Г. П. Агибалов, SIBECRYPT'11. Обзор лекций и докладов,
ПДМ, 2011, номер 4, 105–120

АНАЛИТИЧЕСКИЕ ОБЗОРЫ

УДК 519.7

SIBECRYPT'11. ОБЗОР ЛЕКЦИЙ И ДОКЛАДОВ

Г. П. Агибалов

Национальный исследовательский Томский государственный университет, г. Томск, Россия

E-mail: agibalov@isc.tsu.ru

Приводится аналитический обзор лекций и докладов, представленных на Sibecrypt'11 — X Всероссийской конференции «Сибирская научная школа-семинар с международным участием „Компьютерная безопасность и криптография“», состоявшейся 5 – 9 сентября 2011 г. в Национальном исследовательском Томском государственном университете (г. Томск).

Ключевые слова: *прикладная дискретная математика, криптография, компьютерная безопасность, защита информации.*

Введение

Sibecrypt — это Всероссийская конференция под названием «Сибирская научная школа-семинар с международным участием „Компьютерная безопасность и криптография“». Её ежегодно, начиная с 2002 г., организует и в первой трети сентября проводит кафедра защиты информации и криптографии Национального исследовательского Томского государственного университета (ТГУ, г. Томск) в сотрудничестве с кафедрой программирования и компьютерной безопасности Института криптографии, связи и информатики (ИКСИ, г. Москва) на базе того или иного вуза или научного учреждения Сибири. Кроме докладов, на конференции Sibecrypt для её участников, а также для сотрудников и студентов принимающей организации (вуза, НИИ) ведущими специалистами в данной области (из числа участников конференции) читаются лекции по современным проблемам компьютерной безопасности, защиты информации и криптографии. Материалы конференции публикуются в приложении к журналу «Прикладная дискретная математика».

В 2011 г. Sibecrypt состоялась в 10-й раз — с аббревиатурой Sibecrypt'11, на этот раз — 5 – 9 сентября в Томске на базе ТГУ. Тезисы докладов, представленных в её программу, опубликованы в [1]. Аналитический обзор их содержания, а также содержания лекций, прочитанных на Sibecrypt'11, является целью данной статьи.

1. Лекции по криптографии и компьютерной безопасности

В лекции М. М. Глухова «К анализу некоторых систем открытого распределения ключей, основанных на неабелевых группах» проанализированы некоторые известные системы открытого распределения ключей в некоммутативных группах, основанные на проблеме сопряжённости в последних (A. Yamamura (1998, 1999); I. Anshel, M. Anshel, D. Goldfeld (1999); K. H. Koo, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park (2000)) и на её композиции (неявной или явной) с проблемой логарифмирования в таких

группах — так называемые MOR-системы (S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee, C. Park (2001); S. H. Paeng, D. Kwon, K. C. Ha, J. H. Kim (2001); C. Tobias (2004); E. Sakalauskas, P. Tvarijonas, A. Raulynaitis (2007)), а также система отечественных авторов из компании Молдовянов, сходная с последней из перечисленных MOR-систем (Moldovyan N. A., Moldovyan P. A. (2009); Moldovyan D. N., Moldovyan N. A. (2009); Молдовян Д. Н., Куприянов А. И., Костина А. А., Захаров Д. В. (2009); Молдовян Н. А. (2010)). Показано, в частности, что система E. Sakalauskas, P. Tvarijonas, A. Raulynaitis является частным видом систем, предложенных в работах В. М. Сидельникова, М. А. Черепнева, В. В. Ященко (1993) и В. М. Сидельникова (1994), а криптографическая стойкость системы открытого распределения ключей Молдовянов по порядку не превосходит сложности проблемы дискретного логарифмирования в циклической подгруппе порядка q мультипликативной группы простого поля $\mathbb{Z}_p$ или его расширении 2-й степени, где q является делителем числа $p-1$ или $p+1$ соответственно. Такой же результат получается и для всех других криптосистем подобного типа, в которых используются группы, определенные на алгебрах размерности 4 над полем $\mathbb{Z}_p$, и которые предлагаются в ряде работ Н. А. Молдовяна и его коллег.

Методы алгебраической геометрии в криптографии как предмет для фундаментальных научных исследований и учебной математической дисциплины представлены в одноимённой лекции И. А. Круглова. Интерес специалистов к ним вызван, прежде всего, их широким применением в реальных криптографических системах, в том числе в обретших статус государственного стандарта, и потребностями в их дальнейшем развитии в интересах науки и практики защиты информации. Наибольшее внимание в лекции уделено исследованию эллиптических кривых над конечным полем — их групп точек и реализаций на проективной плоскости, рациональных функций и дивизоров на проективных эллиптических кривых, эллиптических конфигураций и алгоритмов логарифмирования в группе точек эллиптической кривой и факторизации целых чисел с помощью эллиптических кривых.

Важнейшей составляющей компьютерной безопасности является безопасность программного обеспечения. Анализ программных реализаций и защита программ от анализа, программные закладки, пути их внедрения и методы противодействия им, уязвимости в программах и методы их использования, языки безопасного программирования и создание безопасных программ, интеграция политик безопасности и программных продуктов — вот далеко не полный перечень тех проблем, решением которых занимается наука под условным названием «Безопасное программирование». В лекции В. Г. Проскурина рассказано о методах решения части этих проблем, связанных с защитой программ от анализа и закладок. Примечательность этих методов и их особенная ценность заключается в том, что они не продукт досужего ума и теоретических изысков, но выстраданы, рождены и прошли серьёзнейшие испытания в многолетней практической работе Вадима Геннадьевича по защите реальных программных систем в условиях реальных угроз и атак. Заинтересованный читатель может найти их в подробном изложении в учебном пособии: *В. Г. Проскурин.* Защита программ и данных. М.: Издательский дом «Академия», 2011. 208 с.

История криптографии с древнейших времён до сегодняшнего дня стала предметом лекции А. В. Черёмушкина. В ней посредством ярких и запоминающихся иллюстраций прослежен путь развития и применения мировой криптографии от шифра простой замены до современных криптосистем с открытым ключом и отмечены некоторые из наиболее выдающихся достижений отечественных и зарубежных криптографов.

Криптография, базирующаяся на бесконечных разрешимых группах, представлена в одноимённой лекции, прочитанной В. А. Романьковым. Важнейшим тезисом лекции является демонстрация возможности сведения базовых математических задач криптографии к решению систем диофантовых уравнений.

Некоторые малоизвестные факты, относящиеся к первым десяти годам в 50-летней истории криптографии в Томском государственном университете, приведены в лекции Г. П. Агибалова. Они касаются, главным образом, истории создания и опубликования конечно-автоматного шифра, предложенного А. Д. Закревским в 1959 г., и алгоритмов криптоанализа и оценок теоретической стойкости, полученных Г. П. Агибаловым в 1964–1966 гг. для генераторов ключевого потока трёх классов: 1) линейных автономных автоматов над конечным полем; 2) нелинейных автономных автоматов с функцией выхода в качестве ключа и 3) нелинейных генераторов, порождающих многозначные нормальные (максимального периода) рекуррентные последовательности.

2. Теоретические основы прикладной дискретной математики

Как всегда, это направление на конференции Sibecrypt широко представлено результатами исследований дискретных функций и подстановок. Традиционными на ней становятся также методы алгебраической геометрии и комбинаторного анализа.

Два доклада Н. Г. Парватова посвящены проблемам полноты и выразимости в пространствах дискретных функций. Их решение имеет фундаментальное значение для выяснения важнейших закономерностей, существующих в мире дискретных математических объектов, и их приложений к математической кибернетике, информатике, защите информации и криптографии. Установлены необходимые и достаточные условия существования конечных нижних окрестностей у произвольных или заданных конечно порождаемых классов произвольного пространства и пространства с замыканием Галуа. Введены в рассмотрение сильно предупорядоченные пространства и установлено существование в них конечных нижних окрестностей у конечно порождаемых классов и конечных запрещающих множеств у классов с конечными верхними окрестностями. Установлена сильная предупорядоченность относительно подстановки переменных ряда функциональных пространств, в том числе пространства переключательных функций с замыканием. Построена теория Галуа для пространств переключательных функций с замыканием, описывающая его как замыкание Галуа. Тем самым найдено единое обобщение ряда различных теорий Галуа, содержащее их в качестве частных случаев и имеющее собственные приложения в теории переключательных схем. В силу этих результатов проблема выразимости для конечно порождаемого класса переключательных функций имеет решение в виде конечной нижней окрестности, классы которой имеют конечные запрещающие множества и одноэлементные описания. В связи с проблемой конечной порождаемости выделено новое семейство конечно порождаемых клонов — содержащих конечно порождаемый d- или произвольный (c, d)-подклон при натуральном c. Клоны с (c, d)-подклонами охарактеризованы свойствами инвариантных предикатов. Установлена возможность (c, r)-разложений клона над (c, d)-подклоном, известная ранее лишь в случае $c = 0$. Найдены предикатные и-описания клонов квазимонотонных и слабо существенных квазимонотонных функций, монотонных частей этих клонов. В частности, установлено, что монотонная часть является 2-подклоном в клоне квазимонотонных и $(1, 2)$-подклоном в клоне слабо существенных квазимонотонных функций. В связи с задачей выделения замкнутых классов в множествах точечных и минимальных точечных функций доказано, что в каждом из указанных двух множеств всякий замкнутый класс расширяется до некоторого макси-

мального из конечного множества. Построены примеры максимальных таких клонов. Явно описаны классы троичных функций, вычисляемых дизъюнктивными формами и произвольными формулами в каноническом базисе. Конструктивно доказано, что класс минимальных точечных функций на дистрибутивной точечной полурешётке порождается двухместными функциями. В качестве доказательства этого предложен метод формульного представления минимальных точечных функций на дистрибутивной точечной полурешётке в бинарных базисах, содержащих все одноместные минимальные точечные функции и некоторый набор специальных двухместных функций. Установлены необходимые и достаточные условия максимальности подклона, заданного расширенным и-описанием. На основе этого построена безызбыточная критериальная система в клоне квазимонотонных функций на полурешётке при суперпозиции со слабо существенными функциями. Найдена асимптотика её мощности в случае полурешётки всех непустых подмножеств множества k-элементного множества. Для функций на трёхэлементной полурешётке найдены безызбыточная нижняя окрестность множества минимальных точечных функций в клоне монотонных функций и безызбыточные критериальные системы в клонах монотонных и квазимонотонных функций. Эти результаты представляют особый интерес, так как функциями на трёхэлементной полурешётке описывается динамическое поведение дискретных асинхронных управляющих систем с двоичными статическими состояниями, и полученные решения проблем полноты и выразимости для них имеют прямое применение в проектировании таких систем.

Н. А. Коломеец в своём докладе описал все бент-функции, находящиеся на минимальном расстоянии от произвольной квадратичной бент-функции, и подсчитал их количество. Для функции от $2k$ переменных это число равно $2^k(2^1+1)(2^2+1)\cdot\ldots\cdot(2^k+1)$.

В докладе Е. П. Корсаковой введено графовое представление квадратичной булевой функции, в котором вершины графа суть аргументы функции, а рёбра соединяют те пары вершин, которые образуют слагаемые в АНФ функции. Типом графа назван упорядоченный по убыванию набор степеней его вершин. Функции названы графово эквивалентными, если их графы изоморфны. Для всех квадратичных бент-функций от 6 переменных определены типы их графов и построены классы их графовой эквивалентности. Оказалось, число первых равно 37, вторых — 50.

Для множества $\mathcal{B}_n$ бент-функций и множества $\mathcal{BI}_n$ итеративных бент-функций от n переменных Н. Н. Токарева доказала, в частности, что $|\mathcal{BI}_{n+2}| \geqslant |\mathcal{B}_n|^4/|X_n|$, где X_n есть множество всех булевых функций от n переменных, представимых суммой двух бент-функций, и сформулировала три гипотезы о числах $|\mathcal{B}_n|$ и $|\mathcal{BI}_n|$: 1) последняя оценка асимптотически точна; 2) $|\mathcal{B}_n|$ асимптотически равно 2^s, где $s = 2^{n-c} + d\binom{n}{n/2}$, c и d — константы, $1 \leqslant c \leqslant 2$; 3) $|\mathcal{B}_n|$ и $|\mathcal{BI}_n|$ асимптотически совпадают. Она высказала также гипотезу о том, что каждая булева функция от n переменных степени не больше $n/2$ представима суммой двух бент-функций от n переменных, из которой гипотеза 2 следует немедленно.

Говорят, что булева функция f *статистически не зависит* от подмножества Z своих переменных, если для любой её подфункции f', полученной фиксированием значений переменных в Z, имеет место $\Pr[f' = 1] = \Pr[f = 1]$. В докладе О. Л. Колчевой и И. А. Панкратовой, наряду с несколькими простейшими свойствами этого понятия, установлено, что если x, y, z суть непустые наборы различных булевых переменных и $f(x, y)$ статистически не зависит от переменных в x, то для любой булевой функции g от $|z| + 1$ переменной суперпозиция $g(f(x, y), z)$ также статистически не зависит от x, и это утверждение не допускает обобщения на случай, когда под знаком g вместо одной f стоят не менее двух функций от x, y, статистически не зависящих от x.

Дано описание подстановок степени n, представимых произведениями двух подстановок с фиксированным числом q мобильных точек (А. Б. Пичкур). Так, если $n \geqslant 8$, $4 \leqslant q \leqslant n/2$, то всякая подстановка G степени n с числом m мобильных точек не больше $2q-2$ представима произведением двух подстановок степени n с q мобильными точками. В других рассмотренных случаях, а именно когда $n \geqslant 4$, $2 \leqslant q \leqslant n/2$ и $m = 2q$ или $m = 2q-1$, подстановка G, имеющая r неединичных циклов с длинами $m_1, \ldots, m_r$, допускает требуемое представление тогда и только тогда, когда соответственно существует такое $I \subseteq \{1, \ldots, r\}$, что $\sum\limits_{i \in I} m_i = q$, или существуют такие $j \in \{1, \ldots, r\}$ и $I \cup \{k\} \subseteq \{1, \ldots, r\} \setminus \{j\}$, что $m_j > 2$ и $q - m_k + \sum\limits_{i \in I} m_i \in \{2, \ldots, m_j - 1\}$.

Во многих блочных шифрах блоки замены являются подстановками. Вместо приближений их аффинными функциями можно строить для них приближения другими подстановками, в некотором смысле более простыми. В докладе Б. А. Погорелова и М. А. Пудовкиной в роли последних рассматриваются подстановки, сохраняющие некоторую нетривиальную систему W областей импримитивности и образующие, таким образом, некоторую импримитивную группу IG_W. Множество всех таких систем W с r областями импримитивности мощности w обозначается $W_{w,r}$. Расстояние между подстановками определяется по Хэммингу, и для произвольной подстановки g определяются её порядки *W-примитивности* и *(w,r)-примитивности* как наименьшие расстояния от неё до подстановки соответственно в группе IG_W и в объединении $IG_{w,r}$ групп IG_W для всех $W \in W_{w,r}$. Авторам доклада удалось описать некоторые классы подстановок максимального порядка W-примитивности — так называемых бент-подстановок относительно заданной системы импримитивности W — и построить оценки числа таких подстановок. Порядок (w,r)-примитивности подстановки определяется однозначно её цикловой структурой. Перечислены цикловые структуры для всех подстановок в $IG_{w,r}$ и получены порядки их (w,r)-примитивности при чётной степени подстановки и для $w = r = 2$. Вычислены также порядки (w,r)-примитивности для блоков замены AES, ARIA, Whirlpool, MISTY1, Camellia, FOX.

Множество вейерштрассовых точек алгебраического функционального поля, ассоциированного с алгебраической кривой, является её инвариантом и может быть использовано для многих целей, в том числе для изучения группы автоморфизмов кривой, в частности её порядка. В докладе Е. С. Алексеенко предложен алгоритм для вычисления вейерштрассовых точек такого поля произвольной характеристики. Алгоритм сформулирован в предположении о наличии сепарирующего элемента в поле и известных процедур вычисления точек, дивизоров и пространств, ассоциированных с заданным дивизором.

Для натуральных ε и δ отображение f множества вершин графа G в множество вершин графа H называется $\langle \varepsilon, \delta \rangle$-вложением G в H, если для любой вершины v первого f обладает свойством $\langle \varepsilon, \delta \rangle$-ограниченного искажения: $f(S_\delta(v)) \subseteq S_\varepsilon(f(v))$ и сохраняет $\langle \varepsilon, \delta \rangle$-отделимость: $\operatorname{Im} f \cap S_\varepsilon(f(v)) \subseteq f(S_\delta(v))$, где $S_k(v)$ есть шар радиуса k с центром в v. В докладе А. А. Евдокимова конструктивно показано существование $\langle 4, 3 \rangle$-вложения целочисленной решётки размера $m \times m$ в n-мерный булев куб с асимптотически минимальной избыточностью и с мощностью решётки, удовлетворяющей соотношению $m^2 > 2^s$, где $s = n - 2\log_2 n(1+\varepsilon_n)$ и $\varepsilon_n \to 0$ при $n \to \infty$.

Функция $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ *корреляционно-иммунная порядка* $n-m$, если мощность пересечения грани размерности m в гиперкубе $\mathbb{Z}_q^n$ с множеством $f^{-1}(a)$ зависит только от $a \in \mathbb{Z}_q^n$; в этом случае наибольшее из таких $n-m$ обозначается $\operatorname{cor}(f)$. Плотность булевозначной функции $f : \mathbb{Z}_q^n \to \mathbb{Z}_2$ есть число $\rho(f) = |S_f|/q^n$,

где $S_f = \{a \in \mathbb{Z}_q^n : f(a) = 1\}$. Отображение $\mathrm{col} : \mathbb{Z}_q^n \to \mathbb{Z}_2$ называется совершенной 2-раскраской гиперкуба $\mathbb{Z}_q^n$, если существуют целые неотрицательные числа m_{ij} для i, j в $\{0, 1\}$, называемые параметрами раскраски, такие, что для каждой вершины $a \in \mathbb{Z}_q^n$ цвета $i = \mathrm{col}(a)$ число соседей цвета j равно m_{ij}. Среднее число вершин в $S \subseteq \mathbb{Z}_q^n$, находящихся на расстоянии 1 от вершины из дополнения $\mathbb{Z}_q^n \setminus S$, обозначается $A(S)$, т. е. $A(S) = \sum\limits_{x \notin S} |\{y \in S : d(x, y) = 1\}|/(q^n - |S|)$, где $d(x, y)$ — расстояние Хэмминга между наборами x и y. Доказано, что для любой булевозначной функции $f : \mathbb{Z}_q^n \to \mathbb{Z}_2$ справедливо неравенство $q\rho(f)(\mathrm{cor}(f)+1) \leqslant A(S_f)$, и f является совершенной 2-раскраской тогда и только тогда, когда в этом соотношении выполняется равенство (В. Н. Потапов).

Аналог теоремы Клини для языков конечных автоматов представлен в докладе Е. А. Пряничниковой для языков, представимых в отмеченных графах (с отмеченными только вершинами или с отмеченными только дугами). В нём регулярные выражения строятся с помощью операций теоретико-множественного объединения и обобщённых конкатенации и итерации языков. Операция обобщённой конкатенации $\overset{n}{\circ}$ имеет неотрицательный целочисленный параметр n, является бинарной, частичной и над произвольными словами u, w определяется как $u \overset{n}{\circ} w = xyz$, если $u = xy$, $w = yz$, $|y| = n$, и результат операции не определён в противном случае. Над языками L и R она определяется так: $L \overset{n}{\circ} R = \{u \overset{n}{\circ} w : u \in L, w \in R\}$. Унарная операция обобщённой итерации также параметрическая, и результатом её применения к языку L является объединение языков L_i, $i = 1, 2, \ldots$, где $L_1 = L$, $L_{i+1} = L_i \overset{n}{\circ} L$ для всех $i \geqslant 1$.

3. Математические методы криптографии

Важной характеристикой стойкости поточных шифров является расстояние единственности используемого ключевого потока. Основой построения многих ключевых потоков являются линейные рекуррентные последовательности (ЛРП) над конечными полем или кольцом. Часто за ключевой поток принимается последовательность значений старшего разряда в двоичном представлении элементов некоторой ЛРП. В этом случае характеристический многочлен последней называют характеристическим многочленом и данного ключевого потока. Расстояние единственности такого ключевого потока определяется как длина кратчайшего префикса, которым он (поток) отличается от всех других ключевых потоков с тем же характеристическим многочленом. Наибольшее из расстояний единственности ключевых потоков с одним и тем же характеристическим многочленом рассматривают как расстояние единственности самого многочлена. Это есть наименьшее натуральное число l, такое, что по префиксу длины l любого ключевого потока с данным характеристическим многочленом однозначно восстанавливается весь поток. Доклад А. В. Аборнева и Д. Н. Былкова посвящён поиску многочленов над примарными кольцами вычетов с расстоянием единственности, равным двум степеням многочлена. Эти многочлены интересны тем, что префиксы длины $2m$ всех ключевых потоков с одним и тем же характеристическим многочленом степени m задают на кольце подстановку степени m, которая в роли раундовой функции итеративного блочного шифра с аддитивным раундовым ключом часто обладает свойствами, противостоящими дифференциальному и линейному криптоанализам этого шифра. Примерами многочленов степени m с расстоянием единственности $2m$ являются тривиальные многочлены вида $x^m + 1 \pmod 2$. Существование других, нетривиальных, таких многочленов при любом m пока не установлено. Показано, однако, что многочлены вида $f_0(x)+2f_1(x)$, где $f_0(x) \equiv (x+1)^m \pmod 2$, $(f_1(x)+x^s, x+1) = 1$, $m = 2^k + s$, k натуральное и s нечётно, имеют расстояние единственности $2m$.

Отображения декартовой степени A^n конечного множества A в A^n со свойством идентифицируемости на подмножестве их координат рассмотрены в докладе Л. Н. Андреевой. Предложен способ расширения их до отображений большей степени, сохраняющих это свойство. В случае, когда такие отображения являются инволюциями, применяемыми в схемах разделения секрета, и в множество участников схемы вводятся новые участники, данный результат позволяет неавторизованные множества прежней схемы включить в неавторизованные множества новой схемы. Для произвольной инволюции q на A^n сформулирован и доказан тест идентифицируемости её на подмножестве координат I, заключающийся в проверке условий $q(x)[I] \neq q(y)[I]$ для всех x, y в A^n, где $x \neq y$.

Предложена доказуемо безопасная схема групповой подписи, построенная на основе известной схемы BBS, с возможностью отзыва права подписи у любого члена группы и добавления в группу новых членов (А. В. Артамонов, П. Н. Васильев, Е. Б. Маховенко). В ней ключом члена группы является тройка $(A, x, y) \in G_1 \times \mathbb{Z}_p^2$, где $A^{x+\gamma} = g_1 h^y$; $\gamma \in \mathbb{Z}_p$ — секретный ключ выпускающего менеджера группы; $\langle g_1 \rangle = G_1$ — циклическая группа простого порядка p; $h \in G_1$ — элемент открытого ключа группы. Для обеспечения полной анонимности в предложенной схеме вместо CPA-стойкой линейной схемы шифрования BBS используется модифицированная CCA-стойкая линейная схема Крамера — Шоупа. Для решения технических проблем, связанных с сохранением корректности ранее сгенерированных подписей после отзыва права подписи, с синхронизацией остальных субъектов и их баз данных, а также с принудительным обновлением локальных копий ключей всеми субъектами и всей базы данных членов группы выпускающим менеджером, в схему введён доверенный субъект. В результате процесс формирования подписи стал интерактивным с участием удостоверяющего центра, а проверяющий имеет возможность использовать для проверки актуальный на момент создания подписи открытый ключ группы.

Алгебраическая атака на один раунд упрощенного шифра AES, известного как S-AES, исследована в докладе Р. И. Воронина. При известных блоке открытого текста (ОТ) и соответствующем блоке шифртекста (ШТ) атака состоит в решении нелинейной системы из 32 булевых уравнений, связывающих 16 неизвестных бит раундового ключа с известными битами блоков ОТ и ШТ. В своей атаке автор исходит из двух пар известных блоков ОТ/ШТ при одном и том же раундовом ключе, заменяя (аппроксимируя) две соответствующие им нелинейные подсистемы уравнений одной — линейной системой L с 32 уравнениями и 16 неизвестными. Последняя, естественно, может быть несовместной. В докладе показано, что в случае случайного и фиксированного ключа справедливы следующие предложения: 1) при случайном равновероятном выборе блоков ОТ система L совместна с вероятностью 0,6074; 2) в отсутствие дефекта в сумме (побитовой по mod 2) одного блока ОТ с ключом и при случайном равновероятном выборе другого блока ОТ система L совместна с вероятностью 0,7725. Здесь под дефектом в булевом векторе длины 16 понимается наличие блока из одних нулей в его разбиении на 4 блока по 4 бита в каждом. О том, насколько эффективна данная атака, можно судить из следующего экспериментального факта: для некоторых ключа и одного блока ОТ находятся более 68 % вторых блоков ОТ, при которых система L имеет единственное решение — истинный ключ.

С. Ю. Ерофеев доказал диофантовость дискретного логарифма, построив систему уравнений E в натуральных переменных и известных натуральных i, p, n с простым p, такую, что если E имеет решение в натуральных числах и k° — значение некоторой переменной k в этом решении, то $n^{k^\circ} \equiv i \pmod{p}$, и наоборот, если $n^{k'} \equiv i \pmod{p}$

для некоторого натурального k', то система E имеет решение в натуральных числах и $k^\circ \equiv k' \pmod p$ для значения k° переменной k в этом решении.

В докладе С. Ю. Ерофеева и В. А. Романькова предложены схема построения односторонней функции (точнее, кандидата в односторонние функции) в свободной группе G с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости и протокол идентификации в группе, в которой, кроме того, неразрешима проблема двукратной эндоморфной сводимости. Если $X = \{x_1, \ldots, x_n\}$ — базис группы G, $g(x_1, \ldots, x_n)$ есть выражение элемента $g \in G$ через базисные элементы и отображение $\varphi : X \to G$ продолжается до эндоморфизма на G, то значение односторонней функции определяется на $g(x_1, \ldots, x_n)$ как элемент $f \in G$, такой, что $f = g(\varphi(x_1), \ldots, \varphi(x_n))$. Протокол идентификации построен по трёхшаговой схеме запрос-ответной идентификации — аналогично схеме Фиата — Шамира, но на другом математическом аппарате. В нём открытый ключ доказывающей стороны A есть пара различных элементов f, g в свободной метабелевой группе M_n достаточно большого ранга n ($n \geqslant 13$), а её закрытый ключ — эндоморфизм $\varphi \in \mathrm{End}(M_n)$, такой, что $\varphi(g) = f$. 1) Сторона A выбирает обязательство $\psi \in_{\mathrm{R}} End(M_n)$ и посылает проверяющей стороне B свидетельство $v = \psi(f)$. 2) Сторона B направляет стороне A запрос $c \in_{\mathrm{R}} \{0, 1\}$. 3) Если $c = 0$, то A посылает B ответ ψ; в противном случае — ответ $\psi\varphi$. 4) Сторона B проверяет равенство $v = \psi(f)$ или $v = \psi\varphi(g)$ соответственно. Протокол повторяется t раз, и если проверяемое равенство выполняется всякий раз, то идентификация принимается, в противном случае — отвергается. Авторы доклада полагают, что безопасность данного протокола основана на неразрешимости проблем эндоморфной и двукратной эндоморфной сводимости в M_n. Первая доказана В. А. Романьковым ранее (1979 г.), вторая утверждается в докладе.

Информация об аппаратной реализации шифра из японской криптосистемы FAPKC (*Finite Automata Public Key Cryptosystem*) представлена в докладе Д. С. Ковалёва и В. Н. Тренькаева. Реализация осуществлена с помощью САПР Xilinx WebPack ISE на базе ПЛИС Spartan-3 XC3S1500. Показано, в частности, что коэффициент эффективности (отношение производительности к количеству используемых ресурсов) этой реализации на порядок выше коэффициента эффективности известной аналогичной реализации RSA. Оказалось также, что с увеличением величины задержки расшифрования в ней число требуемых ресурсов ПЛИС значительно возрастает, а их рабочая частота убывает незначительно.

Стойкость режима шифрования к некоторой атаке принято оценивать разностью величин, i-я из которых есть вероятность того, что в данный шифртекст в данном режиме посредством данной атаки преобразуется i-й из двух случайно выбранных открытых текстов, $i = 1, 2$. В докладе И. А. Кукало проанализирована стойкость режимов шифрования в ГОСТ 28147-89 к атаке, основанной на парадоксе дня рождения. Приведены оценки такой стойкости для режимов простой замены, гаммирования и гаммирования с обратной связью, из которых следует, что для безопасного шифрования количество блоков открытого текста не должно превышать в первом режиме числа 1, во втором — числа 2^{31}, в третьем — числа $\sqrt{2^{64}/3}$.

В известной многошаговой корреляционной атаке на шифр Keeloq для выбора так называемых слайдовых пар на каждом шаге приходится перебирать пары булевых векторов длины 32 и для каждой из них проводить корреляционную атаку. В докладе О. Н. Лебедевой предложено сократить этот перебор, отсеивая те пары, для которых не выполняется некоторое вероятностное соотношение между битами в паре и известными в этот момент битами ключа.

Разности с нулевой вероятностью, называемые невозможными, успешно используются в криптоанализе ряда блочных шифров. В докладе М. А. Пудовкиной доказано существование трёхраундовых невозможных разностей и сформулированы условия существования четырёхраундовых невозможных разностей в XSL-алгоритмах блочного шифрования.

4. Математические основы компьютерной безопасности

Главные достижения отечественной науки в этом направлении, имеющие мировое значение, связаны с разработкой и исследованием математических моделей безопасности компьютерных систем (КС), и им мы обязаны Петру Николаевичу Девянину, его ученикам и последователям. На Sibecrypt эти достижения традиционно наиболее представительные, вызывают наибольший интерес, особенно в среде молодых и начинающих учёных.

В докладе П. Н. Девянина рассказано о результатах разработки ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux, о её основных отличиях от базовой модели этого класса, в частности о наличии в ней механизма ограничений в условиях и результатах применения правил преобразования состояний, потребовавшего использования наряду с монотонными и немонотонные правила при передаче прав доступа ролей или возникновения информационных потоков, что, в свою очередь, потребовало введения ограничений, инвариантных относительно немонотонных правил преобразования состояний КС в том смысле, что на любой траектории системы применение или неприменение немонотонного правила не влияет на выполнение ограничений в следующих за ним правилах преобразований. Доказано, что при наличии в КС только инвариантных ограничений в анализе условий передачи прав доступа ролей и реализации информационных потоков достаточно использовать только монотонные правила преобразования состояний.

Наиболее распространённым программным средством безопасного управления доступом и информационными потоками в ОС семейства GNU/Linux является КС SELinux. Естественно, возникает задача анализа безопасности самого этого средства. В докладе М. А. Качанова сообщается о разработке с этой целью ролевой ДП-модели безопасности управления доступом и информационными потоками в КС SELinux и о методе её применения для проверки возможности получения в КС права доступа и реализации информационного потока. В модели данная КС представляется системой, где каждое состояние задаётся набором объектов, а каждый переход из состояния в состояние осуществляется по одному из правил преобразования состояний. Применение модели на практике распадается на два этапа. На первом этапе строится начальное состояние модели по набору конфигурационных файлов моделируемой КС, на втором — его memory- и time-замыкания. Возможность получения заданного права доступа или реализации заданного информационного потока в КС обнаруживается проверкой истинности некоторых предикатов на построенных замыканиях.

Проблеме построения ДП-моделей для КС сетевого управления доступом посвящён доклад Д. Н. Колегова. Проблема осложняется рядом особенностей, присущих таким КС, не поддающихся адекватному отражению в ДП-моделях КС других типов. Важнейшие из них связаны со свойствами распределённости компонентов управления, его динамичности, множественности правил управления доступом для одних и тех же субъектов, принадлежности сущностей одновременно нескольким иерархиям и др. Для адекватного описания этих особенностей предложено язык ДП-моделей расширить, включив в него средства для задания множества функций иерархии сущностей,

множеств сущностей, параметрически ассоциированных с субъектом, прав доступа, свойственных сетевой КС, таких, как право доступа к её сушности, право конфигурирования её сущностей и т. п., множеств учётных записей и векторов доступа последних с узлов сети к сущностям, а также правила преобразования состояний с целью создания сессии удалённого доступа с правами доступа учётной записи и назначения субъекту в рамках этой сессии права доступа учётной записи.

Аналогичная проблема, но относящаяся к разработке дискреционной ДП-модели защищенных ОС, решается в докладе В. Г. Проскурина. Для адекватного моделирования таких КС в ДП-модель вводится ряд новых элементов, в том числе: множество учётных записей пользователей, делегирующих субъектам права доступа от имени свих учётных записей; право доступа *grant* для предоставления субъектом-владельцем ограниченного доступа к сущности субъектам, выполняющимся от имени других учётных записей; множество видов совместного действия и функции, задающие текущие доступы и разрешённые совместные доступы к сущностям-не субъектам; множество сущностей-параметров, не являющихся субъектами, для каждого права доступа к сущности; средства описания системы мандатного контроля целостности; правила преобразования состояний с целью порождения первого субъекта в сеансе работы пользователя и прекращения доступа субъекта к сущности.

Один из часто встречаемых видов атак на КС называется *фишинг*. Его название происходит от английского *phishing*, или *password fishing*, переводимого дословно как *выуживание паролей* и означающего по существу получение доступа к конфиденциальной информации обманным путём, использующим слабости человеческого фактора. Наиболее распространённым способом обмана в фишинге является создание вебсайта (фишингового ресурса), внешне почти неотличимого от другого сайта — жертвы фишинговой атаки. Пользователь последнего может не заметить отличий от него в первом и выдать тому свой пароль со всеми вытекающими для себя тяжёлыми последствиями. Для успешной борьбы с фишинговыми атаками такого рода требуется научиться обнаруживать фишинговые ресурсы, а для этого надо изучить характерные признаки таких ресурсов и на их основе разработать эффективные методы оценивания степени опасности информационного ресурса и определения потенциально опасных ресурсов. Этому посвящён доклад молодых исследователей А. В. Милошенко, Т. М. Соловьёва, Р. И. Черняка и М. В. Шумской. В нём описаны многие характерные признаки фишингового ресурса, в том числе сходство графического и (или) текстового контента (его и атакуемого сайта), наличие ресурса в фишинговых базах, применение редко используемых параметров формата URL, подозрительные регистрационные данные ресурса, наличие ресурса на IP-адресе ранее выявленного фишингового ресурса, наличие графического изображения текста, использование слишком большого числа скриптов. Предложены методы оценивания степени опасности ресурса по его признакам, использующие аппарат булевых функций, нейронных сетей, линейной регрессии, и механизмы выбора потенциально опасных ресурсов по отношению к заданному ресурсу, основанные на сравнении доменных имён ресурсов. Авторы полагают, что система защиты каждого информационного ресурса от фишинговых атак должна включать генерацию списка потенциально опасных доменных имён, получение списка зарегистрированных и доступных потенциально опасных информационных ресурсов, определение степени опасности каждого потенциально опасного ресурса, пополнение фишинговых баз вновь обнаруженными опасными ресурсами.

Для борьбы со спамом, распространяемым бот-сетями, нередко применяют графические капчи — картинки с проверочным текстом из символов с искажённым изобра-

жением, таким, что текст легко читается человеком, но не распознаётся компьютером. С их помощью можно предотвращать автоматические регистрацию почтовых ящиков, отправку сообщений, скачивание файлов, массовую рассылку и другие операции, необходимые для осуществления автоматического распространения спама. KCAPTCHA — один из программных продуктов с открытым кодом, предназначенный для генерации графических капч. В нём применяются около 20 шрифтов и волновые алгоритмы искажения символов. В докладе М. Б. Абросимова и А. А. Маторина сообщается о разработанной ими компьютерной программе для автоматического распознавания текста графических капч. В ней реализован алгоритм распознавания отдельных символов на основе анализа контрольных точек скелета изображения и связей между ними. С помощью этой программы были проанализированы цифры и латинские буквы, генерируемые в искажённом виде системой KCAPTCHA, и получен следующий результат: точность распознавания лежит в пределах от 87 до 99 %; время распознавания одного символа на компьютере с тактовой частотой 2,4 ГГц составляет около 30 мс.

О средствах безопасности веб-сервисов, реализованных в интернет-системе поддержки муниципальных заказов администрации г. Красноярска, сообщается в докладе Д. Д. Кононова и С. В. Исаева. Аутентификация пользователя для входа в систему осуществляется по его имени и паролю. Дальнейшие действия по редактированию (добавлению, модификации, удалению) данных в системе подтверждаются цифровой подписью, обеспечивающей юридическую силу и подлинность документов. Сертификат ЭЦП выполнен в стандарте X.509. На стороне клиента хранится только идентификатор сессии, действительный до её завершения. Всю криптографическую службу в системе несёт криптопровайдер КриптоПРО CSP.

5. Математические основы информатики и программирования

В последнее время в теории вычислительной сложности интенсивное развитие получило новое направление, связанное с рассмотрением так называемых параметризированных задач и алгоритмов. *Параметризированная*, или *П-*, задача состоит в том, что для заданных языка $L \subseteq A^* \times \mathbb{N}$ и пары $(I, k) \in A^* \times \mathbb{N}$ требуется определить, является ли (I, k) элементом L. Для алгоритма, решающего эту задачу, I есть вход и k — параметр задачи. Этот алгоритм называется параметризированным, или *П-алгоритмом*, если его вычислительная сложность есть некоторая функция $t(n, k)$ от длины входа $n = |I|$ и параметра k. П-задача считается разрешимой с фиксированным параметром, или FPT-разрешимой (от *Fixed-Parameter Tractable*), если она может быть решена некоторым П-алгоритмом за время $t(n, k) = \mathrm{O}(n^{\mathrm{O}(1)} \cdot f(k))$ для функции f, зависящей только от k. П-алгоритм, решающий такую задачу, называется *FPT-алгоритмом*. В докладе В. В. Быковой вводится мера сложности алгоритмов, называемая частной эластичностью, по которой можно сравнивать между собой и классифицировать все П-алгоритмы, в частности FPT-алгоритмы. Для произвольной функции $z = z(x, y)$ её *частной эластичностью* $E_x(z)$ по аргументу x называется эластичность переменной z как функции только от x при любом фиксированном значении y, где под эластичностью функции одного аргумента понимается предел отношения относительного приращения этой функции к относительному приращению её аргумента, т. е. $E_x(z) = z'_x \cdot x/z$. Аналогично определяется $E_y(z) = z'_y \cdot y/z$. В случае $z = z(x, y) = q(x)f(y)$, что характерно для функции сложности П-алгоритма, $E_x(z) = E_x(q(x))$, $E_y(z) = E_y(f(y))$ — обычные эластичности. По величинам $E_x(q(x))$, $E_y(f(y))$ пара функций $q(x)$, $f(y)$ может быть отнесена к одной из пар сложностных классов SUBPOLY, POLY, SUBEXP, EXP, HYPEREXP. Для П-алгоритма с вычислительной сложностью $z(x, y) = q(x)f(y)$

эта пара классов характеризует сложность данного алгоритма и по длине входа x, и по значению параметра y, и П-алгоритм является FPT-алгоритмом, если и только если она есть (SUBPOLY, POLY).

В аналитической теории формальных языков непосредственно составляющих (нс-языков) найдено новое достаточное условие, при котором система символьных уравнений, сопоставляемая нс-грамматике, имеет решение в виде формальных степенных рядов (К. В. Сафонов, Д. А. Калугин-Балашов). Для их нахождения система линейными заменами переменных приводится к виду, в котором она решается методом последовательных приближений, и ряды в решении исходной системы получаются как линейные комбинации рядов в решении приведённой системы.

О денотационном описании семантики языка аспектно-ориентированного программирования AspectTalk сообщено в докладе Д. А. Стефанцова и А. Е. Крюковой. Оно состоит из множеств L, S, M синтаксических областей, доменов и семантических отображений соответственно. Каждая синтаксическая область есть язык, грамматика которого получается из грамматики AspectTalk заменой аксиомы некоторым нетерминалом. Доменами выражаются сущности языка. Среди них есть, например, домен процедур — функций из домена состояний в домен состояний, и домен программ — функций из домена входных последовательностей в домен выходных последовательностей. Семантические отображения (они из L в S) задают интерпретацию языка.

Разработке и реализации библиотеки ORM (Object-Relational Mapping) на языке C++ посвящён доклад Д. А. Стефанцова, Н. О. Ткаченко, Д. В. Чернова и Р. В. Шамовой. В нём авторы проанализировали недостатки существующих подобных разработок — библиотек ODB (наличие дополнительного транслятора, невозможность автоматической проверки корректности программ до трансляции) и Wt::Dbo (необходимость поддержания данных от своих пользователей, использование частей строк запроса на языке SQL, возможность SQL-инъекций) и сообщили о своей разработке — о библиотеке COT (C++ ORM on Templates), лишённой этих недостатков. В ней использовано метапрограммирование на шаблонах, отмеченное в названии библиотеки. Предварительные испытания показали, что к тому же COT в среднем на 9 % превосходит ODB по производительности.

6. Вычислительные методы в дискретной математике

В связи с вычислительной сложностью комбинаторных алгоритмов решения криптаналитических задач внимание ряда специалистов приковано к проблеме распараллеливания таких алгоритмов. На Sibecrypt на этот раз представлены два доклада по этой проблеме. В докладе О. С. Заикина сообщено о попытках распараллеливания SAT-решателей в грид-системах, а в докладе В. М. Фомичёва — о параллельной реализации метода встречи посередине на кластерных и распределенных вычислительных системах.

Знакомство с этими и другими результатами по распараллеливанию комбинаторных алгоритмов показывает, что, к сожалению, усилия их авторов ограничиваются пока методами распараллеливания алгоритмов по входным данным, которые (методы) на практике принципиально не способны давать ощутимого положительного эффекта, когда речь идёт о задачах криптанализа. Дело в том, что ускорение вычислений от подобных методов в лучшем случае пропорционально количеству используемых процессоров в вычислительной системе, и если размер входных данных алгоритма достигает, скажем, 1000 бит, что по меркам криптанализа на самом деле очень малое число, а количество процессоров в системе равно, скажем, 2^{50}, что на самом деле пока

недостижимо, то лучшее, что может дать метод распараллеливания по входным данным, — это сократить объём перебора возможных вариантов решения задачи с 2^{1000} до 2^{950}, т. е. до величины, которая практически столь же неохватная, как и для последовательного алгоритма.

В докладе А. А. Семёнова, И. В. Отпущенникова и С. Е. Кочемазова традиционно (для А. А. Семёнова и К°) пропагандируется подход к решению всех комбинаторных алгоритмических задач посредством SAT-решателей, т. е. путём сведения задачи к SAT-задаче и решения последней с помощью известных программных комплексов. На этот раз среди решаемых так задач упоминаются анализ недетерминированного автомата, поиск неподвижных точек и циклов автоматных отображений в генных сетях, задачи о назначениях и целочисленного линейного программирования.

Библиотеку программ *Boolean Functions* на языке C++ разработали Н. А. Коломеец и А. В. Павлов. Она работает с булевыми функциями, задаваемыми в АНФ, таблично и в форме следа. На данный момент в ней есть программы перевода функций из одной формы в другую, проверки двух функций на их аффинную эквивалентность, порождения функций, аффинно эквивалентных данной, проверки функции на свойство бент, порождения бент-функций от 4, 5, 6 переменных, построения всех бент-функций на минимальном расстоянии от заданной, построения кодов из векторов значений бент-функций со свойством: прибавлением любой бент-функции к коду образуется линейный код, и др.

Шевченко М. Ю. (в устном сообщении) сформулировал некоторые достаточные условия, при которых задача коммивояжёра сводится с полиномиальной сложностью к задаче о назначениях и тем самым может быть решена за полиномиальное время.

7. Прикладная теория автоматов

Предложена (Ю. В. Березовская, В. А. Воробьёв) каузально-сетевая модель поведения популяции автоматов — совокупности взаимодействующих вероятностных конечных автоматов. Это есть *каузальная*, или *K-*, *сеть*, представляющая собой маркированную сеть Петри, в которой дополнительно для каждого перехода задана интенсивность его срабатывания как функция от маркировки входных позиций перехода. В ней позиции — это возможные состояния автоматов популяции, а вектор маркировки позиций своими компонентами задаёт количества автоматов, находящихся в соответствующих позициям состояниях. В отличие от сети Петри, в качестве маркеров позиций и весов дуг в K-сети допускаются положительные действительные числа, что позволяет маркировать позиции и помечать дуги вероятностями состояний и переходов между ними в автоматах. В качестве примера приводится K-сеть известной популяции «хищник — жертва» в ограниченной экологической нише.

Конечный автомат A называется скелетным, если отношение взаимной достижимости на множестве его состояний тождественно. Нумерация состояний автомата A числами из начального отрезка натурального ряда правильная, если состояния, достижимые из данного состояния, имеют меньшие, чем у него, номера. В докладе В. Н. Салия доказано, что 1) в автомате A существует правильная нумерация состояний, если и только если автомат A скелетный; 2) для автоматов A и B с $\mathrm{Sub}A \cong \mathrm{Sub}B$ число t состояний в B не меньше числа d классов взаимной достижимости в A и для любого автомата A существует скелетный автомат B, такой, что $\mathrm{Sub}A \cong \mathrm{Sub}B$ и $t = d$. Показано также, как путём удаления из диаграммы переходов автомата A минимального числа дуг можно получить скелетный автомат.

Автоматный шифр Закревского допускает аппаратную реализацию в виде перестраиваемого автомата T, в котором ключ шифра задаётся парой (k, s_0), где k — настройка и s_0 — начальное состояние. Автомат T устроен так, что в нём в каждый момент времени функция переходов выбирается из двух вариантов в зависимости от настройки и текущих входного символа и состояния. В докладе В. Н. Тренькаева, автора этой реализации, предложена атака аппаратного сбоя на неё с выбором открытого текста. Целью атаки является построить инициальный сильносвязный автомат Z (обычный, не перестраиваемый), который преобразует входные слова в выходные так же, как и автомат T с неизвестными, но фиксированными k, s_0. Суть атаки следующая. В автомате T вызывается неисправность, при которой функция переходов в нём выбирается в некотором одном известном варианте. С помощью установочного эксперимента определяется текущее состояние s этого неисправного автомата, после чего неисправность ликвидируется и с автоматом T проводится условный идентификационный эксперимент по определению неизвестной таблицы переходов эквивалентного ему автомата Z.

8. Прикладная теория графов

Графовые модели вычислительных систем (ВС) остаются по-прежнему наиболее эффективным средством в анализе и синтезе отказоустойчивых ВС. В роли адекватных моделей ВС, устойчивых к отказам компонент в системе и связей между ними, часто выступают соответственно вершинные и рёберные расширения требуемой кратности графа системы. Их исследования занимают важное место в тематике конференции Sibecrypt.

В докладе М. Б. Абросимова и П. П. Бондаренко рассмотрены минимальные вершинные 1-расширения циклов, в которых (циклах) одна вершина одного типа, а остальные — другого типа. Показано, что для цикла с n вершинами такие расширения имеют $(3n + 4)/2$ рёбер при чётном n и $(3n + 5)/2$ рёбер при нечётном n. Приведены примеры их при всех $n \in \{4k, 4k+1, 4k+2, 4k+3\}$, а также количества неизоморфных из них при $n = 2, 3, \ldots, 8$, подсчитанные путём порождения их всех на компьютере.

М. Б. Абросимов и А. А. Долгов в своём докладе показали, что диграфы из семейств Стокмейера не являются точными вершинными 1-расширениями никаких орграфов, из чего следует, что если есть орграф с тремя или более вершинами и с двумя или более неизоморфными точными вершинными 1-расширениями, то число вершин в нём не меньше 13, и эти его расширения нереконструируемые и не входят ни в одно известное семейство нереконструируемых орграфов.

В докладе М. Б. Абросимова и Д. Д. Комарова минимальное рёберное 1-расширение графа из двух звёзд с соединёнными центрами строится путём соединения рёбрами каждой из двух выбранных вершин степени 1, расстояние между которыми равно 3, со всеми вершинами степени 1, расстояния до которых от неё равно 3, и показано, как такое же расширение можно построить для стройного дерева, являющегося объединением некоторого числа цепей длины 2 и не менее двух цепей длины 1.

Наконец, в докладе М. Б. Абросимова и О. В. Моденовой рассмотрены свойства орграфа G, сохраняемые в его точном — G_t и минимальном — G_m вершинных k-расширениях. Показано, в частности, что 1) отношения смежности в G и G_t (G_m) являются одновременно рефлексивными либо антирефлексивными; 2) симметризация G_t является точным вершинным k-расширением симметризации G, симметризация G_m является вершинным k-расширением симметризации G; 3) если G — диграф с числом вершин больше 1, то G_t, если оно существует, есть также диграф; 4) дополнение G_t является

точным вершинным k-расширением дополнения G; 5) обращение G_t (G_m) является точным (соответственно минимальным) вершинным k-расширением обращения G.

В рамках проблемы синтеза компактных структур ВС рассмотрена задача синтеза компактных графов — регулярных графов минимального диаметра (В. А. Мелентьев). Сформулирован алгоритм синтеза таких графов, использующий представление графа проекциями — слоями вершин S_1, S_2, ..., достижимых из некоторой начальной вершины простыми путями длины 1, 2, ... соответственно. Получены нижняя и верхняя оценки для числа вершин в компактных графах заданной степени и заданного диаметра d, имеющих в себе цикл длины k для $3 \leqslant k \leqslant 2d-1$.

Важнейшей числовой характеристикой любого графа является его древовидная ширина, являющаяся мерой древовидности графа — того, насколько граф близок к дереву. Графы с ограниченной древовидной шириной образуют класс так называемых частичных k-деревьев. Многие NP-трудные задачи теории графов полиномиально разрешимы на частичных k-деревьях. *Древовидная ширина* $\mathrm{tw}(G)$ графа G определяется через понятие дерева декомпозиции этого графа, которое есть дерево T со следующими свойствами: 1) его вершины являются подмножествами множества вершин в G, образующими его покрытие; 2) для всякого ребра графа G имеется хотя бы одна вершина в T, содержащая обе вершины этого ребра; 3) для каждой вершины v графа G подмножество вершин дерева T, содержащих вершину v, порождает поддерево в T. Ширина дерева T есть $\mathrm{w}(T) = \max(|x|-1)$, где max берётся по всем вершинам x в T, и $\mathrm{tw}(G) = \min \mathrm{w}(T)$, где min берётся по всем деревьям декомпозиции T графа G. В докладе В. В. Быковой дан краткий обзор основных свойств древовидной ширины графа, методов её вычисления (точных и приближённых) для произвольных и некоторых специальных графов — хордальных, последовательно-параллельных и др., её нижних и верхних оценок, вычисляемых через другие параметры графа — наименьшую степень вершины, число вершинной связности, плотность, хроматическое число.

Проблеме факторизации графов посвящён доклад Е. А. Кармановой со следующими результатами: 1) связный граф тогда и только тогда является фактор-графом m-рёберной цепи, когда в нём есть обход длины m; 2) связный граф с m рёбрами является фактор-графом цепи P_{2m-1}; 3) для связного графа G с m рёбрами минимальное число $p(G)$ рёбер цепи, фактор-графом которой является данный граф, лежит в границах $m \leqslant p(G) \leqslant 2m-2$; 4) для дерева T с диаметром d и m рёбрами $p(T) = 2m-d$; 5) для звезды S_m верно $p(S_m) = 2m-2$.

В докладе А. А. Кочкарова, Л. И. Сенниковой и Н. Н. Болурова рассмотрены свойства предфрактальных графов. Указаны нижняя и верхняя оценки для числа точек сочленения и для числа мостов в предфрактальном графе, выраженные через длину траектории его получения, количество рёбер и число соответственно точек сочленения и мостов в затравке.

Улучшенные верхние оценки экспонентов (показателей) ε примитивных графов приведены в докладе В. М. Фомичёва. Для n-вершинных орграфов, где $n > 2$, с двумя контурами без общих вершин и с взаимно простыми длинами l и λ эти оценки линейные, а именно: $\varepsilon \leqslant l\lambda - 2l - 3\lambda + 3n$, если контуры не пересекаются, и $\varepsilon \leqslant l\lambda - l - 3\lambda + h + 2n$, если контуры имеют h общих вершин. Для неориентированнного графа с $n > 1$ вершинами и с наибольшей длиной l простого цикла нечётной длины $\varepsilon \leqslant 2n - l - 1$, а если простые циклы нечётных длин содержат все вершины графа, то $\varepsilon \leqslant n-1$. Показано также, что абсолютная оценка $\varepsilon \leqslant n^2 - 2n + 2$ для экспонента ε любого примитивного n-вершинного орграфа, установленная Виландтом, достижима на графах Виландта, и только на них. Здесь под графом Виландта под-

разумевается гамильтонов контур с дополнительной дугой между некоторыми двумя вершинами, находящимися в контуре на расстоянии 2. Множество всех таких графов с n вершинами состоит из $n!$ изоморфных графов. Для всех остальных n-вершинных примитивных орграфов с нечётным $n > 3$ верна оценка $\varepsilon \leqslant n^2 - 3n + 4$. Для неориентированных примитивных графов с $n > 1$ вершинами абсолютная оценка для экспонента есть $\varepsilon \leqslant 2n - 2$. Она достигается на графах, состоящих из гамильтоновой цепи и петли на одном из её концов, и только на них. Их множество состоит из $n!$ изоморфных графов.

Пару (S, δ) с отображением δ на конечном множестве S называют динамической системой, элементы в S — её состояниями. В её графе вершинами являются состояния, а дуги идут из вершин s в вершины $\delta(s)$. Он распадается на компоненты связности, каждая из которых представляет собой контур с входящими в него деревьями. Контуры всех компонент связности называются *аттракторами* системы. В докладе А. В. Власовой сформулирован критерий принадлежности состояния аттрактору в динамической системе (B^n, θ), где B^n есть множество всех булевых векторов длины n, и если каждый вектор $v \in B^n$ рассматривать как цикл, в котором первая компонента следует за последней, то $\theta(v)$ получается заменой в v каждой биграммы 10 биграммой 01. В таком векторе v максимальные из k-грамм $00\ldots0$ и $11\ldots1$ для $k \geqslant 2$ называются его соответственно 0- и 1-блоками длины $k-1$. Суммы длин всех 0-блоков и 1-блоков в v обозначаются $p_0(v)$ и $p_1(v)$ соответственно. Доказано, что состояние v динамической системы (B^n, θ) принадлежит аттрактору, если и только если $p_0(v) = 0$ или $p_1(v) = 0$; в этом случае в аттракторе, содержащем v, следующее (по стрелке) состояние получается из предыдущего циклическим сдвигом на одну компоненту соответственно влево или вправо.

В докладе В. С. Грунского и С. В. Сапунова рассмотрена задача определения своего местонахождения мобильным агентом (МА), блуждающим по графу G с помеченными вершинами. Предложено её решение с использованием понятий топологического идентификатора (ТИ) и диагностического тестового графа (ДТГ). Если через S_g обозначен подграф в G, порождённый всеми вершинами в G, достижимыми из вершины g, то ТИ вершины g есть помеченный граф D_g, такой, что для любой вершины h в G изоморфизм $D_g \cap S_g \cong D_g \cap S_h$ существует тогда и только тогда, когда $g = h$, где $D_g \cap S_h$ есть наибольший связный подграф в G, содержащий вершину g и изоморфно вложимый в S_h с отображением g в h. ДТГ получается отождествлением в ТИ D_g для всех g в G их одинаково помеченных инициальных вершин и преемников каждой вершины, имеющих одинаковые метки с заменой получающихся кратных дуг одной. Рассматриваемая задача решается в два этапа. Сначала по G строится ДТГ. Затем МА, стартуя из неизвестной ему вершины h графа G, на каждом шаге проверяет наличие в G путей, совпадающих по разметке с путями в ДТГ из его инициальных вершин, последовательно сокращая по результатам проверок множество возможных стартовых вершин до единственной. Утверждается, что на графах, в которых в замкнутой 1-окрестности каждой вершины все вершины помечены разными символами, данный алгоритм имеет полиномиальную сложность.

ЛИТЕРАТУРА

1. Тез. докл. X Сибирской научной школы-семинара с международным участием «Компьютерная безопасность и криптография» — Sibecrypt'11 (Томск, ТГУ, 5–9 сентября 2011 г.) // Прикладная дискретная математика. Приложение. 2011. № 4. 111 с.