АНАЛИТИЧЕСКИЕ ОБЗОРЫ

DOI 10.17223/20710410/10/12

УДК 519.7

SIBECRYPT'10. ОБЗОР ДОКЛАДОВ

Г. П. Агибалов

Национальный исследовательский Томский государственный университет, г. Томск, Россия

E-mail: agibalov@isc.tsu.ru

Приводится аналитический обзор докладов, представленных на IX Сибирской научной школе-семинаре «Компьютерная безопасность и криптография» — Sibecrypt'10, состоявшейся 7 – 10 сентября 2010 г. в Тюмени.

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

Введение

Sibecrypt — это 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 (г. Томск) в сотрудничестве с кафедрой программирования и компьютерной безопасности Института криптографии, связи и информатики (г. Москва). Среди её участников — учёные всех возрастов и званий — от студента до академика из вузов и научных учреждений страны, ближнего и дальнего зарубежья (России, Укаины, Беларуси, Канады, Франции и др.). Место проведения школы-семинара привязано к территории России от Урала до Байкала. Из года в год она кочует по городам и весям этого гостеприимного края, неся в него свет большой науки и знакомя своих участников с его достопримечательностями. Её уже принимали Томск (ТГУ, 2002, 2003, 2005), Иркутск (ИДСТУ, 2004), Шушенское (ШуБор, 2006), Горно-Алтайск (ГАГУ, 2007), Красноярск (СибГАУ, 2008), Омск (ОмГТУ, 2009). Школа-семинар 9-го созыва (Sibecrypt'10) состоялась 7 – 10 сентября 2010 г. в Тюмени. Тезисы докладов, включённых в её программу, опубликованы в [1]. Обзор их содержания является целью данной статьи.

Кроме докладов, на школе-семинаре Sibecrypt для её участников, а также для сотрудников и студентов принимающей организации (вуза, НИИ) ведущими специалистами в данной области (из числа участников школы-семинара) читаются лекции по современным проблемам компьютерной безопасности и криптографии. На школе-семинаре Sibecrypt'10 были прочитаны следующие лекции:

1. *Пичкур А. Б.*, *Черёмушкин А. В.* (г. Москва). Теоретико-числовые методы в криптографии.

2. *Девянин П. Н.* (г. Москва). Классическая и расширенная модели *Take-Grant*.

3. *Абросимов М. Б.* (г. Саратов). Графовые модели отказоустойчивости вычислительных систем.

4. *Агибалов Г. П.* (г. Томск). О свойстве обратимости с конечной задержкой конечных автоматов.

К сожалению, формат статьи не позволяет представить содержание этих достаточно насыщенных лекций. Можно только сказать, что материал лекций П. Н. Девянина можно найти в последнем его учебнике, материал лекции Г. П. Агибалова готовится к публикаци в журнале ПДМ, а лекции других авторов вошли в их учебные пособия, сданные в издательства.

1. Проблематика исследований, проводимых в России и за рубежом по тематике школы-семинара

Тематика школы-семинара имеет математическую направленность, и её научную основу образует прикладная дискретная математика. В соответствии с этим проблематику исследований, проводимых в России и за рубежом по тематике школы-семинара, составляют проблемы дискретной математики, возникающие в компьютерной безопасности и криптографии. Они распределяются по следующим основным направлениям:

1) теоретические основы прикладной дискретной математики — алгебраические структуры, дискретные функции, комбинаторный анализ, теория чисел, математическая логика, теория информации, системы уравнений над конечными полями и кольцами;

2) математические основы информатики и программирования — формальные языки и грамматики, алгоритмические системы, языки программирования, структуры и алгоритмы обработки данных, теория вычислительной сложности;

3) вычислительные методы в дискретной математике — теоретико-числовые методы в криптографии, вычислительные методы в теории чисел и общей алгебре, комбинаторные алгоритмы, параллельные вычисления, методы дискретной оптимизации, дискретно-событийное и клеточно-автоматное моделирование;

4) математические методы криптографии — синтез криптосистем, методы криптоанализа, генераторы псевдослучайных последовательностей, оценка стойкости криптосистем, криптографические протоколы, математические методы квантовой криптографии;

5) математические методы стеганографии — синтез стегосистем, методы стегоанализа, оценка стойкости стегосистем;

6) математические основы компьютерной безопасности — математические модели безопасности компьютерных систем (КС), математические методы анализа безопасности КС, математические методы синтеза защищенных КС;

7) прикладная теория кодирования — коды для сжатия данных и защиты информации, коды для обнаружения и исправления ошибок, построение оптимальных кодов, анализ свойств кодов;

8) прикладная теория автоматов — автоматные модели сетевых протоколов, криптосистем и управляющих систем, автоматы без потери информации, эксперименты с автоматами, декомпозиция автоматов, автоматные уравнения, клеточные автоматы;

9) логическое проектирование дискретных автоматов — математические модели и методы анализа, синтеза, оптимизации и оценки сложности дискретных автоматов, аппаратная реализация криптоалгоритмов;

10) математические основы надежности вычислительных и управляющих систем (ВиУС) — математические модели функциональной устойчивости ВиУС (к отказам, неисправностям, сбоям, состязаниям, исследованию), математические методы анализа функциональной устойчивости ВиУС, математические методы синтеза функциональ-

но устойчивых ВиУС, математические методы верификации логических схем и программ, математические методы синтеза самопроверяемых и контролепригодных схем;

11) математические основы интеллектуальных систем — базы данных, базы знаний, логический вывод, экспертные системы;

12) прикладная теория графов — графовые модели в информатике и программировании, в компьютерной безопасности, вычислительных и управляющих системах, в интеллектуальных системах.

В разные годы на школе-семинаре представляются разные направления из этого перечня. В 2010 г. на ней были представлены так или иначе все перечисленные направления.

2. Теоретические основы прикладной дискретной математики

В этом направлении, в связи с решением задач криптографии и защиты информации, внимание теоретиков по-прежнему занимают исследования по дискретным функциям, группам и конечным полям.

С использованием линейных комбинаций координатных функций степенных преобразований конечных полей построены классы нелинейных приближений произвольных булевых функций, сформулированы условия на вид преобразования, при которых эти приближения более точные, чем линейные, описаны множества показателей степени преобразования, удовлетворяющих этим условиям, эффективность таких приближений продемонстрирована применительно к бент-функциям, построенным с помощью координатных функций степенных преобразований поля с 2^n элементами (А. В. Иванов, В. Н. Романов). Для произвольной бент-функции и дуальной к ней функции установлено взаимнооднозначное соответствие между множествами подпространств, на которых соответственно эти функции аффинны (Н. А. Коломеец). Предложен новый метод построения бент-функций $g(a_1, a_2, x)$ от $n + 2$ переменных из бент-функций от n переменных $f_0(x), f_1(x), f_2(x), f_3(x)$ как $g(a_1, a_2, x) = f_i(x)$ для $i = a_1 + 2a_2$ (Н. Н. Токарева).

Исследованы оптимальные (максимальные и минимальные) кривые рода 3 над конечным полем с дискриминантом -19 (Е. С. Алексеенко, С. И. Алешников, А. И. Зайцев); приведены их уравнения и показано, что среди них нет одновременно максимальной и минимальной и нет гиперэллиптической.

Отмечены некоторые отличительные особенности дискретного преобразования Фурье в поле комплексных чисел и в конечном поле (А. М. Гришин).

Изучены возможности порождения подстановок множеством J_N полурегулярных инволюций степени $N = 2n$, а также величины $l(G)$ и $d(G)$, представляющие собой минимальное число соответственно первых и необязательно первых слоёв J_N^k, исчерпывающих группу $G \in \{A_N, S_N\}$ (М. Э. Тужилин); показано, в частности, что $J_4^2 = J_4^4 = W_4$ (четверная группа Клейна), $J_N^4 = A_N$ при $N \neq 4$, $<J_N> = A_N$ и $d(A_N) = 1$, $l(A_N) = 4$ при чётном $n \neq 2$, $<J_N> = S_N$ и $d(S_N) = 2$ при нечётном n и, кроме того, $l(S_2) = 2$ и $l(S_N) = 5$ при $n > 1$; описаны цикловые структуры подстановок, не входящих в J_N^3; рассчитаны мощности слоёв J_N^k для $N \leqslant 20$ и указано количество классов сопряжённых элементов в слое J_N^k для $k = 2, 3, 4, 5$.

Криптографические свойства гаммы, вырабатываемой генератором с внешним управлением, в значительной степени зависят от свойств управляющей последовательности (УП), в частности от свойства её h-периодичности относительно разных функций h, определённых на множестве всех слов в ней. Для конкретной функции h это свойство означает существование натуральных v и s, таких, что на множестве слов

длины s, образующих разбиение части УП, начинающейся с её v-го члена, функция h постоянна. Наименьшие такие v и s называются длинами соответственно h-предпериода и h-периода данной УП. В докладе В. М. Фомичёва показано, что: 1) в случае аддитивной h длина h-периода чисто периодической УП делит её период; 2) длина h-периода линейной рекуррентной последовательности над конечным полем P, имеющей максимальный период, совпадает с длиной последнего, если h является частотой m_a символа $a \in P \setminus \{0\}$, набором m частот символов (функцией маркировки) или (в случае $P = \mathrm{GF}(k)$, $k = 2, 3$) суммой wt всех символов в слове и делит её с делителем, делящим $(k-1)/2$, если $P = \mathrm{GF}(k)$, $k > 3$ и $h = \mathrm{wt}$; 3) длина h-периода последовательности де Брёйна порядка n при всех $h \in \{m_0, m_1, m, \mathrm{wt}\}$ равна 2^r, где $r < n$; 4) в классе генераторов гаммы, включающем генераторы «$\delta-\tau$-шагов» и генераторы с перемежающимся шагом, если длина m-периода УП с длиной m-предпериода, равной 0, равна τ, то при некотором $i \in \{0, 1, ..., t-1\}$ символы $\gamma_{i+r\tau}$ гаммы при каждом $r = 0, 1, ...$ линейно выражаются через символы состояния генератора в i-м такте.

3. Математические методы криптографии

Это направление на школе-семинаре представлено методами анализа и синтеза симметричных шифров — блочных, поточных, автоматных.

Важной характеристикой стойкости всякого поточного шифра к той или иной атаке на него является его теоретическая стойкость, называемая также расстоянием единственности, определяемая как наименьшая длина начального отрезка ключевого потока (гаммы), достаточной для достижения успеха этой атаки. В криптоанализе поточных шифров широко распространена атака на поточный шифр с угрозой однозначного предсказания его гаммы, сводящаяся к однозначному определению текущего состояния генератора гаммы. Теоретическая стойкость шифра к такой атаке есть длина L кратчайшего отрезка гаммы, по которому возможно однозначное восстановление того состояния генератора гаммы, в котором он окажется после выработки этого отрезка. Если через N_t обозначить число состояний генератора, в которые он может перейти за $t \geqslant 0$ тактов работы и не может перейти за меньшее число тактов из всевозможных начальных состояний без предшественников (тех состояний, в которые нет переходов из других состояний), и положить $K_t = K - \Sigma N_i$, где K — число всех состояний генератора гаммы и сумма Σ берётся по всем i от 0 до t, то $L \leqslant \min(t_1, P + T)$, P и T — длины соответственно предпериода и периода гаммы, t_1 — наименьшее t, при котором $K_t = 1$. В докладе С. А. Киселёва поставлена задача вычисления чисел N_t для поточного шифра A5/1 и показано, что для этого шифра $N_0 = 3 \cdot 2^{61}$, $N_1 = 13 \cdot 2^{58}$, $N_2 = 334 \cdot 2^{53}$, $N_3 = 2792 \cdot 2^{49}$. Кроме того, доказаны теорема о том, что обратимость функции переходов схемы генератора гаммы из регистров сдвига с обратной связью и обратимой функцией переходов равносильна возможности однозначного определения текущего значения функции управления сдвигом состояний регистров в ней по её состоянию в следующий такт работы, и с помощью этой теоремы — утверждение о невозможности такого определения в схеме A5/1.

Описана в общем виде дифференциальная атака на произвольный итеративный r-раундовый блочный шифр с желаемой вероятностью успеха (А. И. Пестунов): при заданной дифференциальной характеристике первых $r-1$ раундов шифра с разностью Δ_{inp} на входе первого раунда и с разностью Δ_{out} на выходе $(r-1)$-го раунда создаются $G \cdot T$ пар блоков открытого текста и столько же пар соответствующих блоков шифртекста, разбитых на G групп по T пар в каждой; последовательно перебираются ключи последнего, r-го, раунда; на каждом таком ключе k с помощью функции раунда

расшифровываются пары блоков шифртекста в g-й группе для $g = 1, 2, ..., G$, и если в каждой группе хотя бы одна пара блоков шифртекста расшифровывается в блоки с разностью Δ_{out}, то k принимается за истинный ключ последнего раунда шифра. Параметры G и T этой атаки зависят от вероятности используемой дифференциальной характеристики, от параметров шифра и желаемой вероятности её успеха. Приведена таблица, в которой для разных параметров шифра и вероятности успеха не менее 0,99 указаны расчётные значения G и T и сложности данной атаки — количества шифрований, требуемых блоков и объёма памяти.

В последнее время всё больше работ посвящается атакам на шифры, основанным на методе связанных ключей и использующим подходящие слабости алгоритма развёртывания ключа. Об атаке такого рода на шифры с алгоритмами развёртывания ключа из класса алгоритмов, свойственных таким шифрам, как 25-раундовый ГОСТ 28147-89, LOKI89, LOKI91, MMB, TREYFER, KeeLog, сообщено в одном из докладов М. А. Пудовкиной. Трудоёмкость атаки равна трудоёмкости опробования одного раундового ключа.

Ряд атак на ГОСТ 28147-89 с использованием двух или четырёх связанных ключей продемонстрирован в докладе М. А. Пудовкиной и Г. И. Хоруженко. Так, с использованием пары ключей $k, k' \in \{0,1\}^{256}$, связанных соотношением $k \oplus k' = \varepsilon = (e0\dots0e0\dots0e0\dots0e0\dots0e0\dots0)$, где $e = 10\dots0 \in \{0,1\}^{32}$, на основе метода дифференциального криптоанализа и метода связанных ключей находятся раундовые ключи $k_{26}, \dots, k_{32}$, а раундовый ключ k_{25} определяется с помощью методов бумеранга и связанных ключей. В зависимости от свойств блоков замены трудоёмкость атаки лежит в пределах от $2^{26,6}$ до 2^{40}, количество пар блоков открытого текста — в границах между 2^{15} и 2^{29}; вероятность успеха атаки равна 0,98. Описан класс блоков замены, при которых эта атака неприменима. С использованием четвёрки ключей, связанных соотношениями $k \oplus k' = k'' \oplus k''' = \varepsilon$, $k \oplus k'' = k' \oplus k''' = (e0\dots0)$, предложена атака на основе методов связанных ключей, дифференциального криптоанализа и бумеранга с трудоёмкостью нахождения ключа шифрования $2^{44,8}$ шифрований, с числом блоков открытого текста $2^{26,2}$ и с вероятностью успеха 0,99.

Введено семейство блочных симметричных шифров, в которых алгоритмы шифрования и развёртывания ключа имеют структуру алгоритма шифрования криптосистемы Whirlpool (ещё один доклад М. А. Пудовкиной). Построена атака методом дифференциального криптоанализа на 6 раундов произвольного шифра в этом семействе. В ней первые три раунда моделируются трёхраундовой дифференциальной характеристикой шифра, а прохождение последних трёх раундов обеспечивается возможностью вычисления части блока на выходе 3-го раунда по части раундового ключа 5-го раунда, обязанной свойству алгоритма развёртывания ключа. Трудоёмкость нахождения ключа шифрования оценивается сверху числом $2^{236,3}$, вероятность успеха атаки равна 0,9999999993, число используемых блоков открытого текста — $2^{107,3}$, что меньше квадратного корня из числа всех ключей.

Задача восстановления закрытого ключа по открытому в криптосистеме Мак-Элиса на основе кодов Рида–Маллера и в криптосистеме Мак-Элиса — Сидельникова заключается, как известно, в решении матричного уравнения, связывающего операцией умножения неизвестную порождающую матрицу кода с некоторыми другими матрицами, не все из которых известны. В докладе И. В. Чижова доказано, что если данная задача решается за полиномиальное время для криптосистемы Мак-Элиса, то за полиномиальное время решается как сама эта задача для криптосистемы Мак-Элиса — Сидельникова, так и каждая такая её подзадача для криптосистемы Мак-Элиса, в ко-

торой вместо порождающей матрицы кода фигурирует её подматрица, полученная из неё вычёркиванием некоторой строки, и наоборот, если каждая из этих подзадач для криптосистемы Мак-Элиса решается за полиномиальное время, то за полиномиальное время решается и сама задача для криптосистемы Мак-Элиса — Сидельникова.

В докладе И. В. Широкова предложена новая модель симметричного шифра на основе некоммутативной алгебры полиномов, представляющей собой кольцо многочленов над некоторым полем, взятое вместе с дополнительной операцией — композицией многочленов: $(f \circ g)(x) = f(g(x))$. Открытыми параметрами шифра являются некоторые различные многочлены $f_1(x), \ldots, f_n(x)$ степени $\geqslant 2$ и неприводимый многочлен $h(x)$; секретным ключом является некоторая подстановка $\sigma \in S_n$. Открытый текст представляется многочленом $m(x)$, шифртекстом будет многочлен $c(x) = (f_{\sigma(n)} \circ \ldots \circ f_{\sigma(1)} \circ m)(x) \bmod h(x)$, вычисляемый по рекуррентной формуле: $c_0(x) = m(x)$; $c_i(x) = (f_{\sigma(i)} \circ c_{i-1})(x) \bmod h(x)$, $i = 1, \ldots, n$; $c(x) = c_n(x)$. Расшифрование заключается в последовательном решении последней системы уравнений относительно $c_{n-1}, \ldots, c_1, c_0$. Приведены аргументы за то, что наиболее быстрый способ определения ключа атакой с известным открытым текстом состоит в переборе всего ключевого пространства.

Влияние выбора ключа шифрования и блоков замены шифра ГОСТ 28147-89 на вид системы булевых функций, представляющих процедуру одного раунда шифрования, исследовано в докладе В. Ю. Золотухина и Т. А. Чалкина. Экспериментально установлено ожидаемое, а именно: показатели нелинейности и лавинного эффекта системы для каждой таблицы замен с изменением ключа могут и улучшаться, и ухудшаться, и оставаться неизменными.

На основе клеточных автоматов построен высокоскоростной генератор псевдослучайной последовательности (В. М. Сухинин). В его составе — два двумерных булевых клеточных автомата размера 37×11 каждый и регистр сдвига длиной 63 с линейной обратной связью. Функция клетки в каждом автомате своя. Окрестность клетки в автомате состоит из 8 соседних клеток. Выходом каждого автомата служит 256-битное состояние подрешётки размера 32×8. Выход регистра в каждый такт работы прибавляется по модулю 2 к состоянию одной из клеток каждого автомата. Выход генератора является побитной суммой по модулю 2 выходов обоих автоматов. Схема генератора на базе ПЛИС (программируемой логической интегральной схемы) Altera Cyclone II работает с частотой 100 МГц и вырабатывает 23,8 Гбит/с. Путём тестирования генератора на наборе тестов NIST подобраны функции ячеек автоматов такими, что последовательность, вырабатываемая генератором, успешно проходит все тесты из набора. Ведётся работа над программной реализацией генератора на базе графического адаптера ПЭВМ.

В докладе А. В. Милошенко предложена программно-аппаратная реализация симметричной шифрсистемы на основе сильносвязного конечного автомата с функцией выхода, биективной в каждом состоянии, получившего название автомата Закревского в честь А. Д. Закревского, предложившего его в 1959 г. на эту роль. Программная часть реализации включает в себя генератор шифрующих автоматов, генератор ключей — подмножеств переходов автомата, программу кодирования состояний автомата и транслятор с его табличного задания в язык описания аппаратуры VHDL. Аппаратная часть шифрсистемы строится на базе ПЛИС, программирование которой осуществляется с помощью САПР Xilinx ISE. Экспериментальное исследование показало, что по скорости работы и по эффективности использования ресурсов ПЛИС предложенная

реализация автоматной шифрсистемы сравнима с реализациями на ПЛИС других известных блочных шифров (TripleDES, IDEA и т. п.).

Последние два доклада в равной мере относятся и к направлению 9 (логическое проектирование дискретных автоматов), к тому его разделу, где речь идёт об аппаратной реализации криптоалгоритмов.

4. Математические методы стеганографии

Метод выбора элементов стегоконтейнера, модифицируемых в процессе встраивания информации, оказывает критическое влияние как на стойкость стегосистемы, так и на её пропускную способность. Строго говоря, задача состоит в таком выборе элементов контейнера для встраивания информации, который позволил бы максимизировать либо стойкость стегосистемы при заданном размере скрываемого сообщения, либо пропускную способность стегосистемы при заданной стойкости.

В докладе О. В. Моденовой проанализированы существующие методы встраивания информации в файлы формата MPEG-2 — модификация коэффициентов дискретного косинусного преобразования, удаление нескольких из них и встраивание на уровне битовых элементов. Дан сравнительный анализ этих методов как по критериям стойкости и пропускной способности, так и по сложности техники встраивания информации.

В докладе Е. В. Разинкова и Р. Х. Латыпова предложен общий метод распределения скрываемого сообщения в произвольном контейнере, позволяющий повысить пропускную способность стегосистемы при заданной стойкости или повысить стойкость стегосистемы при заданной пропускной способности. Контейнер разбивается на m групп элементов с k_i элементами в i-й группе и с областью C_i допустимых значений элементов в ней, $C_i = \{c_1^i, ..., c_{k_i}^i\}$. Предполагается, что модификация одного элемента в i-й группе позволяет встроить q_i бит, $q_i = \lfloor \log_2 |C_i| \rfloor$. Количество модифицируемых элементов в i-й группе обозначается x_i, $\Sigma x_i q_i = n$; функции плотности распределения элементов i-й группы неизменённого контейнера и стегоконтейнера со встроенной информацией обозначаются $f_i(c)$ и $f_i'(c, x_i)$ соответственно, $f_i'(c, x_i) = f_i(c)(k_i - x_i)/k_i + x_i/k_i|C_i|$. Если, кроме того, $P(S)$ и $P'(S)$ суть произведения соответственно $f_i(c_j^i)$ и $f_i'(c_j^i, x_i)$, взятые по всем возможным i и j и представляющие собой вероятности соответственно того, что в качестве контейнера будет выбран объект S, и того, что в результате встраивания информации будет получено стего S, то стойкость стегосистемы оценивается относительной энтропией (расстоянием Кулльбака — Ляйблера) как $D(P||P') = \sum\limits_S P(S)\log_2(P(S)/P'(S))$, а именно: чем меньше $D(P||P')$, тем выше стойкость стегосистемы.

Для защиты от копирования и несанкционированного использования медиаконтента широко применяется одна из разновидностей цифровых водяных знаков — идентификационные номера (ИН): в контейнер с медиаконтентом, предназначенным конкретному пользователю, внедряется персональный ИН, по которому можно определить имя этого пользователя и привлечь его к ответственности в случае, если копии контейнера он будет распространять среди других (нелегальных) пользователей. Противодействовать этой защите можно атакой сговором: несколько легальных пользователей путём сравнения своих контейнеров обнаруживают в них ИН, создают контейнер с тем же медиаконтентом, но с другим, ложным, ИН, отличным от ИН в их контейнерах, и распространяют его среди нелегальных пользователей, возможно, подставляя тем самым (идентифицируя) какого-то другого легального пользователя. Противостоять этой атаке можно, используя ИН из так называемого допустимого множества булевых векто-

ров некоторой длины n; в нём разные подмножества векторов покрываются разными минимальными интервалами булева пространства размерности n, и его мощность k не превосходит n. В докладе Т. М. Соловьёва и Р. И. Черняка продолжены исследования свойств допустимых множеств ИН, найден метод построения всех таких множеств, изучены возможности идентификации участников сговора по их ложному ИН и возможности создания ими ложного ИН, не идентифицирующего никого. Основным аппаратом в этих исследованиях стало представление допустимого множества мощности k булевой матрицей размера $k \times n$ со строками в качестве элементов множества. Перестановка строк и (или) столбцов, удаление повторяющихся столбцов и инверсия столбцов не меняют свойства допустимости представляемого матрицей множества, и матрицы, получаемые одна из другой с помощью этих операций, называются эквивалентными. Так же называются и представляемые ими множества. В каждом классе их эквивалентности есть матрица с единичной подматрицей E_k на первом месте. Допустимое множество называется сильно допустимым, если удаление из его матрицы любого одного столбца влечёт потерю свойства допустимости множества. Матрица такого множества эквивалентна E_k. Для матрицы любого допустимого множества мощности k существует эквивалентная матрица вида $[E_k||A]$, являющаяся конкатенацией E_k и матрицы $A = A_{k\times(n-k)}$ недопустимого множества. Тем самым показано, что все допустимые множества с точностью до эквивалентности строятся конкатенацией E_k с любыми матрицами $A_{k\times(n-k)}$. Показано, что три или более участников сговора всегда могут создать ложный ИН, никого не идентифицирующий. В нём каждая компонента является мажоритарной функцией от компонент соответствующего столбца матрицы допустимого множества ИН. Защита от этой атаки пока не найдена.

В математической проблематике стеганографических исследований важное место занимает задача выявления факта наличия вкраплений в случайных последовательностях. Известно, например, что гарантированно обнаружить факт наличия независимых вкраплений в последовательность, полученную по полиномиальной схеме с известными вероятностями исходов, возможно только в том случае, когда объём вкраплений растёт по порядку быстрее корня от длины исходной последовательности. Аналогичное утверждение справедливо и для последовательности, образующей простую цепь Маркова с известной матрицей переходных вероятностей. В докладе А. М. Шойтова этот результат обобщён на случай простой цепи Маркова с неизвестной матрицей переходных вероятностей.

5. Математические основы компьютерной безопасности

В проблематике этого направления важнейшее место по-прежнему занимают разработка и исследование математических моделей безопасности КС. Поиску tg-путей и островов в графе доступов модели *Take-Grant* посвящён доклад Д. М. Бречки. Пути ищутся алгоритмом Дейкстры в графе, полученном из графа доступов исключением рёбер без прав $Take$ и $Grant$, а острова — с помощью алгоритма Флойда в графе доступов без рёбер, не содержащих прав $Take$ и $Grant$, и без рёбер, вершины которых не являются субъектами. Сложности этих алгоритмов на графах с n вершинами оцениваются как $O(n^2)$ и $O(n^3)$ соответственно, а сложность процедуры исключения из графа «лишних» рёбер — как $O(n^2)$.

На основе ФАС, ФПАС и ФС ДП-моделей разработан проект математической модели электронных почтовых систем — ЭПС ДП-модели (К. А. Грищенко). В ней, кроме всего прочего, отражены клиент-серверная архитектура системы с субъектами-операционными системами, защищённые сущности, не являющиеся субъектами, и дове-

ренные субъекты-задачи, обладающие правами доступа и реализующие доступ к защищённым сущностям и кодирование в них данных. На компьютере-сервере субъекту-операционной системе подчинён в иерархии доверенный субъект-сервер, которому подчинены в иерархии доверенные субъекты-задачи. Субъекту-задаче соответствуют процессы (или их потоки) в операционной системе (ОС), реализующие механизмы доступа клиентов к серверу, маршрутизации почты, репликации баз данных и др. Субъекты, не реализующие доступ к защищённым сущностям, не обладают правами доступа и не могут получать доступ к этим сущностям, но они могут обладать правами доступа или получать доступ к сущностям-образам защищённых сущностей. Недоверенный субъект-задача может создать доверенного субъекта в случае, когда недоверенный субъект реализовал к себе информационные потоки по памяти от всех сущностей, параметрически ассоциированных с некоторым потенциальным доверенным субъектом. ЭПС ДП-модель предназначается для анализа возможности получения недоверенными субъектами ЭПС доступа к защищённым сущностям и реализации в ЭПС от данных сущностей запрещённых информационных потоков.

Установлены необходимые и достаточные условия передачи прав доступа и реализации информационных потоков в базовой ролевой ДП-модели компьютерной системы в случае, когда на траекториях функционирования системы субъект-сессии не получают доступа владения друг к другу с использованием информационных потоков по памяти к функционально ассоциированным с субъект-сессиями сущностям (П. Н. Девянин).

В КС ОС GNU/Linux и СУБД MySQL обнаружены примеры информационных потоков по времени, которые не подпадают под описания в существующих ДП-моделях (М. А. Качанов). Так, в ОС GNU/Linux возможна передача информации от одного процесса другому через количество нитей, которыми оперирует первый процесс, фиксируемое операционной системой в файле, доступном любому процессу. Аналогично, один пользователь БД может передать информацию другому пользователю через количество своих запросов к БД, фиксируемое ядром СУБД в счётчике запросов, доступном любому пользователю. В связи с обнаружением в КС информационных потоков по времени нового типа возникает необходимость отражения их в моделях безопасности компьютерных систем. Это можно сделать, например, развив далее подходящим образом ДП-модели, а именно, введя в них ассоциированные сущности нового вида, указывающие на возможность реализации к ним информационных потоков по времени в зависимости от выполняемых субъектом действий, и соответственно новые правила преобразования состояний, а также сформулировав и обосновав новые необходимые и достаточные условия возможности реализации в КС информационных потоков по времени между сущностями системы.

Структура двухсеместрового курса по дисциплине «Основы построения защищённых вычислительных сетей» предложена в докладе Д. Н. Колегова. Теоретическая часть курса базируется на руководстве Cisco Safe и архитектурах сетевой безопасности Cisco, а практическая (лабораторные работы) — на среде эмуляции Cisco Packet Tracer.

В научной проблематике безопасности компьютерных сетей весьма актуальной представляется задача отслеживания аномальной активности на участке сети (в канале связи, сегменте сети или локальной машине) посредством статистического анализа трафика на этом участке. В докладе О. В. Ниссенбаум и А. С. Присяжнюка предложен адаптивный метод решения этой задачи. В его основу положены следующие соображения. Трафик компьютерной сети достаточно хорошо приближается дважды

стохастическим потоком событий, в частности альтернирующим потоком. Последний характеризуется тройкой параметров (λ, a_1, a_2), которые можно оценивать в реальном времени и представлять точкой в трёхмерном пространстве. Следя за этой точкой, можно сделать вывод о типичности или нетипичности трафика на данном участке сети в любой промежуток времени. В этой части работы используются методы фильтрации и кластерного анализа.

В трёхуровневой компьютерной системе, состоящей из клиента, внешнего сервера и внутреннего сервера и построенной по модели доверенной подсистемы, клиент для взаимодействия с внутренним сервером должен пройти аутентификацию от своего имени перед внешним сервером, после чего внешний сервер должен пройти аутентификацию перед внутренним от имени группы пользователей, к которой принадлежит данный клиент. Возникает задача разработки такой схемы двухуровневой аутентификации, при которой внешний сервер для взаимодействия с внутренним смог бы использовать учётную запись только той группы, к которой принадлежит клиент, и только тогда, когда клиент взаимодействует с ним. Например, если клиент относится к группе «гости», то внешний сервер может пройти аутентификацию перед внутренним только от имени учётной записи «гость» и только при помощи клиента из группы «гости». Парольная схема аутентификации не решает эту задачу: после сеанса связи клиента со скомпрометированным внешним сервером злоумышленник получает возможность обратиться с внешнего сервера к внутреннему от имени учётной записи группы этого клиента. В докладе П. А. Паутова предложено решение этой задачи с помощью схемы аутентификации на основе произвольных коммутативного алгоритма шифрования E и хэш-функции H. В ней каждой учётной записи внутреннего сервера ставится в соответствие некоторое число S, каждому клиенту внешнего сервера — ключ K. На внешнем сервере хранится $E_K(S)$, где S соответствует учётной записи внутреннего сервера для группы клиента — владельца K. При аутентификации клиента выполняется следующий протокол: клиент посылает внешнему серверу своё имя; внешний сервер внутреннему — имя учётной записи группы клиента; внутренний сервер внешнему — случайный ключ K' алгоритма E; внешний сервер клиенту — величину $E'_K(E_K(S))$; клиент внешнему серверу — значение $h = H(D_K(E'_K(E_K(S))))$; внешний внутреннему — значение h; внутренний сервер сравнивает h с $H(E'_K(S))$, и в случае сравнения клиент проходит аутентификацию перед внутренним сервером от имени учётной записи своей группы. В асимметричном варианте алгоритма E каждому клиенту ставится в соответствие пара ключей: открытый K_e, закрытый K_d, на внешнем сервере для каждого клиента хранятся $E_{K_e}(S)$ и K_e.

Внедрение кода в процесс в операционной системе расширяет возможности для исследования, в том числе для обнаружения уязвимостей в ОС, и мотивирует разработку адекватных методов защиты ОС от угроз, сопутствующих этому действию. Методы внедрения кода в процесс в ОС Windows хорошо изучены. В докладе И. В. Смита два таких метода перенесены на ОС GNU/Linux. Условиями для их применения являются наличие прав доступа пользователя ОС, в процесс которого внедряется код, и возможность исполнять системный вызов `ptrace` этим пользователем.

В мире компьютерной безопасности популярны международные соревнования Capture the Flag (CTF), в которых участники — студенты и профессионалы в этой области — соревнуются в умении успешно защищать свои компьютерные сети и атаковать сети соперников. Участвующие в них студенты, аспиранты и молодые специалисты получают богатый опыт практической работы по защите компьютерных систем и огромные моральные стимулы к занятию научными исследованиями в области ком-

пьютерной безопасности и криптографии. Существующие правила этих соревнований время от времени совершенствуются с целью достижения большего эффекта от участия в них. Последнее из усовершенствований их предложено командой SiBears Томского государственного университета. Реализация новых правил требует разработки и нового сервера для управления соревнованиями по ним. В докладе Н. О. Ткаченко и Д. В. Чернова сообщается о разработанном и реализованном ими сервере соревнований CTF по новым правилам. Архитектура сервера построена по шаблону Модель — Представление — Контроллер (Model — View — Controller). Модель предоставляет данные (обычно для Представления) и реагирует на запросы (обычно от Контроллера); Представление отвечает за отображение информации (выступает как пользовательский интерфейс); Контроллер интерпретирует данные пользователя и информирует Модель и Представление о необходимости соответствующей реакции. Модель реализована в виде реляционной базы данных, работа с которой ведётся методом Object Rational Mapping. Для представления пользователю информации о состоянии сервера и для приёма его запросов используется клиент-серверная архитектура: жюри и команды с помощью веб-браузера отправляют запросы веб-серверу, который передаёт их обработчикам, возвращающим результат в формате XTML.

В докладе М. И. Цоя приведены результаты качественного анализа автоматизированного средства Scyther, предназначенного для моделирования криптографических протоколов с целью обнаружения в них уязвимостей со стороны нарушителя. Протокол в нём представляется множеством состояний и правилами перехода между состояниями. Состояния, достижимые из начального, проверяются на удовлетворение условиям безопасности. В отсутствие среди них состояния, в котором эти условия нарушаются, протокол считается безопасным. С помощью этого средства промоделирован протокол взаимной аутентификации сторон SCID3, предположительно уязвимый атакой «человек посередине». Однако результаты моделирования говорят скорее за то, что это не так.

6. Математические основы надежности вычислительных и управляющих систем

Надёжность программных и аппаратных средств вычислительных и управляющих систем рассматривается как один из показателей их безопасности. Традиционно это направление на школе-семинаре пользуется заслуженным вниманием и интересом. На этот раз оно представлено работами по синтезу отказоустойчивых и самодиагностируемых систем.

В качестве одной из моделей отказоустойчивой системы часто фигурирует рёберное или вершинное расширение определённой кратности k графа системы G, представляющее собой граф со свойством: удаление из него любых k рёбер или вершин соответственно, вызванное отказами в системе, приводит к графу H, в который вкладывается граф G. В случае $H \simeq G$ расширение называется точным. В докладе М. Б. Абросимова описаны все минимальные рёберные k-расширения всех направленных звёзд при любом $k \geqslant 1$, а доклад М. Б. Абросимова и Д. Д. Комарова посвящён построению и описанию минимальных вершинных 1-расширений сверхстройных деревьев. Каждое такое дерево является объединением некоторого числа t цепей с общей концевой вершиной. Показано, в частности, что число дополнительных рёбер минимального вершинного 1-расширения сверхстройного дерева не меньше $t + 1$ и что при $t > 3$ сверхстройное дерево, являющееся объединением цепей длины не больше 2, среди которых есть цепь длины 1 и цепь длины 2, имеет в точности 2 неизоморфных вершинных 1-расширения.

На данный момент известны турниры, являющиеся точными вершинными расширениями диграфов. В докладе А. А. Долгова построено семейство турниров, которые являются точными вершинными 1- и 2-расширениями турниров же.

В связи с проблемой синтеза отказоустойчивых систем возникает задача порождения графов с соответствующими свойствами. В докладе В. А. Мелентьева предложен аналитический подход к её решению применительно к регулярным графам заданного порядка и заданной степени. Подход основан на представлении графа его проекциями, описываемыми в аналитической форме и содержащими всю информацию о структуре и количественных характеристиках графа. Процесс синтеза состоит в построении базовой проекции остовного дерева с последующим доопределением неизвестных рёбер в соответствии с требуемыми структурой и значениями характеристик синтезируемого графа.

В докладе Ю. К. Димитриева и А. Ф. Задорожного рассмотрена задача самодиагностирования модулярных вычислительных систем в присутствии кратных неисправностей с использованием ненадёжных тестов. Зависимость эффективности самодиагностирования от свойств последних изучена методом имитационно-статистического моделирования. Проведено сравнение эффективности самодиагностирования с использованием ненадёжных тестов, соответствующих известной PMC-модели, и ненадёжных тестов, предложенных авторами, и найдены условия, при которых авторские тесты обеспечивают более высокую эффективность.

7. Математические основы информатики и программирования

Развитие математических основ информатики и программирования рассматривается как одно из необходимых условий успешного решения научных и практических проблем компьютерной безопасности и криптографии.

В сегодняшней программной инженерии выделены пять сложностных классов алгоритмов, определяемых в терминах O-большое и o-малое, — субполиномиальные, полиномиальные, субэкспоненциальные, экспоненциальные и гиперэкспоненциальные алгоритмы. Распознавание класса конкретного алгоритма непосредственно по определению часто сопряжено с трудностями вычислительного характера. В докладе В. В. Быковой в качестве меры вычислительной сложности алгоритма взята эластичность его функции $t(n)$ временной сложности, представляющая собой коэффициент пропорциональности между темпами роста величин $t(n)$ и n, и перечисленные классы функций охарактеризованы в терминах этой меры. Свойства эластичности позволяют без особого труда находить эластичность для широкого спектра алгоритмов и распознавать их сложностной класс. В их числе и многие теоретико-числовые алгоритмы, применяемые в криптографии. Предложена также схема сравнения алгоритмов по асимптотическому поведению их эластичности.

Проблема тестирования программного обеспечения (ПО) становится всё более актуальной, в том числе и в связи с компьютерной безопасностью, что неизменно подтверждается растущим интересом к ней со стороны участников школы-семинара Sibecrypt.

Важными свойствами любой программы являются её надёжность и безопасность. Первая означает способность программы работать без причинения вреда окружению, вторая — её устойчивость к внешнему воздействию, которое может нарушить работу программы. В докладе В. В. Горелова сообщено о системе обнаружения (в процессе отладки) действий или бездействий программы при её работе с ресурсами, нежелательных с точки зрения надёжности и безопасности и классифицируемых как ошиб-

ки, или дефекты программы. В их числе: утечки ресурсов, использование ресурсов после их освобождения, повторные освобождения ресурсов, использование неинициализированных ресурсов без их предварительного захвата, использование ресурсов за их границами (относится к динамической памяти и адресному пространству), нарушение вызываемого механизма захвата и освобождения ресурса (функция захвата возвращает идентификатор ранее захваченного и ещё не освобождённого ресурса) и др. Система включает в себя язык описания ресурсов и функций для работы с ними, программу-преобразователь, которая по описанию ресурсов создаёт код для перехвата функций, работающих с интересующими ресурсами, и программу-анализатор, которая считывает соответствующие события, возникающие в процессе работы отлаживаемой программы, и выводит обнаруженные опасные участки программы для анализа человеком. Система реализована для прикладных программ на языке Си под ОС POSIX и WINDOWS.

В тестировании функциональности ПО на первый план выходит задача разработки такого средства порождения тестов, которое обеспечивало бы создание некорректных данных для тестируемого (целевого) ПО, максимально возможную независимость генератора тестов от целевого ПО, минимальное время построения тестов для нового целевого ПО, достаточно высокий объём покрытия кода целевого ПО. В докладе А. Н. Макарова исследована возможность создания генератора тестов с использованием скриптового языка описания структур исходных данных и процедур их формирования. Выяснена недостаточная выразительность этого языка для описания тестов со сложноструктурированными данными. Предложено расширение его средствами описания дополнительной декларативной информации о внутренних связях, ограничениях и зависимостях в данных, позволяющими автоматически генерировать исходные данные с нарушениями этих связей, ограничений и т. п.

В аналитической теории кс-языков известно, что существуют аффинные кс-языки, коммутативные образы которых являются диагоналями коммутативных образов линейных языков с одним дополнительным символом. В докладе К. В. Сафонова и Д. А. Калугина-Балашова сформулированы новые условия, при которых система уравнений Хомского — Щютценберже определяет кс-язык с тем же свойством.

В настоящее время в анализе криптографических систем значительную роль играют методы решения систем уравнений над конечным полем, в частности над полем GF(2) — булевых уравнений. Для их применения криптоаналитик должен иметь перед собой систему уравнений анализируемого криптоалгоритма, представленную в определённой форме — дизъюнктивной, полиномиальной и т. п. Автоматизированная система представления алгоритмов дискретной математики в виде систем булевых уравнений — Transalg доложена в сообщении И. В. Отпущенникова и А. А. Семёнова. Она включает в себя С-подобный язык описания алгоритмов, транслятор с него в язык булевых уравнений и средства приведения последних к нормальным формам разного вида.

Один из методов защиты КС обработки информации заключается в интеграции её с модулем политики безопасности (ПБ). Возможность такой интеграции без изменения кода КС обеспечивается средствами аспектно-ориентированного программирования (АОП). Для их представления используются языки АОП, один из которых — AspectTalk — разработан специально для целей интеграции КС и ПБ. Для доказательства полноты его выразительных средств в докладе Д. А. Стефанцова и А. Е. Крюковой формально доказана семантическая эквивалентность ядра языка AspectTalk и языка объектно-ориентированного программирования Smalltalk. Сделано

это путём доказательства коммутативности диаграммы гомоморфизмов между множествами синтаксических областей и доменов этих языков. Тем самым доказана возможность автоматической трансляции программ с языка AspectTalk в язык Smalltalk и обратно.

8. Вычислительные методы в дискретной математике

Это направление исследований по-прежнему стимулируется потребностями криптоанализа и синтеза стойких криптоалгоритмов.

В докладе Д. В. Беспалова, В. Г. Булавинцева и А. А. Семёнова исследованы возможности графических ускорителей (GPU) в криптоанализе шифров DES и A5/1 атакой грубой силы и показано вполне ожидаемое — их бесперспективность в этой роли.

В соответствии с теорией К. Шеннона сочетание линейных и нелинейных преобразований в операциях шифрования способствует стойкости шифров ко многим атакам. Для эффективной их реализации в блочных шифрах часто длину n блока представляют как $n = m{\cdot}n' = k{\cdot}m'{\cdot}n'$, а в качестве линейного преобразования блока $x = x_1x_2\ldots x_m$ с $|x_i| = n'$, $i = 1,\ldots,m$, берут композицию $A(P(x_1)P(x_2)\ldots P(x_m))$, где P — перестановка в подблоках длины n', $A = \operatorname{diag}(A_1, A_2, \ldots, A_k)$, $A_j \in \mathrm{GL}(m'\cdot n', 2)$, $j = 1,\ldots,k$. В докладе А. А. Дмуха показано, что наилучшие с точки зрения скорости шифрования и количества тактов процессора, необходимых для обработки одного байта информации, значения параметров $m' \in \{2, 4, 8, 16\}$ и $k' \in \{2, 3, \ldots, 8\}$, полученные экспериментально при $n' = 8$ и сопоставимом по криптографическим характеристикам числе итераций, следующие: $m' = k = 2$, $m' = k = 4$, $m' = k = 8$ при длине блока $n = 32, 128, 512$ соответственно. С этими значениями скорость шифрования в 2,5 – 1,3 раза выше, чем с другими значениями.

Решение задачи криптоанализа нередко состоит в определении значения ключа методом опробования возможных значений до тех пор, пока не будет получено истинное значение. Значения ключа часто неравновероятны, и тогда можно осуществить их направленный перебор, начав с наиболее вероятных. Трудоёмкость такого перебора определяется как математическое ожидание длины перебора $m = \sum\limits_{j=1}^{H} q_j \cdot j$, где H — количество различных значений ключа, q_j — вероятность его j-го значения и $q_1 \geqslant q_2 \geqslant \ldots \geqslant q_H$. При слишком большом H вычисление по этой формуле практически неосуществимо. В докладе И. В. Панкратова и О. А. Теплоуховой предложен следующий метод перебора значений ключа с параметром $n \geqslant 1$: ключевое пространство разбивается на два равномощных подмножества мощности $h = H/2$, сначала опробуются первые n элементов первого подмножества, затем по очереди — оставшиеся элементы первого подмножества и $(h - n)$ элементов второго и наконец — остаток второго подмножества. Построена рекуррентная формула для математического ожидания $m_0(n)$ длины перебора этим методом, которая служит верхней оценкой для искомого m. Варьируя в ней параметр n, можно достичь наименьшего значения $m_0(n)$. Практические исследования показывают, что это значение отличается от истинного не более чем на 17 %.

В докладе Р. Т. Файзуллина задачи существования в графе гамильтонова цикла и существования изоморфизма двух графов сводятся к поиску глобального минимума некоторых функционалов и предложены алгоритмы минимизации последних.

9. Прикладная теория автоматов, графов и кодов

Свойства минимальных детерминированных конечных автоматов, распознающих префиксный код заданной мощности n, представлены в докладе И. Р. Акишева и М. Э. Дворкина. Показано, что задача синтеза такого автомата равносильна задаче построения кратчайшей аддитивной цепочки чисел, заканчивающейся числом n. Последняя задача хорошо известна в дискретной математике. К её решению сводится задача об оптимальном алгоритме возведения числа в заданную степень, представляющая интерес для современной криптографии с открытым ключом.

Упорядоченное множество, элементами которого служат классы отношения σ взаимной достижимости состояний автомата A, а отношением порядка — отношение обратной достижимости, называется каркасом этого автомата. Доклад В. Н. Салия посвящён изучению свойств каркаса, связанных с такими алгебраическими понятиями для автомата, как «подавтомат», «гомоморфизм», «конгруэнция». Доказано, в частности, что: 1) каждое конечное упорядоченное множество изоморфно каркасу некоторого автомата с двумя входными символами; 2) конечное упорядоченное множество тогда и только тогда изоморфно каркасу автономного автомата, когда у каждого его элемента есть не более одного нижнего соседа; 3) решётки подавтоматов двух автоматов изоморфны, если и только если изоморфны каркасы этих автоматов; 4) для автоматов с изоморфными каркасами вложение одного автомата в другой является изоморфизмом автоматов; 5) каркас фактор-автомата автомата A по некоторой конгруэнции θ тогда и только тогда изоморфен каркасу самого автомата, когда $\theta \subseteq \sigma$.

В связи с применением конечных автоматов в криптографии возникает задача построения автоматов с поведением, изменяемым по параметру, задаваемому извне и играющему роль ключа шифра. Проблемы нет, если в этой роли выступает начальное состояние автомата, и совсем другое дело, когда ключевой информацией является, например, подмножество переходов в автомате. В докладе В. Н. Тренькаева предложено решение этой задачи в виде композиции двух автоматов с общими множествами входных символов и состояний и блока управления, вырабатывающего управляющий символ в зависимости от ключа, общего состояния и общего входного символа автоматов. Управляющий символ со значениями, поставленными во взаимнооднозначное соответствие автоматам, в каждый такт работы вызывает считывание состояния в общую память и выходного символа с того из автоматов, который соответствует значению управляющего символа в этот момент. Допускается, что функции переходов и выходов автоматов также могут зависеть от ключа.

И. А. Бадеха и П. В. Ролдугин доказали справедливость следующих соотношений между степенью Δ и плотностью ρ в любом связном регулярном графе G, в котором каждое ребро лежит не менее чем в двух максимальных кликах и нет двух смежных вершин с одинаковыми шарами с центрами в них радиуса 1: 1) $\rho \leqslant \Delta - 1$; 2) если $\rho = \Delta - 1$, то $\Delta = 4$ и G изоморфен графу B, состоящему из цикла длины 4 и двух несмежных вершин, смежных каждой вершине в цикле; 3) если $\rho = \Delta - 2$, то либо в G есть две вершины степени Δ, либо G получается из B добавлением доминирующей вершины.

В докладе А. В. Пролубникова предложен алгебраический полный инвариант ациклических графов, который получается не путём канонизации графа, как это обычно делается, а представляет собой множество (для графа с n вершинами) из $1+n(n+1)/2$ числовых значений, каждое из которых есть произведение собственных значений из спектра графа и спектров его подграфов.

Задача восстановления графа обходом его «в глубину» рассмотрена в докладе Е. А. Татаринова. Указаны два класса графов, для которых верхняя оценка временной сложности восстановления является линейной функцией, — класс деревьев и класс колец. Указаны три операции над графами, которые не ухудшают верхнюю оценку временной сложности восстановления графа, — добавление висячей вершины, добавление вершины в ребро и соединение двух графов через вершину сочленения.

В связи с потребностями стандарта цифровой сотовой связи CDMA возникает задача построения линейных кодов с векторами значений бент-функций в качестве кодовых слов. Известные такие коды, построенные на основе бент-функций из класса Мак-Фарланда, обладают следующими параметрами: длина кода $m = 2^n$, размерность кода $k = 2^{n/2} + n/2$ и кодовое расстояние $d = 2^{n/2}$. Например, при $n = 6, 8$ эти параметры для них имеют значения (26, 11, 8), (28, 20, 16) соответственно. В докладе А. В. Павлова предложен алгоритм построения максимальных линейных кодов на основе любых бент-функций, доставляющий коды с $m = 2^n$ и $d = 2^{n/2}$, среди которых есть коды с $n = 6$ и $k = 15$, с $n = 8$ и $k = 30$. В основе алгоритма лежит утверждение о том, что две бент-функции от n переменных тогда и только тогда находятся на минимальном расстоянии $2^{n/2}$ друг от друга, когда они отличаются на аффинном подпространстве размерности $n/2$ и обе на нём аффинны.

10. Математические основы интеллектуальных систем

В криптографии и компьютерной безопасности есть много задач, в решении которых возможно, а иногда просто необходимо применение интеллектуальных систем. Это и принятие решения в условиях неполной, искажённой или неформализуемой информации, и распознавание текстов и сетевого трафика, идентификация источника информации и обнаружение в последовательностях скрытых вложений или свойств, понимание естественного языка и многое другое. К сожалению, пока нельзя сказать, что математическая теория интеллектуальных систем имеет ощутимое представительство в этом направлении. На школе-семинаре Sibecrypt'10 она представлена двумя докладами, имеющими дело с идентификацией состояний динамических объектов (С. И. Колесникова и А. А. Белоус) и логическим выводом решений в классификации объектов (А. Е. Янковская и А. И. Гедике). В первом докладе предложены новые алгоритмы формирования характеристических признаков как системы обобщённых эталонов, на основе которых возможны распознавание состояний динамического объекта (ДО), сглаживание временного ряда и идентификация тренда фрагмента временного ряда, соотнесённого с состоянием ДО. Во втором докладе представлен алгоритм распознавания принадлежности объекта образу с использованием смешанных (условных и безусловных) диагностических тестов (СДТ), в котором решение принимается одновременно с построением СДТ, сокращая тем самым вычислительные затраты.

ЛИТЕРАТУРА

1. Тезисы докладов IX Сибирской научной школы-семинара с международным участием «Компьютерная безопасность и криптография» — Sibecrypt'10 (Тюмень, ТюмГУ, 7–10 сентября 2010 г.) // Прикладная дискретная математика. Приложение. 2010. № 3. 120 с.