АНАЛИТИЧЕСКИЕ ОБЗОРЫ

УДК 519.7

SIBECRYPT'12. ОБЗОР ДОКЛАДОВ

Г. П. Агибалов, И. А. Панкратова

Национальный исследовательский Томский государственный университет, г. Томск, Россия

E-mail: agibalov@isc.tsu.ru, pank@isc.tsu.ru

Приводится аналитический обзор лекций и докладов, представленных на Sibecrypt'12 — XI Всероссийской конференции «Сибирская научная школа-семинар с международным участием „Компьютерная безопасность и криптография“», состоявшейся 3 – 8 сентября 2012 г. в Институте динамики систем и теории управления СО РАН (г. Иркутск).

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 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.

Конференция посвящена одному из важнейших направлений в области информационной безопасности — математическому и программному обеспечению компьютерной безопасности (КБ). В последние годы в этом направлении наблюдается высокая активность исследовательской работы молодых ученых, и возникает настоятельная необходимость в организации их научного общения друг с другом и с известными специалистами в данной области. Именно эту цель и преследует школа-семинар, имея в виду, в первую очередь, интересы молодых ученых Сибири и крупных учёных европейской части России, Беларуси, Украины. Цель достигается путём организации и проведения обсуждений на её заседаниях фундаментальных проблем защиты информации в компьютерных системах и сетях и обмена научными результатами по их решению методами прикладной дискретной математики (ПДМ).

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 математическим проблемам компьютерной безопасности, защиты информации, информатики и криптографии. Материалы конференции публикуются в приложении к журналу «Прикладная дискретная математика», ставшем с 2012 г. самостоятельным журналом «Прикладная дискретная математика. Приложение».

В 2012 г. конференция состоялась в 11-й раз — с аббревиатурой Sibecrypt'12, на этот раз — 3–8 сентября в Иркутске на базе Института динамики систем и теории управления СО РАН. Тезисы докладов, представленных в её программу, опубликованы в [1]. Аналитический обзор в форме аннотаций их содержания, а также содержания лекций, прочитанных на конференции, является целью данной статьи. В соответствии с тематикой Sibecrypt'12 аннотации докладов разбиты по следующим её направлениям: теоретические основы ПДМ, математические методы криптографии и стеганографии, математические основы КБ, прикладная теория графов, математические основы информатики и программирования, вычислительные методы в дискретной математике.

1. Лекции по криптографии и информатике

О содержании понятия «электронная подпись» в Директиве 1999/93/ЕС от 1999 г. (далее Директива) и в Федеральном законе РФ от 2011 г. (далее ФЗ), регламентирующих порядок использования электронных подписей в Европейском сообществе и в России соответственно, рассказано в лекции А. В. Черёмушкина. Основные выводы докладчика следующие: 1) имеются принципиальные отличия определений основных понятий и систем технических требований в Директивах и ФЗ; 2) определения электронной подписи в Директивах и ФЗ ориентированы в основном на применение в юридической сфере и расходятся с математическим определением этого понятия. Полностью доклад опубликован в [2].

Обстоятельный обзор применения латинских квадратов в криптографии для построения шифров, схем аутентификации, однонаправленных функций, схем разделения секрета, криптографических хеш-функций и протоколов с нулевым разглашением представлен в лекции М. Э. Тужилина. Полностью текст опубликован в [3].

Одной из важнейших научных проблем, если не самой важной проблемой, современной теоретической информатики и компьютерной математики, будь то алгебра, теория чисел, дискретная математика, криптография или информационная безопасность, является сложность алгоритмов решения NP-трудных задач. Её математическое исследование предполагает построение подходящей модели вычислительной сложности и решение в рамках этой модели задач анализа и синтеза алгоритмов. В ряду первых важное место занимают задачи классификации алгоритмов по вычислительной сложности и построения для алгоритмов точных, рекуррентных или асимптотических оценок сложности. Важны также задачи разработки алгоритмов, решающих те или иные NP-трудные задачи с как можно меньшей сложностью.

Именно о решении этих задач шла речь на конференции в лекции В. В. Быковой. В ней за сложность алгоритма принята его эластичность, а точнее, эластичность функции его временной сложности от размера входных данных и, возможно, параметра задачи [4]. Так назван предел отношения относительного приращения этой функции к относительному приращению аргумента. Он характеризует коэффициент пропорциональности между темпами роста его временной сложности и размера входных данных или параметра задачи. Понятие эластичности заимствовано из экономики, где оно относится к производственным функциям. Это не единственный пример полезного заимствования математикой понятий из других областей науки. Достаточно вспомнить понятие энтропии состояния информационной системы по Шеннону как аналога энтропии состояния физической системы. Свойства эластичности алгоритма в теории сложности оказались столь же продуктивными, сколь и свойства энтропии в теории информации. И это открытие не может не восхищать математиков. Эластичность алгоритма легко вычисляется и выражается более простой формулой, чем

соответствующая логарифмически-экспоненциальная функция временной сложности, а построенная классификация по ней алгоритмов — от субполиномиальных до гиперэкспоненциальных — более прозрачна, нежели её прообраз.

В части, касающейся анализа алгоритмов, в лекции построены нижние и верхние асимптотические оценки временной сложности рекурсивных алгоритмов, решающих задачи путём последовательного уменьшения размера входных данных на некоторую константу. Из этих оценок следует, что такие алгоритмы могут быть только субполиномиальные, полиномиальные и экспоненциальные. Первые возможны лишь при одной подзадаче и беззатратном рекурсивном переходе, вторые — лишь в случае полиномиальной сводимости задачи к одной подзадаче меньшего размера, а третьи — всегда при числе подзадач больше 1 и только.

Параметризация задач — самый «молодой» из известных подходов к преодолению проблемы вычислительной сложности. Несмотря на его сравнительно малую изученность, его перспективность доказана в исследованиях многих зарубежных и отечественных учёных, в том числе и В. В. Быковой [4, 5]. В её лекции дана исчерпывающая двумерная классификация параметризированных и, в частности, FPT-алгоритмов по эластичности от размера данных и параметра задачи; в терминах эластичностей охарактеризованы параметризированные алгоритмы с низкой, равносильной и доминирующей зависимостями от параметра и установлены альтернативные формы характеризации FPT-разрешимости — аддитивная и смешанная, равносильные исходной — мультипликативной. Кроме того, рассказано о технологии построения FPT-алгоритмов для решения задач выбора (поиска и оптимизации в конечной области) методом динамического программирования на графах и гиперграфах с ограниченной древовидной шириной. В частности, осуществлена алгоритмизация этого метода на базе бинарного сепараторного дерева декомпозиции, позволившего решить присущую ему проблему памяти. Продемонстрированы FPT-алгоритмы решения задач SAT и о наименьшем вершинном покрытии графа, построенные на этой базе, и полиномиальные алгоритмы вычисления верхних и нижних оценок древовидной ширины графа и гиперграфа. Использование сепараторного дерева декомпозиции позволило для вычисления таблиц динамического программирования привлечь аппарат реляционной алгебры и ациклических баз данных и тем самым существенно снизить теоретическую и практическую сложность получаемых FPT-алгоритмов.

2 ноября 2012 г. В. В. Быкова успешно защитила докторскую диссертацию на тему «Методы анализа и разработки параметризированных алгоритмов» в совете Сибирского федерального университета по теоретическим основам информатики. От имени участников школы-семинара Sibecrypt поздравляем Валентину Владимировну с этим замечательным событием в её научной жизни и желаем ей дальнейших успехов в нашем общем деле.

В лекции А. А. Евдокимова рассмотрены свойства дискретных метрических пространств и метрик, которые возникают в исследовании вложений конечных пространств и графов. Отображения, в классе которых исследуются вложения, являются изометрическими, локально изометрическими и параметрическим семейством отображений ограниченного искажения. Последние при малых значениях параметров могут рассматриваться как дискретные аналоги непрерывных отображений, сохраняющих метрические свойства близости и отделимости элементов [6, 7]. Свойство k-продолжения метрики для связных графов с обычной метрикой пути означает, что любые две вершины графа, расстояние между которыми меньше k, принадлежат некоторой кратчайшей цепи длины k. Второе свойство связано с характеризацией комбинаторной

структуры шаров в графе, когда их радиусы последовательно возрастают от единицы до диаметра графа (раздувающиеся шары). Точнее, свойство r-разнообразия шаров означает, что шары одного радиуса с центрами в любых двух вершинах графа не равны (как множества вершин), если этот радиус не превосходит r (значение r не больше эсцентриситета графа). Приведены теоремы о значении рассмотренных свойств в вопросах вложений и классификации графов, а также некоторые нерешённые задачи.

Лекция А. А. Семенова посвящена основам структурной теории сложности алгоритмов и использованию различных формальных вычислительных моделей для определения классов двоичных языков, распознаваемых этими моделями. Рассмотрены: полиномиальная детерминированная машина Тьюринга и класс P, полиномиальная недетерминированная машина Тьюринга и класс NP, полиномиальная вероятностная машина Тьюринга и определяемые с её помощью классы (RP, co-RP, BPP), а также класс P/poly, образованный языками, распознаваемыми при помощи семейств схем полиномиальной сложности. Кроме этого, рассмотрена полиномиальная иерархия (иерархия Стокмейера), образованная языками, для определения которых используется оракульная машина Тьюринга. Приведены результаты, касающиеся аргументации сложности задач обращения ряда криптографических функций, базирующиеся на принятых предположениях относительно взаимосвязи между основными сложностными классами. В частности, в краткой форме приведено известное доказательство У. Шенинга того факта, что задача определения изоморфности пары простых графов не может быть NP-полной в предположении, что полиномиальная иерархия не стабилизируется на третьем уровне.

2. Теоретические основы прикладной дискретной математики

Дискретные функции по-прежнему находятся в центре внимания теоретических исследований, ориентированных на криптографические приложения.

В докладе А. М. Зубкова и А. А. Серова построены нижние и верхние оценки числа булевых функций, отстоящих по Хэммингу от аффинных и квадратичных функций на ограниченном расстоянии. Оценки получены с использованием формул включения-исключения и оценок хвостов биномиального распределения. Приведены условия, при которых они асимптотически эквивалентны.

Н. А. Коломеец доказал, что нелинейность всякой булевой функции от чётного числа n переменных, равной 0 (1) на наборах веса меньше (больше) $n/2$, не превосходит $2^{n-1} - \binom{n-1}{n/2}$, и эта оценка точная. Примечательно, что все эти функции обладают максимально возможной алгебраической иммунностью $n/2$, но их нелинейность, как видим, заметно отличается от максимально возможной $2^{n-1} - 2^{n/2-1}$.

Продолжая представление результатов исследования по проблеме статистической независимости суперпозиций булевых функций, начатое на предыдущей школе-семинаре, О. Л. Колчева и И. А. Панкратова на этот раз показали, что 1) если функции $f_1(x, y)$, $f_2(x, y)$ и $f_1(x, y) \oplus f_2(x, y)$ статистически не зависят от переменных в x, то этим свойством обладает и любая суперпозиция вида $g(f_1(x, y), f_2(x, y), z)$, и 2) если $f(x, y)$ статистически не зависит от переменных в x, то $f(x, y) \oplus g(x)$ тоже обладает этим свойством тогда и только тогда, когда f уравновешена или $g = \text{const}$. В этих утверждениях x, y, z — произвольные наборы значений булевых переменных.

Булева функция называется *почти уравновешенной*, если в любой грани области её определения количество элементов, на которых она равна 1, отличается от половины мощности грани не более чем на 1. В своём докладе В. Н. Потапов предложил

некоторые конструкции почти уравновешенных функций и установил некоторые свойства этих функций и нижнюю границу их числа. Он показал, в частности, что класс почти уравновешенных булевых функций является наследственным (содержит вместе с любой функцией и все её подфункции) с бесконечным набором минимальных запретов (функций не из класса, все подфункции которых принадлежат классу) и что булева функция f почти уравновешена, если и только если $f - h \in B_0$, где h — булева функция со значением 1 на всех наборах нечётного веса (и только) и $g \in B_0$, если $g : \{0,1\}^n \to \{-1,0,1\}$, $g^{-1}(1)$ и $g^{-1}(-1)$ — подмножества наборов соответственно чётного и нечётного веса и абсолютная величина суммы значений g на любой грани области её определения не превышает 1.

В текущем году С. В. Смышляев доказал гипотезу Голича о перестановочности (линейности) по первой или последней существенной переменной любой сильно совершенно уравновешенной булевой функции. В докладе на школе-семинаре он представил обобщение этой гипотезы как условие Голича в формулировке: «Сильная совершенная уравновешенность в P_k (для любого $k \geqslant 2$) эквивалентна перестановочности по первой или последней существенной переменной» и в свою очередь выдвинул гипотезу: «Условие Голича выполнено тогда и только тогда, когда k простое», доказав её в части необходимости простоты k и установив некоторые утверждения, косвенно подтверждающие эту гипотезу и в части достаточности.

В своё время, в 2011 г., Н. Н. Токарева сформулировала гипотезу о возможности разложения любой булевой функции от чётного числа n переменных степени не более $n/2$ в сумму двух бент-функций от n переменных. В докладе на школе-семинаре она доказала ослабленный вариант этой гипотезы, показав, что при чётном n любая булева функция от n переменных степени $d \leqslant n/2$ может быть представлена суммой не более чем $2\binom{2b}{b}$ бент-функций от n переменных, где b — наименьшее целое, такое, что $b \geqslant d$ и $(2b)|n$.

Булева функция f от чётного числа переменных n называется *функцией Касами*, если для некоторого $\lambda \in \mathrm{GF}(2^n)$ и любого $\beta \in \mathrm{GF}(2^n)$ имеет место $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, где $k = 2^{2d} - 2^d + 1$, $(n,d) = 1$, $0 < d < n$. При λ, не равном кубу элемента в $\mathrm{GF}(2^n)$, она является бент-функцией. Булева функция *s-существенно зависима*, если любое произведение s её переменных входит в моном её АНФ. В докладе А. А. Фроловой показано, что для любого чётного $n \geqslant 8$ функция Касами степени t является s-существенно зависимой, а её кратная производная по s линейно независимым направлениям не равна тождественно 0, если $s = t - 3$, $4 \leqslant t \leqslant n/2$, или $s = t - 2$, $4 \leqslant t \leqslant (n+3)/3$. Кроме того, она 2-существенно зависима, если $t \geqslant 4$.

В докладе К. Л. Глуско и С. С. Титова предложен метод решения квадратного уравнения $x^2 + x = a$ в поле $\mathrm{GF}(2^n)$ путём разложения его в систему булевых уравнений $x_{i-1}^2 + x_i + a_i = 0$, $i = 0, 1, \ldots, n-1$, связывающих компоненты векторов x^2, x и a.

В докладе В. А. Едемского и О. В. Антоновой предложен метод анализа линейной сложности последовательностей с периодом $2^m p^n$, построенных на основе обобщённых циклотомических классов. Метод позволяет для рассматриваемых последовательностей вычислять линейную сложность, получать её оценки, строить минимальный многочлен и определять последовательности с заведомо высокой линейной сложностью. Эти возможности метода продемонстрированы на ряде последовательностей, построенных на основе классов квадратичных и биквадратичных вычетов. Полностью доклад опубликован в [8].

Формулы для среднего и дисперсии числа векторов веса s или не больше s в случайном линейном двоичном (N, k)-коде, имеющем равномерное распределение на множестве всех таких кодов, выведены в докладе А. М. Зубкова и В. И. Круглова. Приведены формулы для среднего и дисперсии веса w покомпонентной суммы по модулю 2 двух независимых случайных булевых векторов длины N, имеющих вес s и t соответственно и равномерные распределения на множествах таких векторов, а также для вероятности равенства $w = m$. Дана также оценка сверху для вероятности линейной зависимости n независимых случайных булевых векторов длины N и веса s, имеющих равномерное распределение на множестве таких векторов.

В докладе А. С. Кузнецовой и К. В. Сафонова указано решение комбинаторной задачи, в которой для последовательности первых n натуральных чисел, записанных в произвольном порядке по окружности, требуется вычислить наименьшее число d транспозиций соседних чисел, чтобы все числа в окружности оказались записанными в естественном порядке: $1, 2, \ldots, n-1, n$, и приведены значения d для $n = 2, 3, \ldots, 12$.

Свойства наборов натуральных чисел с наибольшим общим делителем 1 изучены и алгоритм их перечисления предложен в докладе С. Н. Кяжина и В. М. Фомичёва. Полностью доклад опубликован в [9].

Вектор a из различных натуральных чисел, упорядоченных по возрастанию, называется *инъективным*, если для любого натурального числа α существует не более одного подмножества компонент этого вектора, сумма которых равна α. Вектор a *сверхрастущий*, если любая его компонента больше суммы всех предыдущих его компонент. Говорят также, что вектор $b = b_1 b_2 \ldots b_n$ получен из вектора $a = a_1 a_2 \ldots a_n$ операцией *сильного модульного умножения* относительно модуля m и множителя t, если m больше суммы компонент в a и $b_i = a_i t \bmod m$, $i = 1, 2, \ldots, n$. В докладе Д. М. Мурина показано, что количества инъективных векторов и сверхрастущих векторов с числом компонент (размерностью) n и наибольшим значением компоненты M ведут себя как полиномы степени $n-1$ от M, а пределы их отношений к числу всех векторов с теми же параметрами n и M при $M \to \infty$ и фиксированном n существуют, конечны и не равны 0. На основании результатов компьютерных экспериментов установлено, что при фиксированном натуральном n и значениях натурального M, близких к 2^{2n}, отношение количества различных инъективных векторов размерности n, полученных из сверхрастущих векторов размерности n с наибольшей компонентой меньше M с помощью сильного модульного умножения относительно модуля $m \leqslant \min(M, 2\sum_{i=1}^{n} a_i)$ и всевозможных значений множителя $t = 2, 3, \ldots, m-1$, к числу всех инъективных векторов размерности n с наибольшей компонентой меньше M достигает величины 0,9 и что операция сильного модульного умножения в применении к сверхрастущим векторам приводит чаще всего к векторам с малой евклидовой длиной.

Множество мобильных точек подстановки $G \in S_N$ обозначается $\Gamma(G)$, а множество всех подстановок с q мобильными точками — $\Gamma_N(q)$. Здесь $\Gamma(G) \subseteq \{1, \ldots, N\}$, $2 \leqslant q \leqslant N$. В докладе А. Б. Пичкура доказано, что если $N \geqslant 8$, $3 \leqslant q \leqslant N/2$ и $1 < |\Gamma(G)| < 2q-1$ или $N > 10$, $2 \leqslant t < N-2$, $2 \leqslant q < (N-t)/2+1$ и $t \leqslant |\Gamma(G)| \leqslant 2q+t-2$, то существуют подстановки $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+1)$ или $H_1 \in \Gamma_N(q)$, $H_2 \in \Gamma_N(q+t)$ соответственно, такие, что $G = H_1 \cdot H_2$. Показано также, что при $N \geqslant 4$, $2 \leqslant q < N/2$ подстановка из $\Gamma_N(2q+1)$ принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$, если и только если среди её неединичных циклов есть такие, сумма длин которых равна q, а при $N \geqslant 4$, $2 \leqslant q \leqslant N/2$ подстановка из $\Gamma_N(2q)$ принадлежит множеству $\Gamma_N(q) \cdot \Gamma_N(q+1)$, если и только если среди её неединичных циклов есть цикл длины $m_0 > 2$ и циклы длин

$m_1, \ldots, m_k$, таких, что $q - m_1 + \ldots + m_k \in \{2, \ldots, m_0 - 1\}$. Аналогичные характеризации имеются для подстановок из $\Gamma_N(2q + t - 1)$ и из $\Gamma_N(2q + t)$, принадлежащих произведению $\Gamma_N(q) \cdot \Gamma_N(q + t)$.

В совместном докладе Б. А. Погорелова с М. А. Пудовкиной и в отдельном докладе М. А. Пудовкиной изучены свойства групп преобразований векторного пространства над полем GF(2), порождённых парами операций, в которых одна операция — наложение вектора, а вторая — соответственно линейное преобразование и замена вектора по блокам.

Декомпозиции и аппроксимации недоопределённых данных посвящён доклад Л. А. Шоломова. Первая заключается в представлении, а вторая в реализации каждого недоопределённого символа набором символов 0, 1, * (неопределённость). Доказаны теоремы их существования и алгоритмов их эффективного построения для любого источника недоопределённых данных. Показана также возможность эффективного построения безызбыточных (тупиковых) декомпозиций и аппроксимаций и эффективной проверки равносильности двух разложений; построена полная система равносильных преобразований различных разложений недоопределённого источника.

Алгоритм с субэкспоненциальной сложностью для вычисления изогений (алгебраических морфизмов, являющихся групповыми гомоморфизмами) большой степени между эллиптическими кривыми предложен в устном докладе В. Г. Сухарева. Он построен по схеме алгоритма BCL (Broker — Charles — Lauter), в котором для более быстрой факторизации идеала в кольце изогений кривой используются идеи из субэкспоненциального алгоритма дискретного логарифмирования в классических группах (Hafner and McLurley).

3. Математические методы криптографии и стеганографии

В докладе А. В. Волгина и А. В. Иванова рассматривается генератор, порождающий последовательность $u_0u_1\ldots$ над полем $P = \mathrm{GF}(p^s)$ по рекуррентному соотношению $u_{n+1} = au_n + b$, $n \geqslant 0$, усложнённый маской $(e_0e_1\ldots e_s) \in P^{s+1}$, где все e_i представимы линейными комбинациями одних и тех же k элементов базиса поля P и $k < s$. Известно, что при известных разностях $u_i - e_i$, $i = 0, \ldots, t-1$, для $k+1 \geqslant t > 2$ и известных параметрах a, b, где a не принадлежит фиксированному подмножеству в P мощности меньше $2p^{\sigma_t} + \binom{k}{t-2} p^{2k-t+2}$ (σ_t — наибольший из делителей s, меньших t), значение u_0 находится с полиномиальной сложностью. Утверждается, что это верно и при неизвестном b и прежних остальных условиях.

В 2001 г. М. М. Глухов-мл. построил класс алгебро-геометрических кодов $\{C_r : [768, 3r - 57, 768 - 3r]_{256}, 39 \leqslant r \leqslant 255\}$ на кривой, заданной над $P = \mathrm{GF}(2^8)$ уравнением $y^3 = x^{60} + x^{57} + x^{54} + \ldots + x^3 + 1$. Из каждого кода C_r путём вычёркивания в его порождающей матрице любых $(768 - m)$ столбцов можно получить код $C'_{r,m}$, который при условии $114 < 3r < m \leqslant 768$ будет $[m, 3r - 57, m - 3r]$-кодом. В своём докладе на школе-семинаре автор этих кодов показал, что при $r \leqslant 127$ и фиксированном m число различных кодов $C'_{r,m}$ равно $\dfrac{1}{18}\binom{768}{m}$. Доказательство утверждения конструктивно и даёт возможность выбора столбцов порождающей матрицы так, чтобы все получаемые коды были различны. Этим результатом фактически заявлена новая идея образования порождающей матрицы кода в кодовых криптосистемах с открытым ключом. Изучены также условия на выбор столбцов в порождающей матрице кода C_r для получения кода $C'_{r,m}$ с тривиальной группой автоморфизмов. Доказано, что если композиция ав-

томорфизма и покомпонентного умножения всех кодовых векторов кода $C'_{r,m}$ на вектор $k \in P^m$ является автоморфизмом этого кода, то все компоненты в k одинаковы.

В докладе А. А. Камаевой рассматриваются упрощённые варианты хэш-функции Whirpool, в которых блочный шифр последней усечён до одного (двух) раундов, и показывается, что наибольшая вероятность найти коллизию для них равна 2^{-115} (2^{-225}).

Г. А. Карпунин и Е. З. Ермолаева результатами компьютерного эксперимента показывают, что трудоёмкость известного алгоритма построения коллизии для хэш-функции RIPEMD в квадрат раз выше заявленной его авторами (X. Wang, X. Lai, D. Feng, et al.).

В докладе Д. С. Ковалёва сообщается об аппаратной реализации на базе ПЛИС шифра FAPKC-4 и о его программных реализациях на языках Perl и PHP. Приведены результаты экспериментов с этими реализациями. Показано в частности, что в среднем ПЛИС-реализация на Virtex-5 XCVLX330T работает в 1,34 раза быстрее, чем PHP-реализация на компьютере с процессором Intel Core i5-2300, которая, в свою очередь, в 2,6 раза быстрее, чем Perl-реализация на том же компьютере.

В докладе К. Г. Когоса и В. М. Фомичёва обсуждается хорошо известная проблема разложения системы дискретных уравнений путём фиксации значений некоторых переменных на подсистемы, обладающие полезными свойствами (линейность, треугольность и т. п.), облегчающими их решение. Полностью доклад опубликован в [10].

В докладе А. М. Кореневой и В. М. Фомичёва описан итеративный блочный шифр, построенный путём конкретизации параметров обобщённой схемы Фейстеля, рассматриваемой как регистр сдвига длины m над множеством n-мерных булевых векторов с обратной связью — функцией от раундового ключа и компонент регистра. Шифр представлен как иллюстрация к этому обобщению схемы Фейстеля. В нём $m = 4$, $n = 16$ и функция обратной связи регистра выбрана так, что шифру обеспечивается свойство инволютивности.

В докладе С. Д. Лошкарёва с целью выяснения влияния булевых функций и констант циклических сдвигов в MD5 на стойкость этой хэш-функции к дифференциальному анализу построены разностное уравнение для каждого шага преобразования в ней и формула для среднего значения вероятности угадать решение этого уравнения при случайном и равновероятном выборе значений переменных и различных фиксациях значений параметров. Путём сравнения этих значений для разных булевых функций или разных величин циклических сдвигов можно сравнивать последние по степени их влияния на исследуемую стойкость MD5. Так, показано, что использование функции XOR в MD5 оптимально с точки зрения устойчивости MD5 к дифференциальной атаке и что для каждой булевой функции в MD5 все значения циклических сдвигов с этой точки зрения эквивалентны.

В связи с возможностью задания структур доступа, реализуемых в совершенных идеальных схемах разделения секрета, матроидами в докладе Н. В. Медведева и С. С. Титова вводится понятие *почти порогового* матроида. В нём все циклы имеют некоторую одну и ту же мощность n, но возможны подмножества мощности n, которые не являются циклами. Утверждается, что для $n = 1, 2, 3$ связного почти порогового, но не порогового матроида не существует. Матроид называется *разделяющим*, если для любых двух его элементов в нём есть цикл с одним из этих элементов, не содержащий другого. Утверждается, что бинарные (в $\mathrm{GF}(2^m)$) связные разделяющие почти пороговые матроиды исчерпываются кодами Рида — Маллера первого порядка.

В докладе Е. Л. Столова предложена последовательностная схема генератора случайных чисел, состоящая из конечного числа одинаковых комбинационных блоков,

работающих асинхронно и реализующих функцию 3-значной логики от двух переменных. Утверждается, что последовательность состояний схемы является марковским процессом с единственным финальным распределением вероятностей и с равномерным распределением на выходе каждого блока.

Один из видов цифровой подписи — *кольцевая* — позволяет любому участнику группы подписать сообщение от имени всей группы, а проверяющему убедиться, что подпись сделана участником действительно этой группы, но кем именно — ему не дано знать. В докладе Г. О. Чикишева кольцевая подпись наделяется свойством одноразовости: при подписании двух сообщений одним и тем же участником группы его личность становится известной. Это свойство требуется во многих приложениях, в том числе для электронного голосования, для обеспечения неотслеживаемости платежей в системах электронных денег и др. В предложенной кольцевой подписи оно достигается благодаря тому, что каждый участник имеет две пары (открытый ключ, закрытый ключ), и подписывающий использует оба закрытых ключа так, что повторное применение второго из них приводит к некоторому одному и тому же значению одной из компонент в разных кольцевых подписях, указывающему на соответствующие два открытых ключа и тем самым идентифицирующему подписавшего.

В докладе Г. И. Шушуева утверждается, что уравнение $(a, x_0) \oplus (a, x_5) = (c, k_4) \oplus \oplus (c, k_5)$, где x_0 — блок открытого текста, x_i и k_i для $i > 0$ — соответственно блок шифртекста на выходе i-го раунда и раундовый ключ этого раунда, $a = (0^{32}, 0^{32}, 0^{32}, c)$ и $c = \texttt{0x0011ffba}$, является оптимальным линейным приближением пяти раундов SMS4 (стандарта блочного шифра КНР для беспроводных сетей). Утверждается также, что минимальная трудоёмкость линейного криптоанализа девяти раундов SMS4 составляет 2^{115} операций зашифрования.

Результат обнаружения цифровых водяных знаков на основе модифицированной контрольной карты Хотеллинга существенно зависит от содержимого обучающей выборки. Опыт показывает, что лучшие результаты получаются, когда значения соответствующих пикселей изображений обучающей выборки и тестируемого контейнера близки, или, говоря другими словами, изображения в выборке и контейнере подобные. Задача автоматизации поиска подобных изображений решается в докладе Б. Б. Борисенко, предложившего считать изображение I более подобным изображению I_1, чем изображению I_2, если для некоторой хэш-функции h значение $h(I)$ ближе к $h(I_1)$, чем к $h(I_2)$, в некоторой метрике. В качестве h предложено использовать вейвлет-преобразование Хаара, последний уровень в котором определяется как первый из тех, на которых хотя бы один из размеров матрицы коэффициентов аппроксимации не превышает 32.

4. Математические основы компьютерной безопасности

Как и прежде на школе-семинаре, в проблематике этого направления важнейшее место занимают разработка и исследование математических моделей безопасности компьютерных систем (КС).

В докладе Д. М. Бречки представлен алгоритм поиска мостов в графе доступов модели Take-Grant между известными островами графа. Алгоритм основан на поиске в глубину, имеет полиномиальную сложность, предназначен для применения в анализе безопасности КС.

Достаточные условия для реализации информационного потока по памяти в операционных системах (ОС) семейства Linux сформулированы в докладе П. Н. Девянина.

Их проверка заключается в установлении истинности некоторого предиката ролевой ДП-модели управления доступом и информационными потоками в таких ОС.

Нередко реализация запрещённых информационных потоков по времени в ОС осуществляется с использованием интерфейса сокетов: наличие или отсутствие слушающего сокета на некотором порту может служить посылкой одного бита информации — соответственно 1 или 0. Некоторые известные методы предотвращения подобных информационных потоков проанализированы в докладе А. Н. Долгих. Предложен механизм регистрации событий с целью идентификации таких потоков.

В известных ролевых моделях управления доступом (RBAC и др.) отсутствуют средства задания и контроля прав доступов, учитывающие иерархию сущностей в КС. Модель иерархического ролевого управления доступом, RBAC-H, предложена в докладе Д. Н. Колегова. В ней, кроме всего прочего, введены типы сущностей, верхняя полурешётка $(L, \geqslant)$ уровней иерархии сущностей, функция f_e, задающая для каждой сущности её уровень в этой полурешётке, и предикат, истинный для тех и только тех субъект-сессий s, сущностей e и прав доступа p, для которых $f_e(e) \leqslant f_e(s)$ и право доступа p к сущности типа e принадлежит множеству прав доступа ролей субъект-сессии s. Это существенно расширяет класс компьютерных систем, в которых ролевое управление доступом адекватно выражается в математической модели.

Ещё одно расширение языковых средств ДП-моделей предложено в докладе П. Ю. Свиридова с целью адекватного описания мандатных и ролевых механизмов системы управления доступом RSBAC в ОС GNU/Lunux. А именно, в ДП-модель вводятся: множества атрибутов, ассоциируемых с сущностями и учитываемых при проверке прав доступа к последним; новые права и виды доступа и типы сущностей, характерные для RSBAC — право доступа на создание (клонирование) процесса, доступ для изменения рабочей директории, тип сущностей межпроцессорного обмена и т. п.; вместо линейной — произвольная решётка уровней доступа; множество прав доступа к сущностям определённого типа и функция прав доступа ролей к таким сущностям, как в RBAC-H.

Для анализа безопасности систем управления базами данных В. Ю. Смольянинов построил СУБД ДП-модель как модификацию известной РОСЛ ДП-модели и сформулировал в ней достаточные условия похищения прав доступа.

В докладе Н. О. Ткаченко показывается, как в СУБД MySQL (с дискреционным управлением доступом) может быть реализовано мандатное управление доступом путём использования механизма расширения безопасности системы SELinux. Для этого надо для каждой сущности СУБД MySQL задать контекст безопасности в виде набора атрибутов — пользователя, роли, типа и уровня безопасности, создать модуль политики безопасности средствами системы SELinux и разработать для СУБД MySQL компоненту с функциями Object Manager. Сообщается, как это сделано в конкретной реализации данного метода.

Обзор шести публикаций последних лет, посвящённых моделям атрибутного управления доступом в КС, дан в докладе Д. В. Чернова, сделавшего попытку изложить их основные свойства в терминах языка ДП-моделей.

Информация о лабораторном практикуме «Основы построения защищённых компьютерных сетей» на платформе Cisco Packet Tracer содержится в докладе Д. Н. Колегова и Б. Ш. Хасанова. Его целью является привлечение студентов к исследовательской работе по разработке архитектуры и методов проектирования защищённых компьютерных сетей, планированию и построению подсистем защиты информационных технологий, настройке механизмов и средств защиты сетевой инфраструк-

туры, поиску и устранению неисправностей в системах защиты компьютерных сетей. Кроме традиционной формы обучения практикум позволяет проводить многопользовательские и ролевые игры студентов по проектированию и анализу защищённых компьютерных сетей.

5. Прикладная теория графов

Много докладов на школе-семинаре было посвящено приложениям теории графов к синтезу отказоустойчивых управляющих и вычислительных систем. Традиционно сильно в данном направлении выступает Саратовская научная школа, от которой в этом году было представлено 6 докладов.

В 1995 г. Ф. Харари и М. Хурум высказали утверждение о том, что минимальное вершинное 1-расширение сверхстройного дерева с k цепями и p сложными вершинами содержит в точности $k+p+1$ дополнительных ребер, и предложили метод построения такого расширения. Здесь вершина сверхстройного дерева T, расположенная на ярусе $j>1$ в цепи длины m, называется *сложной*, если в T нет концевых вершин на $(j-1)$-м и $(m-j)$-м ярусах. В докладе М. Б. Абросимова и Д. Д. Комарова отмечается, что в общем случае построенное 1-расширение не обязательно является минимальным; приводятся примеры сверхстройных деревьев, имеющих 1-расширения с меньшим, чем $k+p+1$, числом дополнительных рёбер.

В докладе М. Б. Абросимова и Н. А. Кузнецова сообщается о вычислительном эксперименте с использованием распределённых вычислений, в рамках которого удалось построить все минимальные вершинные (MB-1P) и рёберные (MP-1P) 1-расширения циклов с числом вершин до 17; приводятся данные о количестве таких расширений.

В докладе М. Б. Абросимова и О. В. Моденовой изучаются орграфы, имеющие минимальные вершинные 1-расширения с одной и двумя дополнительными дугами; доказано, что 1) объединения нескольких двухвершинных цепей с одной или более изолированными вершинами, и только они, имеют MB-1P с одной дополнительной дугой; 2) среди связных орграфов гамильтоновы цепи, и только они, имеют MB-1P с двумя дополнительными дугами; 3) среди несвязных орграфов без изолированных вершин только орграфы, являющиеся объединением гамильтоновой цепи P_n с несколькими контурами C_{n+1} при $n>2$, имеют в своём MB-1P две дополнительных дуги; при $n=2$ добавляется ещё один случай: вместо контура C_3 можно взять транзитивную тройку. Представлен вид всех этих расширений.

Расширения неориентированных графов, вершинам которых могут быть приписаны различные типы, рассматриваются в докладе П. П. Бондаренко. Описаны все MB-1P и MP-1P цепей P_n, концевые вершины которых считаются принадлежащими одному типу, а неконцевые — другому. Доказано, что MB-1P таких цепей имеют $3k$ рёбер при $n=2k$ и $3k+2$ рёбер при $n=2k+1$, а MP-1P имеют $3k-1$ рёбер при $n=2k$ и $3k+1$ рёбер при $n=2k+1$.

Индексом состояния динамической системы называется расстояние от этого состояния до аттрактора. В докладе А. В. Жарковой предложен алгоритм вычисления индекса состояния динамической системы булевых векторов (B^n,θ), где для вектора v в B^n, рассматриваемого как цикл, в котором первая компонента следует за последней, $\theta(v)$ получается заменой в векторе v каждой биграммы 10 биграммой 01. Доказано, что максимальный индекс состояния в такой системе равен $(n-1)/2-1$ для нечётного n и $n/2-1$ для чётного.

В докладе Е. О. Кармановой рассматриваются *конгруэнции цепей*, т. е. такие отношения эквивалентности на множестве вершин цепи, все классы которых являются

независимыми множествами. Доказано, что количество конгруэнций m-рёберной цепи равно количеству эквивалентностей на m-элементном множестве; найдена длина кратчайшей цепи, фактор-графом которой является данный граф G; она равна $m + l - k$, где m — количество рёбер G, l — количество рёбер в минимальном цепном паросочетании на множестве вершин нечётной степени и k — максимальная из длин цепей в таких паросочетаниях.

Авторы И. С. Грунский и С. В. Сапунов рассматривают задачу разметки блуждающим агентом вершин графа так, чтобы в окрестности радиуса 2 каждой вершины все вершины были размечены разными метками. Предложены алгоритмы выполнения такой разметки агентом, наблюдающим из каждой вершины её окрестность радиуса 3, и агентом, наблюдающим только окрестность радиуса 2, но способным ставить метки двух типов; доказана вычислительная эквивалентность этих агентов.

Интервальной рёберной раскраской графа называется правильная раскраска его рёбер, при которой для каждой вершины графа рёбра, инцидентные ей, окрашены в последовательные цвета. Известно, что задача об интервальной рёберной раскраске NP-полна. В докладе А. М. Магомедова сформулирована теорема о том, что задача об интервальной рёберной раскраске остаётся NP-полной и для двудольных мультиграфов $G = (X, Y, E)$ с $|X| = 2$.

Разбиение множества рёбер двудольного графа $G = (X, Y, E)$ на паросочетания E_1, E_2, ... называется *непрерывным*, если любое ребро, инцидентное вершине x степени d из X, включено в одно из первых d паросочетаний. В докладе Т. А. Магомедова представлен алгоритм поиска такого разбиения, состоящий в последовательном удалении из графа минимальных паросочетаний, насыщающих все вершины максимальной степени. Доказано, что последний элемент разбиения является полным паросочетанием X с Y.

Задача построения графа, изоморфного заданному графу G, при помощи блуждающего по G агента A рассмотрена в докладе Е. А. Татаринова. Ранее автором был предложен базовый алгоритм решения этой задачи со сложностью $O(n + qt)$, где n — количество вершин графа, q — его цикломатическое число и t — длина максимального простого цикла в G. Наибольшего времени при этом требует проход по так называемому «красному пути» — пути, состоящему из уже пройденных вершин, для которых не все инцидентные им рёбра восстановлены. Здесь предложена модификация базового алгоритма, состоящая в том, что в помощь агенту A придаются ещё j агентов, располагающихся вдоль красного пути и способных передавать информацию (в частности, о расстоянии от агента до начала или конца красного пути) по цепочке. Тем самым сложность алгоритма понижена до $O(n + qt/j)$ в случае, если вспомогательные агенты поддерживают равные расстояния между собой.

В докладе Л. И. Сенниковой и А. А. Кочкарова рассмотрены предфрактальные графы, т. е. графы, полученные из связного графа-затравки за конечное число итераций, где каждая итерация состоит в замене в графе каждой вершины графом-затравкой и каждого ребра — ребром между произвольными вершинами соответствующих его концам графов-затравок. Предложен параллельный алгоритм поиска остовного дерева минимального веса (ОДМВ) на взвешенном предфрактальном графе. Алгоритм применяет стратегию «разделяй и властвуй»: ОДМВ отыскиваются (алгоритмом Прима) на подграф-затравках, изоморфных исходной затравке, затем результаты объединяются. Сложность алгоритма равна $O(n^{L+2})$, где n — количество вершин затравки и L — количество итераций. Заметим, что если алгоритм Прима применить к предфрактальному графу целиком, то получим сложность $O(n^{2L})$.

6. Математические основы информатики и программирования

В докладе А. Ю. Бернштейна и Н. В. Шилова исследуется задача о роботах в пространстве, которые, зная собственные координаты и координаты всех укрытий и имея возможность попарного общения и обмена укрытиями друг с другом, хотят перераспределить укрытия между собой так, чтобы пути от них к своим укрытиям не пересекались. Утверждается, что в случае бесконечного пространства не существует протокола решения этой задачи, если роботы обмениваются ограниченным числом бит информации, и что в случае конечного пространства существует протокол, который позволяет роботам, обмениваясь ограниченной информацией, узнать, пересекаются или нет их пути к своим укрытиям, не раскрывая своих координат другим.

В настоящее время существует множество распределённых СУБД со свойством масштабируемости, большая часть которых не использует реляционных схем данных. В работе И. Н. Глотова, С. В. Овсянникова и В. Н. Тренькаева предлагаются принципы построения системы управления реляционной MySQL-совместимой распределённой базой данных со свойствами масштабируемости и отказоустойчивости. За основу взята открытая СУБД MariaDB (ветка MySQL), которая изначально ориентирована на управление локальными данными. Особенностью предлагаемого решения является разделение сервера MariaDB на две части: ядро и движок. При этом движок вынесен на удалённый узел, который по сети принимает запросы от ядра. Для реализации данной схемы разработаны дополнительные модули для сервера MariaDB: виртуальный движок и виртуальное ядро, а также протокол VSVD сетевого взаимодействия этих модулей.

Проект добровольных вычислений SAT@home, созданный ИДСТУ СО РАН и ИСА РАН и предназначенный для решения задачи о выполнимости КНФ, представлен в докладе О. С. Заикина, М. А. Посыпкина и А. А. Семенова. Распределённое приложение проекта состоит из управляющей и расчётной частей. Управляющая часть отвечает за создание заданий в базе данных проекта и обработку результатов их выполнения. Основу расчётной части составляют SAT-решатели minisat-1.14.1 и minisat-2.0, модифицированные с учётом особенностей КНФ, кодирующих задачи обращения дискретных функций. На момент представления доклада в проекте SAT@home принимали участие более тысячи активных добровольцев и были задействованы более двух тысяч активно работающих ПК; успешно решены 9 из 10 тестов по криптоанализу генератора ключевого потока A5/1, не поддающихся анализу с использованием радужных таблиц. Средняя производительность проекта за весь период работы составляет 1,7 терафлопс.

В докладе А. Г. Банных рассматривается проблема выполнения массовых операций на многомерных массивах данных. Доказаны утверждения, позволяющие свести задачу с массовыми обновлениями к хорошо изученной задаче с единичными обновлениями, которую можно решать с использованием любых существующих структур данных. Это свойство позволяет выбирать оптимальную структуру данных для каждой задачи отдельно.

Большое внимание на школе-семинаре было уделено проблеме анализа программного обеспечения с целью восстановления алгоритма по тексту программы, исполняемому или объектному файлу. А. С. Бурлаков в своём докладе представил разрабатываемую им систему динамического анализа исполняемых файлов, которая эмулирует оперативную память и устройства ввода/вывода и может настраиваться на разные типы процессоров и компиляторов. Семантика машинных команд описывается на искусственном языке, разработанном автором; эмулятор при запуске читает описание

семантики, инициализируется должным образом и затем может дизассемблировать программы, скомпилированные для данного процессора, и выполнять их пошаговую отладку.

Проблеме декомпиляции объектных файлов DelphiB посвящён доклад А. А. Михайлова. С помощью разработанных автором структур данных, предназначенных для описания семантики машинных команд процессоров семейства Intel x86, решаются задачи извлечения имён вызываемых виртуальных методов, распространения констант, подстановки имён используемых переменных и т. д., которые существенно ускоряют восстановление алгоритма исследуемой программы.

В докладе А. М. Сауха рассматривается задача синтаксического и семантического анализа программ на языках высокого уровня, лексика которых задаётся с помощью регулярных выражений, синтаксис — контекстно-свободной грамматикой. Целью такого анализа является построение таблицы идентификаторов и выявление областей их использования. В результате получается абстрактное представление разбираемой программы, не зависящее от языка программирования и доступное для семантического анализа. В настоящее время в терминах системы формально описан язык C#; в дальнейшем предполагается расширить список языков.

7. Вычислительные методы в дискретной математике

Алгоритмы решения задач построения инволюции по её номеру и вычисления номера инволюции (в лексикографическом порядке) предложены в докладе Л. Н. Андреевой и В. А. Потеряевой. Приводятся результаты испытаний алгоритмов для инволюций порядков от 25 до 31.

Авторы Ю. Л. Зачёсов и А. М. Гришин, проведя (по опубликованным данным) сравнение оценки производительности метода решета числового поля факторизации чисел с экстраполированными оценками производительности самых мощных суперкомпьютеров из списка Top500, пришли к выводу, что трудоёмкость алгоритма факторизации при прогнозируемом увеличении размеров чисел, используемых в качестве параметров криптосистем, будет возрастать быстрее, чем производительность суперкомпьютеров.

Два доклада посвящены проблеме построения и исследования параллельных алгоритмов решения комбинаторных задач. В докладе А. В. Медведева сообщается об опыте реализации на видеокарте с использованием технологии CUDA алгоритма поиска совершенной нелинейности (т. е. расстояния до класса функций с линейной структурой) булевой функции, которая оказалась быстрее, чем последовательный алгоритм, примерно в 106 раз, а в сравнении с параллельной реализацией на центральном процессоре — примерно в 26,5 раз. Значительное увеличение производительности алгоритмов приведения базиса целочисленных решёток за счёт замены рекуррентного алгоритма Грама — Шмидта параллельными алгоритмами ортогонализации экспериментально продемонстрировано в работе В. С. Усатюка.

Для построения статистических критериев с заданными вероятностями ошибок требуется знание распределений используемых в этих критериях статистик. Вместо точных формул (которые зачастую слишком громоздки с вычислительной точки зрения) в качестве приближений часто используют формулы из соответствующих предельных теорем, относящихся к случаям, когда объём выборки неограниченно возрастает. Представляют интерес методы точного вычисления распределений статистик для выборок умеренного объёма. В докладе А. М. Зубкова и М. В. Филиной обсуждается такой способ точного вычисления распределений разделимых статистик с помощью

аппарата неоднородных по времени цепей Маркова и результаты численного исследования распределений статистики Пирсона для схем с числом исходов до нескольких сотен и числом испытаний до нескольких тысяч.

Авторами А. А. Семеновым и А. С. Игнатьевым ранее был предложен алгоритм гибридного SAT+ROBDD-логического вывода, решающий задачу обращения дискретной функции с помощью сведения её к задаче выполнимости КНФ. В представленном на школе-семинаре докладе строго доказана сходимость этого алгоритма.

ЛИТЕРАТУРА

1. Тезисы докл. Всерос. конф. «XI Сибирская научная школа-семинар с международным участием „Компьютерная безопасность и криптография“» — Sibecrypt'12 (Иркутск, 3–8 сентября 2012 г.) // Прикладная дискретная математика. Приложение. 2012. № 5. 135 с.
2. *Черёмушкин А. В.* О содержании понятия «электронная подпись» // Прикладная дискретная математика. 2012. № 3(17). С. 53–69.
3. *Туэжилин М. Э.* Латинские квадраты и их применение в криптографии // Прикладная дискретная математика. 2012. № 3(17). С. 47–52.
4. *Быкова В. В.* FPT-алгоритмы и их классификация на основе эластичности // Прикладная дискретная математика. 2011. № 2(12). С. 40–48.
5. *Быкова В. В.* FPT-алгоритмы на графах ограниченной древовидной ширины // Прикладная дискретная математика. 2012. № 2(16). С. 65–78.
6. *Евдокимов А. А.* Вложения графов в n-мерный булев куб и интервальное кодирование табло // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 15–19.
7. *Евдокимов А. А.* Вложения в классе параметрических отображений ограниченного искажения // Ученые записки Казанского госуниверситета. Сер. Физико-математические науки. 2009. Т. 151. № 2. С. 72–80.
8. *Едемский В. А., Антонова О. В.* Линейная сложность обобщённых циклотомических последовательностей с периодом $2^n p^m$ // Прикладная дискретная математика. 2012. № 3(17). С. 5–12.
9. *Кяжин С. Н., Фомичёв В. М.* О примитивных наборах натуральных чисел // Прикладная дискретная математика. 2012. № 2(16). С. 5–14.
10. *Когос К. Г., Фомичёв В. М.* О разветвлениях криптографических функций на преобразования с заданным признаком // Прикладная дискретная математика. 2012. № 1(15). С. 50–54.