактор-группу группы $B_0(2,5)$ следующего вида:

$$B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle.$$

Очевидно, что $|B_k| = 5^k$ и $\forall g \in B_k\ (g = a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_k^{\alpha_k})$.

К. А. Филипповым в [5] вычислена функция роста группы B_{14} в алфавите $A_2 = \{a_1, a_2\}$. Аналогичная задача для симметричного порождающего множества $A_4 = \{a_1, a_1^{-1}, a_2, a_2^{-1}\}$ решена Ч. Симсом [6]. В обоих случаях решение было получено при помощи длительных компьютерных вычислений.

Одной из причин интереса исследователей к функциям роста B_k является то, что получаемая информация может оказаться полезной при решении открытой проблемы о конечности $B(2,5)$ — свободной двупорождённой бернсайдовой группы периода 5.

Дальнейшее изучение функций роста групп B_k для $k > 14$ сталкивается с серьёзными вычислительными трудностями ввиду их больших порядков.

Настоящая работа посвящена разработке эффективного алгоритма для вычисления функций роста указанных групп, который бы дал возможность преодолеть существующий барьер. За основу взят алгоритм, описанный в [7]. Для быстрого умножения элементов группы использовались полиномы Холла, полученные в [8]. Введён новый метод упорядочивания элементов, который позволил значительно повысить быстродействие. Модифицированный алгоритм реализован на 4-процессорном компьютере (на каждом по 16 ядер) с общей памятью объемом 256 Гб. В результате вычислены функции роста групп B_k для $k = 15$, 16 и 17.

В таблице приведены значения диаметров графов Кэли групп B_k, полученные в настоящей работе, а также уже известные; на рис. 1 и 2 приведены графики роста функций B_k.

k	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$D_{A_2}(B_k)$	8	10	13	20	20	25	30	31	32	35	40	40	45	46	50	55
$D_{A_4}(B_k)$	4	6	9	10	13	15	19	20	20	24	26	28	30	30	33	34

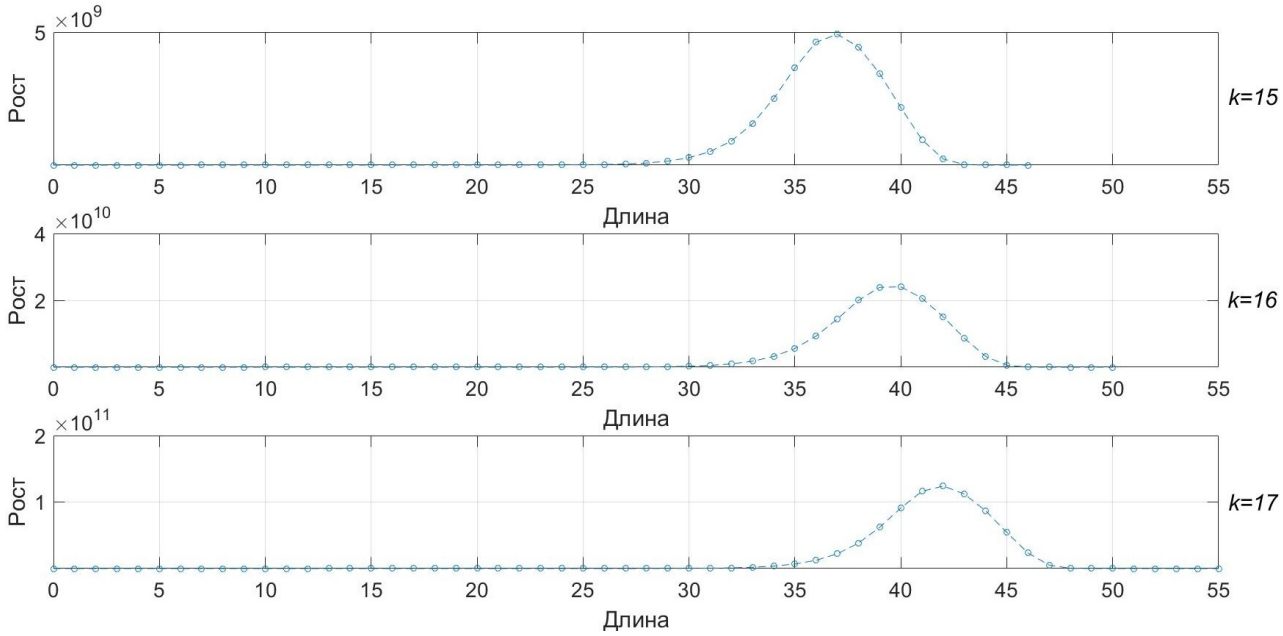


Рис. 1. Графики функций роста групп B_k в алфавите A_2

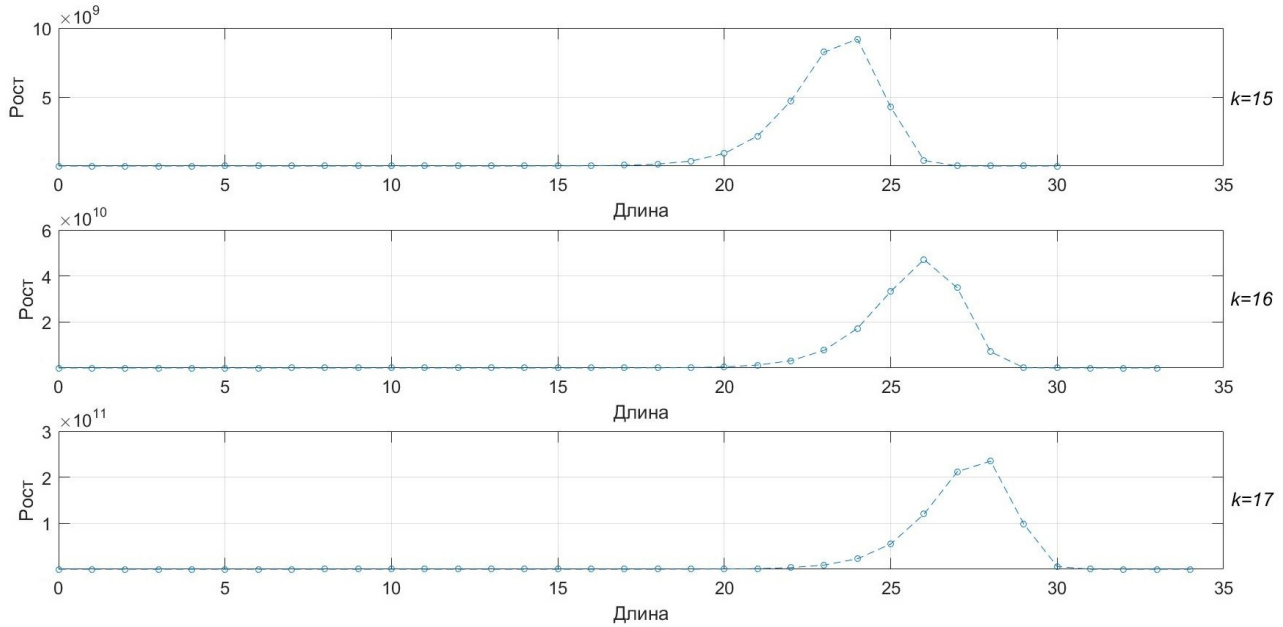


Рис. 2. Графики функций роста групп B_k в алфавите A_4

ЛИТЕРАТУРА

1. *Even S. and Goldreich O.* The minimum length generator sequence is NP-hard // J. Algorithms. 1981. V. 2. No. 3. P. 311–313.
2. *Havas G., Wall G., and Wamsley J.* The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. 1974. No. 10. P. 459–470.
3. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.
4. *Holt D., Eick B., and O'Brien E.* Handbook of Computational Group Theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.

5. *Филиппов К. А.* О диаметре Кэли одной подгруппы группы $B_0(2,5)$ // Вестник СибГАУ. 2012. Т. 41. № 1. С. 234–236.
6. *Sims C.* Fast multiplication and growth in groups // Proc. 1998 Intern. Symp. on Symbolic and Algebraic Computation. N. Y., USA, 1998. P. 165–170.
7. *Кузнецова А. С., Кузнецов А. А., Сафонов К. В.* Параллельный алгоритм вычисления функций роста в конечных двупорождённых группах периода 5 // Прикладная дискретная математика. Приложение. 2013. № 6. С. 119–121.
8. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. № 1. С. 110–116.

СВЕДЕНИЯ ОБ АВТОРАХ

АБРОСИМОВ Михаил Борисович — доктор физико-математических наук, профессор Саратовского государственного университета имени 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, профессор кафедры 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 технологического университета, г. Пенза.
E-mail: **ama@sura.ru, alekhina@penzgtu.ru**

АНИСЕНЯ Николай Ильич — аспирант кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **anisenya@gmail.com**

БАРСУКОВА Оксана Юрьевна — кандидат физико-математических наук, доцент Пензенского государственного университета, г. Пенза. E-mail: **kuzya_7@mail.ru**

БОНДАРЕНКО Леонид Николаевич — кандидат технических наук, доцент, доцент кафедры компьютерных технологий Пензенского государственного университета, г. Пенза.
E-mail: **leobond5@mail.ru**

БОРОДИН Михаил Алексеевич — аспирант кафедры ИБ ВМК Московского государственного университета им. М. В. Ломоносова, г. Москва. E-mail: **bor1m@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**

ВИТКУП Валерия Александровна — аспирантка Института математики им. С. Л. Соболева, г. Новосибирск. E-mail: **vvitkup@yandex.ru**

ВЛАСОВА Виктория Владимировна — студентка Национального исследовательского ядерного университета (МИФИ), г. Москва. E-mail: **victvlasova@yandex.ru**

ВОБЛЫЙ Виталий Антониевич — доктор физико-математических наук, доцент МГТУ им. Н. Э. Баумана, г. Москва. E-mail: **vitvobl@yandex.ru**

ВОЛГИН Артем Владимирович — преподаватель МГТУ МИРЭА, г. Москва.
E-mail: **artem.volgin@bk.ru**

ГОРБАТЕНКО Дмитрий Евгеньевич — аспирант Института математики, экономики и информатики Иркутского государственного университета, г. Иркутск. E-mail: **gorbadima@yandex.ru**

ГОРОДИЛОВА Анастасия Александровна — аспирантка Института математики им. С. Л. Соболева СО РАН, г. Новосибирск. E-mail: **gorodilova@math.nsc.ru**

ГРЕЧНЕВ Сергей Юрьевич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **sgrechnev@gmail.com**

ГРИБАНОВА Ирина Александровна — аспирантка Института динамики систем и теории управления им. В. М. Матросова СО РАН, г. Иркутск. E-mail: **the42dimension@gmail.com**

ДЕВЯНИН Петр Николаевич — доктор технических наук, доцент, председатель УМС ФУМО ВО ИБ, г. Москва. E-mail: **peter_devyanin@hotmail.com**

ЕВДОКИМОВ Александр Андреевич — кандидат физико-математических наук, профессор, заведующий лабораторией Института математики им. С. Л. Соболева, г. Новосибирск.
E-mail: **evdok@math.nsc.ru**

ЕГОРУШКИН Олег Игоревич — старший преподаватель Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнёва, г. Красноярск.
E-mail: **olegegoruschkin@yandex.ru**

ЖАРКОВА Анастасия Владимировна — кандидат физико-математических наук, доцент кафедры теоретических основ компьютерной безопасности и криптографии Саратовского национального исследовательского государственного университета имени Н. Г. Чернышевского, г. Саратов.
E-mail: **ZharkovaAV3@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 лаборатории 3.2 Института динамики систем и теории управления СО РАН, г. Иркутск. E-mail: **zaikin.icc@gmail.com**

ЗУЕВА Анна Игоревна — студентка кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **zueva@isc.tsu.ru**

КАРАНДАШОВ Максим Валерьевич — ассистент кафедры дискретной математики и информационных технологий Саратовского национального исследовательского университета им. Н. Г. Чернышевского, г. Саратов. E-mail: **norg113@gmail.com**

КАРПОВ Артем Валерьевич — аспирант кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **karpov@isc.tsu.ru**

КАРЧЕВСКИЙ Сергей Сергеевич — инженер-программист КБ «Искра», г. Красноярск.
E-mail: **sergey.ext@gmail.com**

КАЩЕЕВ Михаил Робертович — магистрант Института математики, механики и компьютерных наук им. И. И. Воровича, Южный федеральный университет, г. Ростов-на-Дону.
E-mail: **kashcheyewm@gmail.com**

КНЯЗЕВ Владимир Николаевич — студент математического факультета специальности «Компьютерная безопасность» Ярославского государственного университета им. П. Г. Демидова, г. Ярославль. E-mail: **darknyaz@yandex.ru**

КНЯЗЕВА Марина Сергеевна — студентка математического факультета специальности «Компьютерная безопасность» Ярославского государственного университета им. П. Г. Демидова, г. Ярославль. E-mail: **ututun@yandex.ru**

КОЛБАСИНА Ирина Валерьевна — аспирантка Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: **kabaskina@yandex.ru**

КОЛЕГОВ Денис Николаевич — кандидат технических наук, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, старший специалист отдела защиты приложений ЗАО «Позитив Текнолоджис», 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**

КОРЕНЕВА Алиса Михайловна — аспирантка НИЯУ МИФИ, системный аналитик ООО «Код Безопасности», г. Москва. E-mail: **alisa.koreneva@gmail.com**

КОСОЛАПОВ Юрий Владимирович — кандидат технических наук, доцент кафедры алгебры и дискретной математики Института математики, механики и компьютерных наук им. И. И. Воровича, Южный федеральный университет, г. Ростов-на-Дону. E-mail: **itaim@mail.ru**

КОСОЛАПОВ Юрий Владимирович — кандидат технических наук, доцент кафедры алгебры и дискретной математики Института математики, механики и компьютерных наук им. И. И. Воровича, Южный федеральный университет, г. Ростов-на-Дону. E-mail: **itaim@mail.ru**

КОЧЕМАЗОВ Степан Евгеньевич — программист Института динамики систем и теории управления им. В. М. Матросова СО РАН, г. Иркутск. E-mail: **veinamond@gmail.com**
КУЗНЕЦОВ Александр Алексеевич — доктор физико-математических наук, профессор, директор института Сибирского государственного аэрокосмического университета имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: **alex_kuznetsov80@mail.ru**
КУЗЬМИН Сергей Алексеевич — сотрудник лаборатории ТВП, г. Москва.
E-mail: **kzmn_sr@mail.ru**
КУЦЕНКО Александр Владимирович — студент механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **AlexandrKutsenko@bk.ru**
КУЦЕНОГАЯ Елизавета Петровна — магистрантка Новосибирского государственного университета, г. Новосибирск. E-mail: **ekutsenogaya@yandex.ru**
КЯЖИН Сергей Николаевич — аспирант кафедры криптологии и кибербезопасности Национального исследовательского ядерного университета (МИФИ), математик Центра специальных разработок МО РФ, г. Москва. E-mail: **s.kyazhin@kaf42.ru**
ЛЕБЕДЕВ Филипп Владимирович — студент кафедры криптологии и кибербезопасности Национального исследовательского ядерного университета (МИФИ), г. Москва.
E-mail: **philka9498@gmail.com**
ЛИНЕЙЦЕВ Павел Алексеевич — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **lineycevp@gmail.com**
ЛОГВИНА Ольга Александровна — кандидат технических наук, доцент, доцент Пензенского государственного технологического университета, г. Пенза. E-mail: **olga_kr@list.ru**
МАРТЫШИН Владимир Николаевич — студент НИЯУ МИФИ, г. Москва.
E-mail: **martyshin.v@gmail.com**
МЕДВЕДЕВА Наталья Валерьевна — кандидат физико-математических наук, доцент, доцент Уральского государственного университета путей сообщения, г. Екатеринбург.
E-mail: **medvedeva_n_v@mail.ru**
МЕЛЕШКО Анна Константиновна — ассистент МГТУ им. Н. Э. Баумана, г. Москва.
E-mail: **akmeleshko@gmail.com**
МОДЕНОВА Ольга Владимировна — аспирантка Саратовского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: **oginiel@rambler.ru**
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 лаборатории 3.2 Института динамики систем и теории управления СО РАН, 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**
ПЕРШИН Владислав Владимирович — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **v.pershin.93@gmail.com**
ПОГОРЕЛОВ Борис Александрович — доктор физико-математических наук, профессор, действительный член Академии криптографии РФ, г. Москва.
ПОКРАСЕНКО Денис Павлович — студент механико-математического факультета Новосибирского государственного университета, г. Новосибирск. E-mail: **pokrasenko.d.p@gmail.com**
ПУДОВКИНА Марина Александровна — кандидат физико-математических наук, доцент Национального исследовательского ядерного университета (МИФИ), г. Москва.
E-mail: **maricap@rambler.ru**

РОМАНЬКО Дмитрий Андреевич — студент Национального исследовательского ядерного университета (МИФИ), г. Москва. E-mail: **dmax.rda@gmail.com**

РЯБКО Борис Яковлевич — доктор технических наук, профессор, заведующий лабораторией Института вычислительных технологий СО РАН, г. Новосибирск. E-mail: **boris@ryabko.net**

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 имени академика М. Ф. Решетнёва, г. Красноярск. E-mail: **safonovkv@rambler.ru**

СЕМЁНОВ Александр Анатольевич — кандидат технических наук, доцент, заведующий лабораторией 3.2 Института динамики систем и теории управления СО РАН, г. Иркутск.
E-mail: **biclop.rambler@yandex.ru**

СОШИН Данил Андреевич — сотрудник ФГУП «НИИ «КВАНТ», г. Москва.
E-mail: **danil_re@list.ru**

СТЕФАНЦОВ Дмитрий Александрович — старший преподаватель кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **d.a.stefantsov@isc.tsu.ru**

СУХОВ Сергей Александрович — студент Саратовского государственного университета имени Н. Г. Чернышевского, г. Саратов. E-mail: **serega_suhov@mail.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 кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, специалист отдела защиты приложений ЗАО «Позитив Текнолоджис» 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 СО РАН, г. Новосибирск.
E-mail: **tokareva@math.nsc.ru**

ТОМСКИХ Павел Александрович — студент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск.
E-mail: **pavlic148@gmail.com**

ТРЕНЬКАЕВ Вадим Николаевич — доцент, кандидат технических наук, доцент кафедры защиты информации и криптографии Национального исследовательского Томского государственного университета, г. Томск. E-mail: **tvnik@sibmail.com**

ТУРЧЕНКО Олег Юрьевич — студент Института математики, механики и компьютерных наук им. И. И. Воровича, Южный федеральный университет, г. Ростов-на-Дону.
E-mail: **olegmmcs@gmail.com**

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, профессор НИЯУ МИФИ, ведущий научный сотрудник ФИЦ ИУ РАН, научный консультант ООО «Код Безопасности», г. Москва. E-mail: **fomichev@nm.ru**

ЧЕРЕМУШКИН Александр Васильевич — доктор физико-математических наук, член-корреспондент Академии криптографии РФ, научный консультант ФГУП «НИИ «Квант», г. Москва.
E-mail: **avc238@mail.ru**

ЧИЖОВ Иван Владимирович — кандидат физико-математических наук, доцент кафедры ИБ ВМК Московского государственного университета им. М. В. Ломоносова, г. Москва.
E-mail: **ichizhov@cs.msu.ru**
ЧУШКИН Михаил Сергеевич — аспирант Института систем информатики СО РАН, г. Новосибирск. E-mail: **chushkinm@rambler.ru**
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**
ШЕЛЕХОВ Владимир Иванович — заведующий лабораторией Института систем информатики СО РАН, г. Новосибирск. E-mail: **vshel@iis.nsk.su**
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. **GENERALIZED NARAYANA POLYNOMIALS AND THEIR q-ANALOGUES.** Generating polynomials of the statistics rise, des and inv are considered on the entered 312-avoiding GS-permutations of an order $r \geqslant 1$. It is shown that the polynomials of the statistics rise and des are some generalizations of the known Narayana polynomials. For the generalized Narayana polynomials, the inverse generating function, an algebraic equation for the generating function and a recursion relation with multiple convolutions are obtained. For the generating polynomials of pair $(\mathrm{des}, \mathrm{inv})$, an analogue of the obtained recursion relation and an equation for the generating function of these polynomials are found. Their particular case leads to the corresponding q-analogues of generalized Narayana polynomials.

Keywords: *312-avoiding GS-permutations, generalized Narayana polynomials, generating function, inverse function, convolution, q-analogues.*

Volgin A. V. **A CRITERION FOR CHECKING THE HYPOTHESIS ABOUT THE EXISTENCE OF EMBEDDINGS INTO A BINARY MARKOV CHAIN.** A condition on the mutual asymptotic ratio of the length of a sequence and the volume of bit embeddings in it guaranteeing the existence of embeddings is given.

Keywords: *Markov chains, embeddings into pseudorandom sequences, statistical criteria to distinguish hypotheses.*

Evdokimov A. A. **AN ALGORITHM FOR RECOGNIZING THE COMPLETENESS OF A SET OF WORDS AND DYNAMICS OF PROHIBITIONS.** Some reduction operations on a set of words are introduced. For recognizing the completeness of such sets, an algorithm using these operations is proposed. A theorem substantiating the algorithm is given.

Keywords: *a set of words, completeness, dynamics, prohibitions, algorithm, recognition.*

Kuzmin S. A. **ON A SUFFICIENT CONDITION FOR IMPOSSIBILITY TO REDUCE THE PERIOD OF THE HIGH ORDER BINARY DIGIT POSITION SEQUENCES OVER PRIMARY RINGS.** Binary digit position sequences over primary rings of odd characteristics are studied. In the case, when not all possible elements appear in a periodic part of a given linear recurring sequence, a sufficient condition that there is no twofold reduction of the period in the high order binary digit position sequence is given.

Keywords: *linear recurring sequences, periods of sequences, primary rings, digit position sequences.*

Pogorelov B. A., Pudovkina M. A. **ON GROUPS GENERATED BY MIXED TYPE PERMUTATIONS AND KEY ADDITION GROUPS.** Three groups are often used as key addition groups in iterated block ciphers: V_n^+, $\mathbb{Z}_{2^n}^+$ and $\mathbb{Z}_{2^n+1}^{\odot}$. They are the regular permutation representations, respectively, of the group of vector key addition, of the additive group of the residue ring $\mathbb{Z}_{2^n}$, and of the multiplicative group of the residue ring $\mathbb{Z}_{2^n+1}$, where 2^n+1 is a prime number. In this paper, we describe some properties of the extensions of the group $G_n = \langle V_n^+, \mathbb{Z}_{2^n}^+ \rangle$ by transformations and groups related to cryptographic applications. The groups $\mathbb{Z}_{2^d}^+ \times V_{n-d}^+$, $V_{n-d}^+ \times \mathbb{Z}_{2^d}^+$ and a pseudoinverse permutation of the field

GF(2^n) or the Galois ring GR($2^{md}, 2^m$) are examples of such groups and transformations.
Keywords: *key addition group, additive regular group, wreath product, multiplicative group of the residue ring, Galois ring.*

Pogorelov B. A., Pudovkina M. A. **ON THE CLASSIFICATION OF DISTANCE-TRANSITIVE ORBITAL GRAPHS OF OVERGROUPS OF THE JEVONS GROUP.** The Jevons group is the exponential group $S_2 \uparrow S_n$. It is generated by the group of all permutation $(n \times n)$-matrices over GF(2) and the translation group on the n-dimensional vector space V_n over GF(2). For a permutation group G on V_n being an overgraph of $S_2 \uparrow S_n$, an orbital of G is an orbit of G in its natural action on $V_n \times V_n$. The orbital graph associated with an orbital Γ is the graph with the vertex set V_n and the edge set Γ. In this paper, we classify distance-transitive orbital graphs of overgroups of the Jevons group $S_2 \uparrow S_n$ and show that some of them are isomorphic to the following graphs: the complete graph K_{2^n}, the complete bipartite graph $K_{2^{n-1},2^{n-1}}$, the halved $(n+1)$-cube, the folded $(n+1)$-cube, alternating forms graphs, the Taylor graph, the Hadamard graph.
Keywords: *orbital graph, Jevons group, distance-transitive graph, Hamming graph.*

SECTION 2

Vitkup V. A. **ON SPECIAL CLASS OF VECTORIAL BOOLEAN FUNCTIONS AND THE PROBLEM OF APN PERMUTATIONS EXISTENCE.** The existence of APN permutation of even dimension is an important unsolved problem on vectorial Boolean functions. In this paper, we consider the special set of vectorial Boolean functions, such that the sum of any function in the set and an affine vectorial function is a permutation. We study properties of this set and conditions for existence of its nonempty intersection with the set of APN functions.
Keywords: *vectorial Boolean function, APN function, bijective function, permutation.*

Gorodilova A. A. **ON DIFFERENTIAL EQUIVALENCE OF QUADRATIC APN FUNCTIONS.** A vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if the equation $F(x) + F(x + a) = b$ has at most 2 solutions for all vectors $a, b \in \mathbb{F}_2^n$, where a is nonzero. For a given F, an associated Boolean function $\gamma_F(a, b)$ in $2n$ variables is defined so that it takes value 1 iff a is nonzero and the equation $F(x) + {+}F(x{+}a) = b$ has solutions. We introduce the notion of differentially equivalent functions as vectorial functions that have equal associated Boolean functions. The problem to describe the differential equivalence class of a given APN function is very interesting since the answer can potentially lead to some new constructions of APN functions. We start analyzing this problem with the consideration of affine functions A such that a quadratic APN function F and $F + A$ are differentially equivalent functions. We completely describe these affine functions A for an arbitrary APN Gold function F. Computational results for known quadratic APN functions in small number of variables $(2, \ldots, 8)$ are presented.
Keywords: *vectorial Boolean functions, almost perfect nonlinear functions, differential equivalence.*

Zueva A. I., Karpov A. V. **FUNCTIONS WITH VARIATIVE-COORDINATE POLYNOMIALITY OVER GROUP.** A class of VCP-functions, that is, of functions with the variative-coordinate polynomiality over group, is defined. It is an extension of the class of VCP-functions over primary ring of residues. An algorithm for finding coordinates for group elements is presented. It is shown that the class of VCP-functions over $UT_n(\mathbb{Z}_p)$ does not coincide with the class of polynomial function. A formula for constructing the

inverse of a bijective VCP-function over $UT_n(\mathbb{Z}_p)$ is proposed.
Keywords: *functions over group, functions with variative-coordinate polynomiality, coordinate functions.*

Kolomeec N. A. **ON THE HAMMING DISTANCE BETWEEN TWO BENT FUNCTIONS.** This work is devoted to the Hamming distance between two bent functions. Using the construction of bent functions at the minimal distance, some possible values of the distance are obtained. All possible distances between two Maiorana — McFarland bent functions are described.
Keywords: *Boolean functions, bent functions, Hamming distance.*

Kutsenko A. V. **ON THE SET OF VALUES FOR HAMMING DISTANCE BETWEEN SELF-DUAL BENT FUNCTIONS.** It is shown that the Hamming distance between self-dual Maiorana — McFarland bent functions of the form $\langle x, \pi(y)\rangle \oplus h(y)$, where $\pi \in \mathrm{GL}(n/2, \mathbb{Z}_2)$, belongs to the set $\{2^{n-1}, 2^{n-1}(1 \pm 1/2), 2^{n-1}(1 \pm 1/2^2), \ldots, 2^{n-1}\left(1 \pm 1/2^{n/2-1}\right), 2^n\}$.
Keywords: *Boolean function, bent function, Walsh — Hadamard transform, self-dual bent, Maiorana — McFarland bent function.*

Pokrasenko D. P. **NECESSARY CONDITION FOR MAXIMUM COMPONENT ALGEBRAIC IMMUNITY OF A VECTORIAL BOOLEAN FUNCTION.** It is shown that if a vectorial Boolean function $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ has the maximum component algebraic immunity, then $m \leqslant 2^{\lceil (n+1)/2 \rceil} - 1$.
Keywords: *component algebraic immunity, vectorial Boolean function.*

Soshin D. A. **THE PRESENTATION OF MAGMA AND 2-GOST BLOCK CIPHER SEMIBYTE SUBSTITUTIONS BY ALGEBRAIC THRESHOLD FUNCTIONS.** The paper deals with the implementation of Magma and 2-GOST block cipher semibyte substitutions by algebraic threshold functions (ATF). For each Magma substitution, an ATF-presentation of some linear combinations of its coordinate functions is proposed. Some linear combinations of ATF representing 2-GOST substitutions are found.
Keywords: *algebraical threshold functions, substitution.*

Tokareva N. N. **ON THE SET OF DERIVATIVES OF A BOOLEAN BENT FUNCTION.** Is it true that any balanced Boolean function in n variables of degree less than $n/2$ is a derivative of a bent function in n variables? We study this question in the case when n is small.
Keywords: *bent functions, derivative, affine classification.*

Cheremushkin A. V. **ON QUADRATIC FORM RANK DISTRIBUTION AND ASYMPTOTIC BOUNDS OF AFFINITY LEVEL.** An affinity level $\mathrm{la}(f)$ of a Boolean function f is defined as minimal number of variable fixations, that produce an affine function. A general affinity level $\mathcal{L}a(f)$ of Boolean function f is defined as minimal number of fixations of variable linear combination values, that produce an affine function. The general affinity level of quadratic form equals r iff the rank of quadratic form equals $2r$. The paper contains some asymptotic properties of the rank of quadratic forms. As a corollary some asymptotic bounds of the general affinity level of quadratic forms are formulated. Let $0 \leqslant c \leqslant 1$. If $n = 2k + \varepsilon$, $0 \leqslant \varepsilon \leqslant 1$, then for almost all quadratic forms of n variables,

$$\mathrm{la}(f) \geqslant \mathcal{L}a(f) \geqslant k - \left\lceil \sqrt{\frac{1}{2}\log_2 k} + \frac{c + (-1)^{\varepsilon}}{2} \right\rceil + 1$$

as $n \to \infty$.
Keywords: *Boolean functions, affinity level, quadratic form.*

Shushuev G. I. **FUNCTIONS ON DISTANCE ONE FROM APN FUNCTIONS IN SMALL NUMBER OF VARIABLES.** In this paper, we deal with vectorial Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ of dimension $n \geqslant 1$. Functions F and G are EA-nonequivalent if $G \neq A_1 \circ F \circ A_2 \oplus A$ for any affine functions A_1, A_2 and A, where A_1 and A_2 are permutations. A function F is called APN if for any $a, b \in \mathbb{F}_2^n$, where a is nonzero, the equation $F(x) \oplus F(x \oplus a) = b$ has at most two solutions. We prove that there are no APN functions on the distance one from an APN functions up to dimension 5, from all quadratic APN functions of dimension 6, and from all known EA-nonequivalent APN functions of dimensions 7 and 8.
Keywords: *vectorial Boolean function, APN function.*

SECTION 3

Agibalov G. P., Pankratova I. A. **TO CRYPTANALYSIS OF 2-CASCADE FINITE AUTOMATA CRYPTOGRAPHIC GENERATORS.** An abstract finite automaton cryptographic generator generalizing the register (δ, τ)-step generator is defined. Some attacks on it with the object to determine initial states or (and) output functions of its automata are presented. The complexity of these attacks are much less than the complexity of the brute-force attack.
Keywords: *finite automaton, cryptographic generator, (δ, τ)-step generator, cryptanalysis, linearization attack.*

Vlasova V. V., Pudovkina M. A. **ON THE GROUP GENERATED BY THE ROUND FUNCTIONS OF THE BLOCK CIPHER KUZNECHIK.** One of the research areas for iterative block cyphers is to describe the properties of the group generated by the set of all partial round functions. Kuznechik is a new Russian block encryption standard. In this paper, we prove that the group generated by the set of all partial round functions of Kuznechik is alternating.
Keywords: *"Kuznechik", GOST R 34.12-2015, alternating group.*

Zaikin O. S., Otpuschennikov I. V., Semenov A. A. **ESTIMATIONS OF CRYPTOGRAPHIC RESISTANCE OF CIPHERS IN THE TRIVIUM FAMILY TO SAT-BASED CRYPTANALYSIS.** Here we present the cryptanalysis results for three stream ciphers in the Trivium family: Bivium, Trivium toy, and Bivium toy. The cryptanalysis was performed via reducing the inversion problems for corresponding discrete functions to Boolean satisfiability problem (SAT). This approach made it possible to perform the cryptanalysis of Bivium toy cipher using common sequential SAT solvers. On average, to solve one cryptanalysis instance for Bivium toy on one core of AMD Opteron 6276 processor, it took about two minutes. For cryptanalysis of Bivium, we designed a variant of "guess-and-determine" attack, in which it is assumed that the values of the last 9 cells at the end of the second Bivium register are known. Thus, the problem is to find values of 168 remaining cells of Bivium registers (the total length of two registers used in Bivium is 177 bits). For this purpose, we analyze 200 bits of keystream. To solve one corresponding cryptanalysis instance, it took about two weeks of work of volunteer computing project SAT@home. The Trivium toy cipher, in its non-weakened form, turned out to be highly resistant to SAT-based cryptanalysis. It proves once more that the general design of the Trivium cipher is very good. We considered the recovery problem for values of registers

in Trivium toy based on 100 bits of keystream. At the current stage, we only managed to perform in a reasonable time the variant of "guess-and-determine" attack, in which we know the initial values of the first 16 cells of the second register. Thus, in the corresponding cryptanalysis instances, we need to find values of remaining 80 out of 96 cells. Using the computing cluster of Irkutsk Supercomputer center SB RAS, we managed to solve several instances of Trivium toy cryptanalysis. For this purpose, we used the PD-SAT parallel solver developed in ISDCT SB RAS. On average, to solve one instance using 320 cores of AMD Opteron 6276, it took about one day.
Keywords: *stream cipher, Trivium, Bivium, cryptanalysis, Boolean satisfiability problem.*

Koreneva A. M., Martyshin V. N. **EXPERIMENTAL RESEARCH ON EXPONENTS OF MIXING MATRICES FOR GENERALIZED FEISTEL NETWORKS.** In this work, we research the mixing properties of round functions in generalized Feistel networks based on shift registers of length 4 over the set of binary 32-dimensional vectors. Register functions with different number of register feedbacks were considered. By an experiment, we obtain recommendations for selecting parameters of the register functions to implement the fast mixing of input bits.
Keywords: *generalized Feistel network, encryption round, exponent of matrix, mixing matrix.*

Koreneva A. M., Fomichev V. M. **SUFFICIENT VARIABLES FOR TRANSITION FUNCTION OF A MODIFIED ADDITIVE GENERATOR.** We consider the class of bijective shift registers of length n over the set V_r of binary vectors of length r. In this paper, we research registers constructed on the additive generators modulo 2^r modified by a transformation of V_r. The feedback function of such a register is a composition of additive generator feedback function and the transformation of V_r. It is known that determination of sufficient variables for the composition of nonlinear functions is a complicated problem. By using combinative properties of the bijection $\mathbb{Z}_{2^r} \leftrightarrow V_r$, we describe the set of all sufficient variables for feedback function of the registers researched.
Keywords: *additive generator, sufficient variable, mixing properties.*

Kosolapov Y. V., Turchenko O. Y. **SEARCH OF AN INFORMATION MESSAGE IN NOISY CODE BLOCKS AT REPEATED DATA TRANSMISSION.** The security model using the method of code noising is considered. It is assumed that the information blocks of length k contain a fixed message m of length $l \leqslant k$ on a fixed position q, $1 \leqslant q \leqslant k - l + 1$, and an observer gets noisy codewords of length n through a binary symmetric channel with error probability $(1 - \Delta)/2$, $0 < \Delta \leqslant 1$. The aim of the observer is to find the unknown message m, when position q is unknown, and the length l is known. We propose a method for finding m and obtain an estimate for a sufficient number of observed codewords needed to recover the message m in this way.
Keywords: *code noising, repeated data transmission.*

Kyazhin S. N., Lebedev P. V. **ON THE ACCURACY OF MATRIX-GRAPH APPROACH TO INVESTIGATION OF TRANSFORMATION MIXING PROPERTIES.** Experimental results of evaluating the accuracy of matrix-graph approach to investigation of nonlinear transformation mixing properties are obtained. The experiment has been carried out with all those transformations of the binary n-dimensional vectors set, for which the mixing graph is the Wielandt graph with n vertices, and also with the round substitutions used in AES, Kuznechik, and Magma block ciphers. It is shown that results obtained by matrix-graph approach are accurate for 25 % of transformations with the mix-

ing Wielandt graph (for $n = 9, 10, 11$) and for round substitutions in AES and Kuznechik algorithms. The results are not accurate for round substitution in Magma algorithm and for 75 % of transformations with the mixing Wielandt graph.
Keywords: *mixing properties, matrix-graph approach, Wielandt graph, AES, Kuznechik, Magma.*

Kyazhin S. N., Fomichev V. M. **MIXING PROPERTIES OF 2-CASCADE GENERATORS.** The important properties of the dependence of gamma signs on all signs in the initial state of a gamma generator are called the mixing properties of the generator. It is known that if the mixing properties of a generator are good, then the transition graph of the generator is primitive or local primitive. In this paper, mixing properties are evaluated for the following 2-cascade generators constructed of Linear Feedback Shift Register (LFSRs): generator based on shift register series, generator of 1-2 steps, and generator of intermittent steps. Namely, for these generators, some necessary and sufficient conditions for local primitiveness or quasiprimitiveness are given and upper bounds for appropriate local exponents or quasiexponents depending on the parameters of LFSR are obtained. For many values of parameters, the bounds are close to the sum of lengths of LFSRs in the generator.
Keywords: *shift register, generator of 1-2 steps, generator of intermittent steps, local primitiveness, local exponent.*

Medvedeva N. V., Titov S. S. **ANALOGUES OF THE SHANNON THEOREM FOR NON-MINIMAL ENDOMORPHIC PERFECT CIPHERS.** This work deals with some analogues of the Shannon's theorem for endomorphic perfect ciphers (which are absolutely immune against the ciphertext-only attack). Examples of the perfect and transitive ciphers, minimal by inclusion, are constructed.
Keywords: *perfect ciphers, endomorphic ciphers, non-minimal ciphers.*

Romanko D. A., Fomichev V. M. **A METHOD FOR BUILDING A CRYPTOGRAPHIC GENERATOR OF SEQUENCES WITH SPECIFIED INDEX OF UNREPEATABILITY.** It is known that iterative symmetric block ciphers may have a few specific keys termed "weak keys" and "semi-weak keys". Due to this fact, we consider a method for constructing the key schedule providing the absence of duplication in round key sequence. For key generation, we propose the autonomous automaton based on one-two step generator consisting of two maximal period linear feedback shift registers of length n and m. The output alphabet of this automaton is V_m and the subsequence of length 2^{m-1} does not contain repeating vectors for any initial state of the automaton.
Keywords: *block cipher, round key, r-unrepeatable sequence, r-unrepeatable automaton, index of unrepeatability.*

Ryabko B. Ya. **APPLICATIONS OF TWO-FACED PROCESSES TO PSEUDO-RANDOM NUMBER GENERATION.** Random and pseudorandom number generators (RNG and PRNG) are used for many purposes including cryptographic applications. For such applications, a generated bit sequence should mimic true random, i. e., by definition, such a sequence could be interpreted as the result of the flips of a "fair" coin with sides that are labelled 0 and 1. It is known that the Shannon entropy of this process is 1 per letter, whereas for any other stationary process with binary alphabet the Shannon entropy is strictly less than 1. On the other hand, the entropy of the PRNG output should be much less than 1 bit (per letter), but the output sequence should look like truly random. We describe random processes, for which those, in a first glance contradictory, properties

are valid. More precisely, it is shown that there exist binary-alphabet random processes whose entropy is less than 1 bit (per letter), but a frequency of occurrences of any word u goes to $2^{-|u|}$, where $|u|$ is the length of u. In turn, it gives a possibility to construct RNG and PRNG, which possess theoretical guarantees. This is important for applications of them in cryptography.
Keywords: *random number generator, pseudorandom number generator, Shannon entropy.*

Fomichev V. M. **ON KEY SCHEDULE FOR BLOCK CIPHERS WITHOUT WEEK KEYS.** This paper describes the key schedule providing all different round keys for r-round symmetric block cipher. The key schedule is implemented by a series connection of automata: an autonomous automaton A generating an output sequence of binary vectors with the period length is not less than r, and internally autonomous automaton with permanent memory containing the encryption key of a block cipher. As an example, a linear shift register with a maximum period is considered as the automaton A.
Keywords: *block cipher, round key, r-unrepeatable sequence, r-unrepeatable automaton, index of unrepeatability.*

Chizhov I. V., Borodin M. A. **CRYPTANALYSIS OF THE MCELIECE PKC BASED ON $(k-1)$-REED — MULLER SUBCODES.** In this paper, we describe two types of McEliece cryptosystems based on some Reed — Muller subcodes and study the question of equivalent keys for these cryptosystems. A method for reduction of one cryptosystem to the another is obtained. Also, we show that these cryptosystems based on Reed — Muller subcode with the most widely used parameters can be attacked with the authors' algorithm.
Keywords: *McEliece cryptosystem, Reed — Muller subcode, automorphism of Reed — Muller code, Schur product codes, square of code.*

SECTION 4

Anisenya N. I. **UNDENIABLE ONION ROUTING PROTOCOL WITH MESSAGE CREATION TIME VERIFICATION.** The problem of message routing in competitive environment of decentralized network is considered and demonstrated by the example of holding task-based CTF contest. Message creation time verification is introduced as an additional requirement of the protocol. An improvement of the undeniable onion routing protocol is described. It allows network participants to verify creation time for transferred messages.
Keywords: *distributed protocols, protected computing, fault-tolerant systems.*

Gorbatenko D. E., Kochemazov S. E., Semenov A. A. **ON DISCRETE AUTOMATON MODELS OF ATTACKS IN COMPUTER NETWORKS.** We propose a new model for describing the development of attacks in computer networks. The basis of the model is a synchronous discrete automaton defined by the network graph, where vertices are hosts. We consider transitions between the states of this automaton, that take place in discrete time moments. At each time moment, we associate with the graph vertices Boolean vectors referred to as host states. At each consecutive time moment, the host states are synchronously computed according to some fixed pre-defined rules. In more detail, let $G = (V, A)$ be a graph interpreting the computer network. Let $Q = \{q_1, \ldots, q_l\}$ be the set of possible host vulnerabilities. The process of development of an attack in the network is the process of exploiting the available vulnerabilities by an adversary. At the next time moment,

new available vulnerabilities can appear as a result of such exploitation. Therefore, we can consider the network as discrete automaton, that functions in time moments $t \in \{0, 1, \ldots\}$. We refer to the moment $t = 0$ as initial moment. For each t, let us associate with each host $v \in V$ a Boolean vector $\alpha^v(t) = \left(\alpha_1^v, \ldots, \alpha_l^v, \alpha_{l+1}^v, \ldots, \alpha_r^v(t)\right)$, $r \geqslant l$, called the state of the host v at time moment t. The first l coordinates of this vector form the so-called vector of vulnerabilities: we assume that $\alpha_j^v = 1$ iff host v has the vulnerability q_j, $j \in \{1, \ldots, l\}$. This vector of vulnerabilities is fixed and does not change. The coordinates of $\alpha^v(t)$ with indices $l + 1, \ldots, r$ contain the information that can change for time. In particular, the corresponding vector values reflect some access permissions the considered host has on other hosts. The coordinates $l+1, \ldots, r$ of $\alpha^v(t)$ form the vector of possibilities of host v at moment t. If we assume that we know the states of all hosts at initial time moment, we can consider the transitions of the network to the consecutive states by changing the vectors of possibilities of the hosts according to pre-defined rules. As such rules, we used the pairs of the kind (pre-condition, post-condition), by means of which in the widely known work by M. Danforth the elementary attacks are defined. In the context of the proposed model, we analyzed several types of attacks in computer networks. To obtain superuser permissions on a desired host, we considered combinatorial problems of finding best distributions of adversary hosts in the attacked networks. In this process, it is possible to take into account various additional constraints. Also, we considered the combinatorial problem referred to in the work by M. Danforth as the problem of distributing patches. All considered problems were reduced to Boolean satisfiability problem and solved using state-of-the-art SAT solvers. In our experiments, we considered random graphs with several hundred vertices.
Keywords: *discrete automaton, attack graph, Boolean satisfiability, SAT.*

Devyanin P. N. **ABOUT RESULTS OF DESIGNING HIERARCHICAL REPRESENTATION OF MROSL DP-MODEL.** This article describes new approach to the hierarchical representation of mandatory entity-role DP-model of secure access and information flows control in OS of Linux set (MROSL DP-model). Existing "monolithic" description of MROSL DP-model is the basis of the access control mechanism in secure OS Astra Linux Special Edition. However, "monolithic" description of MROSL DP-model has considerable size and complexity. It is inconvenient for scientific analysis, verification and further development, as well as for its direct application in OS Astra Linux Special Edition. For this reason, a hierarchical representation of MROSL DP-model is completely revised, and we can describe it through its levels. Thus, each lower level of MROSL DP-model is an abstract system, whose elements are independent of the new elements belonging to a higher level of MROSL DP-model. When it is necessary, a higher level inherits, corrects or complements the lower level elements. There are four levels in this hierarchical representation of MROSL DP-model. First level corresponds to role-based access control (RBAC), second level — RBAC and mandatory integrity control (MIC), third level — RBAC, MIC and mandatory access control (MAC) with information flows by memory, and fourth level — RBAC, MIC and MAC with information flows by memory and by time. New levels of lateral "branches" may be added to MROSL DP-model in the future. Some alternative levels can be: alternative third level — RBAC, MIC and a model of hypervisor, or alternative fourth level — RBAC, MIC, MAC with information flows by memory and a model of RBAC in a network.
Keywords: *computer security, formal model, hierarchical description, Linux.*

Kascheev M. R., Kosolapov Y. V. **CONFIDENTIALITY PRESERVING SCHEME FOR THE ALGORITHM RAID-PIR.** We consider the problem of confidentiality of

information in the database scheme of private information retrieval from remote servers. It is assumed that r servers are used to store the database (r is odd), and anonymous access to information scheme is used by RAID-PIR scheme. We built encryption method and the distribution of the database so that the encrypted data in each of the storage could not violate the privacy of the information base. Also, we built a read and a rewrite algorithms without violating data confidentiality and anonymity.
Keywords: *data anonymity, PIR, data distribution.*

Kolegov D. N., Broslavsky O. V., Oleksov N. E. **HMAC OBFUSCATION METHOD FOR IMPLEMENTATION IN UNTRUSTED SYSTEMS.** We propose an obfuscation method for using hash-based message authentication codes (MAC) in untrusted systems. Our method is implemented for MAC in a form $H(k, x) = h(k, p_1, h(k, p_2, x))$. The main idea is to use inner states of a hash function h. We calculate both h intermediate values in a such way that all key related blocks are already reduced by the hash compression function. That values are $h(epad(k, p_1))$ and $h(epad(k, p_2))$, where *epad* is a key padding algorithm. Then we use them in functions h_1 and h_2, which calculate h with the initial block equalled $h(epad(k, p_1))$ and $h(epad(k, p_2))$ respectively. So, accordingly to the following equation, these new functions implement original MAC algorithm: $H(k, x) = h(k, p_1, h(k, p_2, x)) = h_1(h_2(x))$.
Keywords: *white-box cryptography, message authentication codes, HMAC, obfuscation, web application security.*

Kolegov D. N., Lineytsev P. A. **WEB APPLICATION FIREWALLS IDENTIFICATION IN MitB-MODEL.** The existing methods of web application firewalls identification in "Man in the Browser" attacker model is considered. An implementation of the methods as a module for BeEF (Browser Exploitation Framework) is proposed.
Keywords: *application security, web application firewall, fingerprinting.*

Kolegov D. N., Tkachenko N. O. **LIGHTWEIGHT IMPLEMENTATION OF ABAC MECHANISM ON DATABASE FIREWALL.** We propose a lightweight non-invasive method for implementing attribute based access control for RDBMS *MySQL* on *DatabaseFirewall*. Implemented access control mechanism consists of two parts. According to NIST ABAC terminology, the first part is Policy Enforcement Point (PEP) and the second one is Policy Decision Point (PDP). PDP and PEP communicate using HTTP protocol. PEP is handling SQL queries from client, parsing it and sending to PDP via HTTP. PDP implements lightweight core of ABAC. The main purpose of this part is taking a decision to permit or deny access based on stored policies. After the decision is made, PDP sends it to PEP. We developed a new role view mechanism to combine RBAC and ABAC. This mechanism is used to translate privileges from RBAC roles to ABAC rules. ABAC rules are configured using a special language named *AF Rules* and specified in JSON format. These rules are translated to PDP code, which implements access control checks.
Keywords: *access control, ABAC, RBAC, Database Firewall.*

SECTION 5

Alekhina M. A., Barsukova O. Yu. **ON THE RELIABILITY OF CIRCUITS IN THE ROSSER — TOURKETT BASIS (IN P_k).** We consider the implementation of k-valued logic functions with circuits consisting of unreliable functional elements in the Rosser — Tourkett basis. It is assumed that all elements of the circuit are independently

subjected to inverse failures on the outputs. The upper and lower bounds of circuit reliability are found, and the class of functions, for which the lower bounds hold, is found too.
Keywords: *k-valued logic functions, unreliable functional elements, the reliability and unreliability of a circuit, inverse failures on outputs of elements.*

Alekhina M. A., Logvina O. A. **THE UNRELIABILITY OF CIRCUITS IN CASE COALESCENCES OF ELEMENTS INPUTS.** We consider the implementation of Boolean functions by circuits of unreliable functional elements in some complete finite bases. It is assumed that each of the circuit elements is exposed to disjunctive (conjunctive) coalescence of inputs independently of the other elements. It is shown that in some bases any Boolean function can be implemented by a circuit with any high reliability, and in some ones it can be done by a circuit with the unreliability, which is equal to zero.
Keywords: *unreliable functional elements, circuit reliability, circuit unreliability, coalescences of elements inputs.*

SECTION 6

Abrosimov M. B., Modenova O. V. **REFINEMENT OF LOWER BOUNDS FOR THE NUMBER OF ADDITIONAL ARCS IN A MINIMAL VERTEX 1-EXTENSION OF ORIENTED PATH.** Previously known result states that the minimal vertex 1-extension of any nonhamiltonian path orientation with the number of vertices more than 4 contains at least 4 additional arcs. In this paper, this bound is significantly refined, and upper bound for the number of additional arcs is given.
Keywords: *minimal vertex extension, path orientation, fault-tolerance.*

Abrosimov M. B., Suhov S. A. **ON THE NUMBER OF OPTIMAL 1-HAMILTONIAN GRAPHS WITH THE NUMBER OF VERTICES UP TO 26 AND 28.** A graph is called 1-vertex-hamiltonian (1-edge-hamiltonian) one, if it becomes Hamiltonian after deleting any its vertex (edge). 1-vertex-hamiltonian (1-edge-hamilton) graph is optimal if it has the minimum number of edges among all 1-vertex-hamiltonian (1-edge-hamiltonian) graphs with the same number of vertices. In the paper, the previous data on the number of optimal 1-vertex- and 1-edge-hamiltonian graphs with the number of vertices up to 26 are verified, and new data for 28-vertex graphs are given.
Keywords: *optimal 1-hamiltonian graph, minimal 1-extension of cycle, fault-tolerance.*

Avezova Y. E., Fomichev V. M. **ABOUT ONE HERITAGE CHARACTER IN CYCLIC SEMIGROUPS OF GRAPHS.** This paper is devoted to describing the character of loop existing at the given vertex subset in a cyclic semigroup of digraphs named as loop-character. Some attained bounds and formulae for the loop-character index are obtained. They are expressed in terms of circuit lengths in a digraph, which is the generator of the cyclic semigroup. An example showing the exactness of the bounds is given. The results can be used for estimating exponents of wide range primitive digraph systems.
Keywords: *loop-character, index of loop-character, exponent of graph system.*

Voblyi V. A., Meleshko A. K. **ENUMERATION OF LABELLED FLOWER WHEEL GRAPHS.** The exact formula is obtained for the number of labelled flower wheel graphs with the given numbers of vertices and petals.
Keywords: *rooted graph, wheel graph, flower wheel graph.*

Evdokimov A. A., Kutcenogaya E. P., Fedoryaeva T. I. **ON THE FULL DIVERSITY OF BALLS FOR GRAPHS.** The diversity of balls is studied for finite connected ordinary graphs. Some properties of graphs with full diversity of balls are obtained. As a

consequence, cactuses with such diversity of balls are described.
Keywords: *graph, metric ball, radius of ball, the number of balls, the diversity vector of balls.*

Zharkova A. V. **ON ATTRACTORS IN FINITE DYNAMIC SYSTEMS OF COMPLETE GRAPHS ORIENTATIONS.** Finite dynamic systems of complete graphs orientations are considered. The states of such a system $S = (\Gamma_{K_n}, \alpha)$, $n > 1$, are all possible orientations G of the complete graph K_n, and evolutionary function α transforms a given state G by reversing all arcs in G that enter into sinks, and there are no other differences between the given (G) and the next ($\alpha(G)$) states. The following criterion for belonging states to attractors in S is given: a state G belongs to an attractor if and only if it hasn't a sink or its indegrees vector is a permutation of numbers $0, 1, \ldots, n-1$. All attractors in S are the attractors of length 1, each of which consists of states without sinks, and the attractors of length n, each of which consists of states with indegrees vectors being permutations of numbers $0, 1, \ldots, n-1$. Any such an attractor represents a circuit, for every state G in which if the indegrees vector of G is $(d^-(v_1), d^-(v_2), \ldots, d^-(v_n))$, then the indegrees vector of $\alpha(G)$ is $(d^-(v_1)+1, d^-(v_2)+1, \ldots, d^-(v_n)+1)$, where the addition is calculated modulo n. Note that in system S, the number of attractors of length n is equal to $(n-1)!$ and the number of states belonging to them is equal to $n!$.
Keywords: *attractor, complete graph, evolutionary function, finite dynamic system, graph, graph orientation.*

Zhukovskaja A. O., Trenkaev V. N. **ABOUT SIMPLE CONDITIONAL EXPERIMENTS IDENTIFYING INVERTIBLE AUTOMATA OF A CERTAIN CLASS.** It is shown that, for any class of strongly connected automata obtained from an initialized invertible automaton R by changing its transition function in dependence on a key, there exists an identifying experiment of a length not more than $mn(m+3)/2$, where m and n are the numbers of states and input (output) symbols respectively in R.
Keywords: *initialized automaton, invertible automaton, strongly connected automaton, automaton identification, simple adaptive experiments.*

Karandashov M. V. **ABOUT TRANSITIVE PROPERTY OF MAPPINGS ASSOCIATED WITH A FINITE STATE MACHINES FROM THE GROUPS AS_P.** Checking the transitive property of the automaton mappings is discussed. A general criterion for transitivity of automaton mappings on words of length $k \in \mathbb{N}$ is presented. For automata from groups AS_p, an algorithm for checking transitive property is proposed. The complexity of the algorithm depends on the number of automaton states and does not depend on the input word length. The upper bound of the algorithm complexity is specified.
Keywords: *finite state machines, automata mappings, AS_p groups, transitivity.*

SECTION 7

Egorushkin O. I., Kolbasina I. V., Safonov K. V. **ON CONSISTENCY OF SYSTEMS OF SYMBOLIC POLYNOMIAL EQUATIONS AND THEIR APPLICATION.** Approaches to solving the systems of non-commutative polynomial equations in the form of formal power series are developed. The problems concerning the consistency of such a system are investigated on the base of the investigation of the commutative image of this system, which is obtained under the assumption that the symbols in the system denote variables taking values in the field of complex numbers and the operations in the system

are commutative.
Keywords: *non-commutative variables, polynomial equations, formal power series, commutative image.*

Knyazev V. N., Knyazeva M. S. **LYAPAS-T INTO FASM TRANSLATOR FOR WINDOWS AND LINUX.** Free translator from LYaPAS-T to fasm is presented. Fast Fourier transform for effective long numbers' multiplying, factorization and primality test algorithms implemented in LYaPAS-T are presented too. The purpose of the presentation is to popularize LYaPAS as a candidate for national programming language that can be used for writing trusted programs and building secure computer systems. Free translator is important for studying language now, when we don't have OS with LYaPAS integrated in. Lexical analyzer and parser generators flex and Bison were used for getting effective LALR-parser.
Keywords: *LYaPAS-T, translator, computer security, programming.*

Stefantsov D. A., Safonov V. O., Pershin V. V., Grechnev S. Yu., Tomskikh P. A. **MODULAR TRANSLATOR FROM LYAPAS.** The development of the modular translator from LYaPAS is discussed. The final goal of the development is having a compiler from LYaPAS written in LYaPAS. The translation process is divided into stages, each handled by a translator module. The modules are implemented as executable files that exchange data via files. The intermediate translation results are represented in auxiliary languages.

Chushkin M. S., Shelekhov V. I. **METHODS FOR SYNTHESIZING PREDICATE PROGRAM PIECES.** In the predicate language P, a program is a set of computable predicates. The formal operational semantics of P is developed. A total correctness formula for a predicate program with respect to its specification is presented on the base of the formal operational semantic. The synthesis problem for small pieces of a program in P is considered. The synthesized program is defined as a composition of subprograms. Some synthesis rules are applied. The rules are developed on the base of the total correctness rules for deductive verification of the predicate programs. The synthesis problem for the predicate programs is clarified on the example program for an effective calculation of Fibonacci numbers. Some methods to synthesize functional programs are developed. These methods may be successfully used in developing the program synthesis methods starting from a program specification and the specifications of additional programs in a decomposition of the source program.
Keywords: *formal operation semantics, program synthesis.*

SECTION 8

Gribanova I. A. **APPLICATION OF SOLVING SAT ALGORITHMS TO CONSTRUCTING DIFFERENTIAL PATHS FOR FINDING COLLISIONS OF CRYPTOGRAPHIC HASH FUNCTIONS IN THE MD FAMILY.** In this paper, we present a new method for constructing differential paths to find collisions of cryptographic hash functions in the MD family. The method is based on using the algorithms for solving Boolean satisfiability problem (SAT). The proposed method can be applied to hash functions based on the Merkle — Damgard construction, which, on its internal stages, use inner variables of relatively small size. We consider two copies of the algorithm for computing hash function value, that process some messages M and M', respectively. On the initial stage of the method, we construct two "template" CNFs C and C', which encode the process of computing hash-images for M and M'. The sets of Boolean variables used

in these two CNFs are disjoint. We combine CNFs C and C' via conjunction and add to the result the constraint specifying that hash values for M and M' are equal. Thus, we obtain the CNF $\tilde{C}$ that encodes the problem of finding collisions for the considered hash function. Then we add to $\tilde{C}$ additional constraints (in the form of clauses), that encode the corresponding differential path. In the context of the proposed method, we then explore the satisfiability of CNF of the form $\tilde{C} \wedge C_\Delta \wedge C_{\delta_k=c}$, where by C_Δ we denote the CNF, that takes the value 1 iff the difference between integer values specified by 512-bit vectors M and M' is equal to some constant Δ. By $C_{\delta_k=c}$ we denote the CNF, that takes value 1 iff a variable δ_k takes the value c. Here, δ_k is a 32-bit variable, that encodes the difference of integer values of hash registers at the step number k. The algorithms in the MD family use 32-bit inner variables. In this case, c is a 32-bit constant. Therefore, it is possible to check all of its possible values and consider SAT for CNFs of the kind $\tilde{C} \wedge C_\Delta \wedge C_{\delta_k=c}$. The SAT instances of this kind, for which we cannot obtain the answer in relatively small time (several seconds), are interrupted. Let c' be the value of δ_k, for which the solving of such SAT instance is interrupted, and assume that c' is not equal to the corresponding value in the known differential path. Then we can consider c' as a possible candidate for the value of δ_k in the new differential path.

The described algorithm is implemented in the form of parallel MPI program and tested on the computing cluster. As a result we managed to construct new differential path for finding collisions of MD4 hash function. This path differs from the path proposed by X. Wang in differential constraints for steps number $k \in \{13, 17, 20, 21\}$. We incorporated it into the propositional encoding of MD4, constructed the corresponding CNF, and applied to it the SAT solver `cryptominisat`, that has an option of enumerating multiple solutions. For the constructed CNF, the solver managed to find 1000 solutions in 416 seconds. In the application to the similar CNF produced for the Wang differential path, `cryptominisat` finds 1000 solutions in 520 seconds.

Keywords: *cryptographic hash function, collision, Boolean satisfiability problem, SAT, MD family hash functions.*

Kuznetsov A. A., Karchevsky S. S. **ON THE GROWTH FUNCTIONS OF FINITE TWO GENERATOR BURNSIDE GROUPS OF EXPONENT FIVE.** Let $B_0(2,5) = \langle a_1, a_2 \rangle$ be the largest 2-generator Burnside group of exponent 5. It has the order 5^{34}. There is a power commutator presentation of $B_0(2,5)$. In this case, every element of the group can be uniquely represented as $a_1^{\alpha_1} \cdot a_2^{\alpha_2} \cdot \ldots \cdot a_{34}^{\alpha_{34}}$, where $\alpha_i \in \mathbb{Z}_5$, $a_i \in B_0(2,5)$, $i = 1, 2, \ldots, 34$. Here, a_1 and a_2 are generators of $B_0(2,5)$, commutators $a_3, \ldots, a_{34}$ are recursively defined by a_1 and a_2. We define $B_k = B_0(2,5)/\langle a_{k+1}, \ldots, a_{34} \rangle$ as a quotient of $B_0(2,5)$. It is clearly that $|B_k| = 5^k$. A new algorithm for computing the growth function of B_k is created. Using this algorithm, we calculated the growth functions of B_k relative to generating sets $\{a_1, a_2\}$ and $\{a_1, a_1^{-1}, a_2, a_2^{-1}\}$ for $k = 15$, 16, 17.

Keywords: *Burnside group, the growth function.*