МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

УДК 519.7

50 ЛЕТ КРИПТОГРАФИИ В ТОМСКОМ ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ

Г. П. Агибалов

Томский государственный университет, г. Томск, Россия

E-mail: agibalov@isc.tsu.ru

Реферативный обзор результатов криптографических исследований научной школы прикладной дискретной математики Томского государственного университета за последние 50 лет.

Ключевые слова: *криптография, криптоанализ, поточные шифры, генераторы ключевого потока, нормальные рекуррентные последовательности, блочные шифры, дифференциальный криптоанализ, схемы разделения секрета, конечные автоматы, булевы функции с криптографическими свойствами, теоретико-числовые алгоритмы в криптографии, уравнения над конечным полем, криптографические протоколы, цифровые деньги.*

Введение

В 50-летней истории криптографии в Томском государственном университете (ТГУ) можно выделить три периода, назвав их условно военным, переходным и гражданским.

В первый период (1960-е годы) исследования по криптографии в ТГУ проводились по заказу оборонного предприятия и носили закрытый характер. Они велись, что называется, «с чистого листа», в отсутствие какой-либо литературы по этому предмету, опираясь в основном на собственные представления задач криптографии и волю заказчика. В значительной степени это были наивные исследования, но в их процессе было уяснено главное: создание стойких криптосистем, говоря современным языком, невозможно без их тщательного криптоанализа. Именно алгоритмы криптоанализа некоторых поточных шифров и полученные с их помощью оценки стойкости последних и стали основными достижениями наших исследований этого периода. Именно таким путём мы доказали тогда непригодность линейных автономных автоматов в качестве генераторов ключевого потока. Некоторые результаты тех исследований, в частности относящиеся к генераторам нормальных рекуррентных последовательностей и к автоматным генераторам ключевого потока с функцией выхода в качестве ключа, до сих пор не превзойдены и по-прежнему актуальны.

На исходе этого периода нами был проявлен интерес и к теории кодирования как к средству для создания кодовых систем шифрования. Впервые в мировой науке мы разработали пакет программ (на алгоритмическом языке ЛЯПАС) для решения алгоритмических задач теории кодирования [1, 5], но так случилось, что наши исследования кодовых шифрсистем были отложены на целых 30 лет.

Второй период развития криптографии в ТГУ (1970 – 1980-е годы) был периодом осмысления полученных результатов, их легализации и обобщения в рамках теории

экспериментов с автоматами [16] и приобщения к ним студентов. С позиций чистой криптографии это был «вялотекущий» период, протекавший в отсутствие заказчика и стимулов с его стороны, но в этот период нами была разработана применяемая и ныне технология решения комбинаторно-логических задач [15], каковыми собственно и являются задачи анализа и синтеза криптоалгоритмов, а также была развита теория декомпозиции конечных автоматов [17] — одного из инструментов создания современных конечно-автоматных криптосистем с открытым ключом. Монография [17] остаётся до сих пор единственной отечественной книгой по декомпозиции автоматов.

Третий период развития криптографии в ТГУ (с 1990-х годов) связан с известными переменами в стране и с появлением возможности проведения открытых теоретических и экспериментальных исследований в этой области. Нельзя сказать, что в теоретическом плане наши исследования этого периода значительно более глубокие, чем прежние, но они охватывают практически всю проблематику современной «гражданской криптографии».

В предлагаемой вниманию работе в реферативной форме обозреваются основные криптографические результаты, полученные научной школой прикладной дискретной математики ТГУ в каждом из указанных периодов. Учитывая характер и предназначение данной публикации, в ней библиография приводится в хронологическом порядке, а материал даётся с разбивкой по направлениям исследований.

1. Наша «военная» криптография

1.1. Шифрующие автоматы А. Д. Закревского

В научной школе прикладной дискретной математики ТГУ криптографические исследования занимают важное место на протяжении всех 50-ти лет её существования. Впервые автор этой статьи прочитал научную работу по криптографии ещё в 1960 году, будучи студентом 4 курса университета. Это была рукопись статьи основателя школы, моего научного руководителя Аркадия Дмитриевича Закревского, посвящённая применению конечных автоматов для шифрования с закрытым ключом. В ней для этой цели был предложен класс автоматов, называемых ныне *шифрующими*, в которых функция выходов биективна в каждом состоянии. К сожалению, А. Д. Закревский не принадлежит к числу тех, кому в ту пору было позволено заниматься криптографией, и его рукопись никогда не была опубликована под тем предлогом, высказанным «чёрным» рецензентом, что её результаты «совершенно секретны». Для восстановления исторической справедливости мы впервые публикуем её в этом номере без каких-либо купюр и редакторской правки (см. [57]).

1.2. Криптоанализ линейного автономного автомата

Тремя годами позже мне, уже аспиранту, было предложено участвовать в выполнении закрытого хоздоговора для предприятия,известного ныне как ЦКБ «Алмаз», по которому, с подачи А. Д. Закревского, мне предстояло исследовать класс шифров, в открытой отечественной литературе известных теперь как шифры гаммирования и входящих в класс современных поточных шифров. Как потом выяснилось, аналогичный договор заказчик уже имел с МВТУ им. Н. Э. Баумана, в котором в качестве генератора гаммы (ключевого потока) предлагалось использовать двоичный регистр сдвига с линейной обратной связью максимального периода (LFSR). В первом же нашем отчёте заказчику было показано, что такой генератор не обладает никакой стойкостью к криптоанализу. Более того, мы показали, что столь же слабым генератором гаммы является всякий инициальный линейный автономный автомат над любым конечным

полем, а именно: любой такой автомат с размерностью состояния n эквивалентен LFSR длины n и восстанавливается (с точностью до эквивалентности) по отрезку его выходной последовательности длиной не более $2n$.

Конечный инициальный линейный автономный автомат над полем $F = GF(q)$ задается пятеркой объектов $L = (S, Z, A, B, s_0)$, где $S = F^n$ и $Z = F^m$ для некоторых натуральных n и m суть множества соответственно состояний и выходных символов автомата, A и B — его матрицы переходов и выходов размеров $n \times n$ и $n \times m$ соответственно с элементами в F и $s_0 \in S$ — начальное состояние автомата. Число n называется размерностью автомата L. Он порождает последовательность выходных символов $z = z_0 z_1 \ldots$, где для любого целого $t \geqslant 0$ символ z_t вычисляется по правилам: $z_t = s_t B$ и $s_{t+1} = s_t A$. В его применении в роли генератора гаммы ключ шифра составляют матрицы A, B и начальное состояние s_0, а гамму — последовательность z. В его криптоанализе предполагается известной верхняя граница N для размерности n. Целью криптоанализа является раскрытие алгоритма генерации гаммы, а именно: с известным N и неизвестными A, B и s_0 требуется построить (если возможно) некий алгоритм, который точно воспроизводит весь ключевой поток z по заданному конечному его отрезку $z_0 z_1 \ldots z_{l-1}$. Ниже показывается, как такой алгоритм можно построить, если $l \geqslant 2N$.

В самом деле, в последовательности состояний $s_0 s_1 \ldots$, где $s_{t+1} = s_t A$ для $t \geqslant 0$, вектор s_N является линейной комбинацией векторов s_0, s_1, …, s_{N-1}, т. е. $s_N = \sum_{j=0}^{N-1} c_j s_j$ для некоторых $c_0, \ldots, c_{N-1}$ в F. После умножения последнего равенства на A^i для каждого $i \geqslant 0$ получим $s_{N+i} = \sum_{j=0}^{N-1} c_j s_{i+j}$ для всех $i \geqslant 0$. После умножения, в свою очередь, этих равенств на B получим рекуррентные соотношения $z_{N+i} = \sum_{j=0}^{N-1} c_j z_{i+j}$ для $i \geqslant 0$. Решая систему первых N из них, т. е. для $i = 0, 1, \ldots, N-1$, относительно неизвестных c_0, …, c_{N-1}, получаем алгоритм вычисления из начального отрезка $z_0 z_1 \ldots z_{N-1}$ последовательности z остальных ее членов z_{N+i}, $i \geqslant 0$, по рекуррентной формуле $z_{N+i} = \sum_{j=0}^{N-1} c_j z_{i+j}$.

Это был 1964 год. Начались поиски стойких генераторов ключевого потока в классе нелинейных автономных автоматов. Так мы вышли на автоматные генераторы с функцией выхода в качестве ключа и на генераторы нормальных рекуррентных последовательностей (НРП) — регистры сдвига с нелинейной обратной связью максимального периода. Для них мы разработали оптимальные алгоритмы криптоанализа и получили экспериментальные оценки их теоретической стойкости, или расстояния единственности — наименьшей длины отрезка последовательности на выходе генератора, достаточной для восстановления его ключа. Оптимальность алгортма как раз и означает тот факт, что он находит ключ генератора по отрезку ключевого потока длиной, равной расстоянию единственности.

1.3. Криптоанализ автоматного генератора с ключевой функцией выхода

Генератор ключевого потока, который мы здесь рассматриваем, представляет собой произвольный инициальный конечный автономный автомат $G = (Q, Z, f, g, q(0))$ с множеством состояний $Q = \{0,1\}^n$, множеством выходных символов $Z = \{0,1\}$, с начальным состоянием $q(0)$, функцией переходов $f\colon Q \to Q$ и функцией выходов $g\colon Q \to Z$, зависящей существенно от k переменных для некоторого $k \leqslant n$. Последнее означает, что существуют функция $h\colon \{0,1\}^k \to Z$ и натуральные $i_1 < i_2 < \cdots < i_k$ в $\{1, 2, \ldots, n\}$, такие, что $g(q_1, q_2, \ldots, q_n) = h(q_{i_1}, q_{i_2}, \ldots, q_{i_k})$ для всех наборов $(q_1 q_2 \ldots q_n) \in Q$; в этом случае i_1, i_2, …, i_k суть номера существенных переменных функции g. Предполагает-

ся, что ключом генератора G служит его функция g. Это значит, что криптоаналитику известны все атрибуты в G, кроме g. Ключевой поток $z = z_0 z_1 \dots$ на выходе G вычисляется по следующим рекуррентным уравнениям: $z_i = g(q(i))$, $q(i+1) = f(q(i))$, $i \geqslant 0$. Он является периодической последовательностью с периодом не больше 2^n. Задача криптоанализа генератора G заключается в определении его ключа по отрезку $z_0 z_1 \dots z_{l-1}$ его ключевого потока. Наименьшее l, при котором это возможно, называется теоретической стойкостью генератора G. Предполагается, что длина l отрезка ключевого потока в задаче криптоанализа не превышает периода всего потока, так как иначе надобности в решении этой задачи не возникает.

Предложены два алгоритма решения задачи его криптоанализа: один, называемый далее A, — в предположении, что криптоаналитику, кроме прочего, известно еще и число k существенных аргументов искомой ключевой функции g, и другой, называемый далее B, — в предположении, что криптоаналитик знает не k, но верхнюю границу k_0 для него.

Оба алгоритма построены по следующей общей схеме.

На вход алгоритма символ за символом поступает ключевой поток с генератора G. После поступления символа z_0 алгоритм располагает начальным состоянием $q(0)$ и значением $z_0 = g(q(0))$ искомой ключевой функции g на нем. В момент поступления очередного символа z_i для $i \geqslant 1$ алгоритм уже имеет состояния $q(j)$ генератора и значения $z_j = g(q(j))$ функции g на них для $j = 0, 1, \dots, i-1$, вычисляет очередное состояние $q(i)$ генератора, получает значение $z_i = g(q(i))$ функции g на нем, строит множество M покомпонентных разностей $q(r) \oplus q(s)$ для всех таких векторов $q(r)$, $q(s)$ в $\{q(0), q(1), \dots, q(i)\}$, для которых $z_r \neq z_s$, и отбирает в M подмножество $\inf M$ всех минимальных по порядку $\leqslant$ векторов. Далее действия алгоритмов A и B расходятся.

В алгоритме A выясняется, единственно ли покрытие из k столбцов матрицы $||\inf M||$, строками в которой являются все векторы в $\inf M$, и если — нет, то наблюдается очередной символ ключевого потока. Это продолжается до тех пор, пока не будет получена матрица $||\inf M||$ с единственным покрытием (строк столбцами) мощности k. Номера столбцов последнего являются номерами существенных аргументов функции g.

В алгоритме B, в отличие от A, ключевой поток наблюдается до той поры, пока не выполнится условие единственности: все покрытия (строк) не более k_0 столбцами матрицы $||\inf M||$ образуют звезду, т. е. имеют общее пересечение — ядро; в этом случае номера столбцов в последнем являются номерами существенных аргументов функции g.

С нахождением существенных аргументов ключевой функции g оба алгоритма делают одно и то же следующим образом. Пусть к этому моменту в алгоритм поступил отрезок ключевого потока длиной m. Тогда находится наименьшее $l \geqslant m$, такое, что в наборах $q(0)$, $q(1)$, …, $q(l-1)$ содержатся все наборы значений существенных переменных функции g, после чего равная ей функция h на произвольном наборе значений ее существенных переменных определяется как $h(q_{i_1}, q_{i_2}, \dots, q_{i_k}) = z_j$, где j находится из условий $0 \leqslant j \leqslant l-1$ и $q(j) = q_1 q_2 \dots q_n$.

В отсутствие у генератора эквивалентных ключей условие единственности, проверяемое при нахождении существенных переменных ключевой функции, и правило выбора l после их нахождения гарантируют оптимальность данных алгоритмов. Их испытания на компьютере и экспериментальные оценки теоретической стойкости самого генератора убедили заказчика в возможности применения этого генератора в его целях.

1.4. Криптоанализ генератора нормальной рекуррентной последовательности

В рамках договора с ЦКБ «Алмаз» были разработаны также оптимальный алгоритм криптоанализа генератора НРП и алгоритм вычисления его теоретической стойкости. Эти исследования базировались на классической работе Н. М. Коробова по нормальным периодическим системам (Изв. АН СССР, сер. матем. 1951. Т. 15. №1. С. 17–46).

Для натуральных $k \geqslant 2$ и $n \geqslant 1$ *нормальная рекуррентная последовательность* значности k и порядка n, или сокращённо *НРП*(k, n), — это такая последовательность $s = s_0 s_1 ...$, в которой $s_i \in E = \{0, 1, \ldots, k-1\}$ для каждого $i \geqslant 0$ и $\{s_i s_{i+1} \ldots s_{i+n-1} \colon i = 0, 1, \ldots, k^n - 1\} = E^n$. Она периодическая с периодом k^n и обозначается как $< s_0 s_1 \ldots s_{k^n-1} >$. Функция $f \colon E^n \to E$, определяемая равенствами $f(s_i s_{i+1} \ldots s_{i+n-1}) = s_{i+n}$ для $i = 0, 1, \ldots, k^n - 1$, называется её *генератором*. При заданном начальном состоянии $s_0 s_1 \ldots s_{n-1}$ генератор f порождает НРП(k, n) s как решение системы рекуррентных уравнений $s_{i+n} = f(s_i s_{i+1} \ldots s_{i+n-1})$, $i \geqslant 0$. В случае $k = 2$ генератор f любой НРП(k, n) представляется в виде $f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus g(x_1, \ldots, x_{n-1})$, где функция $g(x_1, \ldots, x_{n-1}) = f(0, x_1, \ldots, x_{n-1})$ называется *порождающей функцией* этой последовательности.

Для начального отрезка $s^* = s_0 s_1 \ldots s_{l-1}$ некоторой НРП(k, n) s, имеющего длину l в границах $n < l < k^n$, определяется *область запрета* как подмножество всех слов $a_1 a_2 \ldots a_n$ в E^n, в которых a_n есть символ в s^*, примыкающий справа к слову $a_1 a_2 \ldots a_{n-1}$, когда оно в $s*$ встречается t-й раз, считая слева направо, и $1 \leqslant t < k$.

Подмножество из $q = k^{n-1} - 1$ слов в E^n

$$\delta_{i1}\delta_{i2} \ldots \delta_{in} \ (i = 1, 2, \ldots, q) \tag{1}$$

называется *особой системой*, если все слова $\delta_{12}\delta_{13} \ldots \delta_{1n}$, $\delta_{i1}\delta_{i2} \ldots \delta_{in-1}$ $(i = 1, 2, \ldots, q)$ различны, и возможно такое упорядочение слов в ней, при котором для любого $j \geqslant 2$ слово $\delta_{j2}\delta_{j3} \ldots \delta_{jn}$ совпадает с одним из слов $\delta_{12}\delta_{13} \ldots \delta_{1n}$, $\delta_{i1}\delta_{i2} \ldots \delta_{in-1}$ $(i = 1, 2, \ldots, j-1)$. Особая система (1) называется *соответствующей отрезку* s^*, если $\delta_{11}\delta_{12} \ldots \delta_{1n} = \delta_{11} s_0 s_1 \ldots s_{n-2}$ и её пересечение с областью запрета для s^* пустое.

Доказана теорема, согласно которой с отрезка s^* начинается единственная НРП(k, n), если и только если единственна особая система, соответствующая этому отрезку, и любое слово из E^{n-1} по крайней мере $(k-2)$ раз содержится среди слов $s_{i+1} s_{i+2} \ldots s_{i+n-1}$ для $i = 0, 1, \ldots, l-n$.

Доказано также, что все НРП(k, n), начинающиеся с отрезка s^*, и только их, можно построить следующим методом.

Метод A_3. Выбираем произвольную особую систему (1), соответствующую отрезку s^*. Первые l знаков последовательности выписываем совпадающими соответственно со знаками данного отрезка. Выписывание остальных знаков, начиная с $(l+1)$-го, производим по следующему индуктивному правилу: пусть уже выписаны $l + j$ знаков

$$s_0 s_1 \ldots s_{l+j-1}, \tag{2}$$

$j \geqslant 0$; выбираем такой знак $s_{l+j} \in E$, что слово $s_{l+j-n+1} s_{l+j-n+2} \ldots s_{l+j}$ не встречается в последовательности (2) и совпадает с одним из слов выбранной особой системы лишь в случае, если все остальные слова вида $s_{l+j-n+1} s_{l+j-n+2} \ldots s_{l+j-1} z$, где $z \neq s_{l+j}$, в (2) уже встречаются, и приписываем его справа к (2). Построение заканчивается с

получением последовательности длиной k^n. Это будет периодическая часть некоторой НРП(k, n).

Необходимые для метода A_3 особые системы, соответствующие отрезку s^*, строятся следующим методом.

Метод B_1. В первой строке выписываем любое слово $\delta_{11}\delta_{12}\dots\delta_{1n} = \delta_{11}s_0s_1\dots s_{n-2}$, не все знаки которого одинаковы и которое не принадлежит области запрета для s^*. Все остальные строки, начиная со второй, строим по следующему индуктивному правилу. Пусть уже выписаны $j-1$ строк $\delta_{i1}\delta_{i2}\dots\delta_{in}$ $(i = 1, 2, \dots, j-1)$ для $j \geqslant 2$. Тогда в j-й строке выписываем любое такое слово $\delta_{j1}\delta_{j2}\dots\delta_{jn} \in E^n$, не принадлежащее области запрета для s^*, для которого слово $\delta_{j1}\delta_{j2}\dots\delta_{jn-1}$ отлично от каждого из слов $\delta_{12}\delta_{13}\dots\delta_{1n}$, $\delta_{i1}\delta_{i2}\dots\delta_{in-1}$ $(i = 1, 2, \dots, j-1)$ и слово $\delta_{j2}\delta_{j3}\dots\delta_{jn}$ содержится среди них. Построение методом B_1 заканчивается с построением q строк.

Доказано, что методом B_1 можно построить все особые системы, соответствующие заданному отрезку s^*, и только их.

Оптимальный алгоритм криптоанализа генератора НРП(k, n) выглядит следующим образом: последовательность на выходе генератора наблюдается до тех пор, пока не будет получен её отрезок, удовлетворяющий условиям единственности его продолжения, после чего вся НРП, порождаемая генератором, восстанавливается методом A_3. Длина этого отрезка фиксируется как расстояние единственности (теоретическая стойкость) данной НРП.

Экспериментальные исследования алгоритма на компьютере показали, что расстояние единственности для НРП$(2, n)$ лежит в пределах от $2^{n-1} - 1$ до $2^n - 1$, что свидетельствует о высокой стойкости их генератора.

Это был 1965 год — последний год нашего сотрудничества с ЦКБ «Алмаз» в этой области. К сожалению, по моему человеческому простодушию, в отношения нас с заказчиком вмешался генерал Козлов, и заказчику было запрещено прибегать к нашим криптографическим услугам. Через 40 лет история повторится, но это будет уже в другой стране, с другим заказчиком и при другом генерале.

2. Переходный период

2.1. Под вывеской экспериментов с автоматами

Наши дальнейшие криптографические исследования проводились без ориентации на какого-либо заказчика, носили чисто научный характер и вплоть до признания за криптографией права защищать информацию в интересах не только государства, но и его граждан, касались, главным образом, теории экспериментов с автоматами, имеющей очевидный криптографический «окрас» и в то же время не ограниченной теми запретами, которые сопровождают практическую криптографию. Именно как результаты этой теории, хотя и с большой задержкой, были опубликованы приведённые выше алгоритмы криптоанализа и оценки теоретической стойкости линейного автономного автомата [4, 6], автоматного генератора с ключевой функцией выхода [2, 4, 7] и генератора НРП [3, 4, 8, 10].

В [12] показано, что любой инициальный линейный автомат над конечным полем с размерностью входного символа k и состояния n можно восстановить простым экспериментом длиной не больше $2n + k(n + 1)$.

Решена задача синтеза конечного автомата с минимальным числом состояний, которому присущ заданный кратный эксперимент [14, 16].

Установлены необходимые и достаточные условия, при которых произвольный простой эксперимент отличает любой заданный инициальный автомат от любого другого

автомата в классе всех инициальных автоматов с тем же или меньшим числом состояний [18].

Дальнейшие теоретические исследования генератора НРП привели к построению аналитического выражения для точной верхней оценки его расстояния единственности [13]. Для k-значной последовательности порядка n она равна $2^n - 2$, если $k = 2$ и $n = 2, 3, 4$, и равна $k^n - 1$ в остальных случаях. К сожалению, точная нижняя оценка для этой характеристики генератора НРП до сих пор не установлена. В эксперименте на компьютере исследована сложность булевых функций, порождающих двоичные НРП [9], и показано, что среди таких функций с любым числом переменных n до 20 с небольшим существуют функции, представимые в бесповторной ДНФ [17, 46]. Гипотеза автора о том, что это верно для любого натурального n, к сожалению, пока не доказана.

2.2. Декомпозиция конечных автоматов

Здесь мы дадим краткий обзор наших результатов из монографии [17], подразумевая под декомпозицией автомата его представление автоматной сетью без обратных связей. Вместе с последней декомпозиция бывает каскадной, последовательной, параллельной и параллельно-последовательной. Рассматриваются задачи характеризации (описания) всевозможных декомпозиций того или иного вида для заданного автомата, оценки их сложности и задачи соответствующей приводимости автоматов по состояниям, входам, представлению и полугруппе. Для натуральных $m \geqslant 2$ и $k > 1$ автомат A называется *каскадно m-приводимым по состояниям* и *k-приводимым по входам*, если он представим каскадной сетью автоматов, каждый из которых имеет не более m состояний и не более k входных символов соответственно. Автомат A *каскадно приводим по представлению*, если он допускает каскадную декомпозицию на компоненты, не представляющие в отдельности автомат A. Он *каскадно приводим по полугруппе*, если для него существует каскадная декомпозиция на компоненты, полугруппы которых не делятся его полугруппой. Аналогично определяются все эти виды последовательной, параллельной и параллельно-последовательной приводимости автомата.

Попытки решить задачу характеризации всевозможных декомпозиций автомата привели к необходимости расширения известного понятия покрытия множества состояний автомата, сняв требования непустоты, различности и несравнимости по включению его блоков. Вместе с многозначной нумерацией состояний в блоках сохраняемого покрытия последнее образует так называемое *сохраняемое нумерованное покрытие* (СНУП). Показано, что в терминах СНУП могут быть охарактеризованы все каскадные декомпозиции на две компоненты всех автоматов, и сформулирован метод сохраняемых нумерованных покрытий, который в отличие от известных ранее методов декомпозиции позволяет построить любую из возможных двухкомпонентных каскадных декомпозиций для любого заданного автомата. Аналогичные результаты получены относительно многокомпонентных каскадных декомпозиций, которые характеризуются в терминах вводимых понятий каскадно непротиворечивого кодирования состояний автомата и композиционного ряда сохраняемых покрытий множества его состояний. В частности, в терминах последовательно, параллельно и параллельно-последовательно непротиворечивых кодирований состояний любого автомата охарактеризованы всевозможные его соответственно последовательные, параллельные и последовательно-параллельные декомпозиции.

Известно (H. P. Zeiger), что любой конечный автомат можно разложить в каскадную сеть из перестановочно-возвратных (ПВ-) автоматов. Нами доказано, что в такой

сети, построенной для автомата с $n \geqslant 3$ состояниями методом Зейгера, гарантирующим делимость полугруппы автомата группами компонент сети, число последних может достигать $2^{n-1} - 1$. Показано также, что без требования групповой делимости всякий автомат с n состояниями разлагается в каскадную сеть из ПВ-компонент, число которых не первышает $n-1$. С применением аппарата СНУП доказано, что эта оценка точная.

Автомат с $n \geqslant 2$ состояниями каскадно приводим по представлению, если и только если он не является константным автоматом 2-го порядка.

Автомат каскадно m-приводим по состояниям, если и только если каждый простой делитель его полугруппы изоморфен группе подстановок степени $< m$.

Перестановочный автомат каскадно m-приводим по состояниям, если и только если каждый композиционный фактор его группы изоморфен группе подстановок степени $< m$.

Автомат параллельно m-приводим по состояниям, если и только если его полугруппа делит прямое произведение полугрупп преобразований множества $\{1, \ldots, m-1\}$, взятых в степенях, показатели которых не превосходят их порядков в степени n^n.

Перестановочный автомат с полупростой группой G параллельно m-приводим по состояниям, если и только если в G существуют нормальные делители с единичным пересечением, фактор-группы по которым являются гомоморфными образами групп подстановок степени $< m$.

Перестановочный автомат с полупростой группой параллельно приводим по полугруппе, если и только если в его группе существует система неединичных нормальных делителей с пересечением, равным 1.

Таким образом, установлена алгоритмическая разрешимость проблем каскадной приводимости по состояниям и по представлению и параллельной приводимости по состояниям произвольных автоматов, каскадной приводимости по входам и состояниям автоматов с разрешимыми полугруппами, параллельной приводимости по полугруппе перестановочных автоматов с полупростыми группами.

Установлены также параллельная неприводимость по представлению любого сильно связного автономного автомата, порядок которого есть степень простого числа, и параллельная приводимость по представлению любого перестановочного автомата, порядок которого не есть степень простого числа.

Генераторы НРП интересны не только как источники ключевого потока, но и, подобно LFSR, как компоненты других более сложных криптоалгоритмов. В этой связи представляет интерес наше утверждение, доказанное конструктивно в [17], о том, что для любых натуральных m и $n \geqslant m$ любой конечный автомат с m состояниями можно разложить в каскадную сеть из триггеров и генераторов НРП порядка n.

Исследуя автономные автоматы как генераторы ключевого потока, мы выяснили в [17], при каких необходимых и достаточных условиях для заданных натуральных m и k произвольный автономный автомат с m состояниями можно представить каскадной или параллельной сетью автоматов с числом состояний меньше m и числом входных символов меньше k в каждом. В случае каскадной сети и $k > 2$, $m > 2$ это возможно, если и только если $m > p$, где p — наибольший простой делитель периода полугруппы автомата, а в случае параллельной сети и $k > 1$, $m > 2$ — если и только если $m > \max(r, p^a)$, где r — индекс полугруппы автомата и p^a — наибольший сомножитель в каноническом разложении её периода.

2.3. Развитие алгоритмической базы для компьютерной криптографии

Эти исследования являются частью общего направления нашей научной школы в ТГУ — автоматизации решения комбинаторных задач прикладной дискретной математики. Это значит, что конечными результатами исследований в этом направлении должны быть алгоритмы решения комбинаторных дискретно-математических задач, аттестованные в эксперименте на электронной вычислительной машине (ЭВМ, или по-современному — компьютере). Фактически уже тогда речь шла о создании нового направления в математике — компьютерной дискретной математики. Первые «кирпичи» в фундамент этой науки заложил А. Д. Закревский [11], предложивший системы подмножеств конечных множеств представлять в ЭВМ при помощи булевых и троичных матриц и разработавший иерархическую систему математических операций над такими матрицами и эффективные алгоритмы их выполнения. Система охватывает широкий спектр операций — от простейших (нахождение минимального столбца и максимальной строки) до предельно сложных (кратчайшее покрытие булевой матрицы или минимальное разбиение множества ее столбцов на совместимые подмножества, например). Фундаментальное и прикладное значение этой системы состоит в том, что через операции в ней легко выражаются алгоритмы решения многих задач как в самой дискретной математике, так и в ее приложениях — и не только к синтезу дискретных автоматов, но и к математической логике и криптографии.

Компьютерная криптография — это раздел прикладной криптографии, имеющий дело с разработкой, реализацией и экспериментальным исследованием на ЭВМ эффективных алгоритмов решения комбинаторых задач, возникающих в анализе и синтезе различных криптосистем — шифрования, электронной подписи, аутентификации, идентификации и др. Среди этих задач наиболее частыми являются задачи: перечислительные — когда в конечном множестве комбинаторных объектов требуется перечислить все объекты с заданным свойством; поисковые — когда в конечном множестве требуется найти хотя бы один комбинаторный объект (если он есть) с заданным свойством; оптимизационные — когда дополнительно требуется, чтобы найденный объект доставлял минимум (или максимум) заданной целевой функции. Кроме уже упомянутых выше кратчайшего покрытия и минимального разбиения на классы совместимости, к ним относятся, например, такие задачи, как генерация простых чисел с дополнительными свойствами, генерация сочетаний, перестановок и разбиений, решение систем нелинейных уравнений над конечным полем, задача о рюкзаке, алгоритмические задачи на числах, графах, кодах, булевых функциях и многие другие. Отличительными особенностями всех этих задач являются:

1) большая размерность данных (до тысяч и миллионов бит), затрудняющая разработку и программную реализацию алгоритмов;

2) дискретность данных, исключающая возможность приближённых вычислений и применения традиционных методов вычислительной математики;

3) высокая вычислительная сложность, часто исключающая существование эффективного решения задачи в общем случае;

4) комбинаторный характер, вследствие которого единственно возможным универсальным компьютерным методом построить решение оказывается переборный метод, в котором последовательно порождаются кандидаты в решение и оставляются те из них, которые удовлетворяют условию задачи.

Один из способов организации систематического порождения возможных кандидатов в решение комбинаторной задачи даёт так называемое *дерево поиска*, в котором все

они (кандидаты) представляются путями от корня к листьям дерева и порождаются обходом дерева с возвращением, которое производится всякий раз, когда достигается некоторый лист или становится понятным, что дальнейшее продвижение вперёд не приведёт к листу, где оканчивается путь, представляющий решение. Выбор очередной вершины для продвижения вперёд осуществляется при помощи алгоритма ветвления, а условие для возвращения в предшествующую вершину вычисляется как значение оценочного предиката. Порождение начинается с кандидата, найденного некоторым эвристическим алгоритмом, который вместе с алгоритмом ветвления и оценочным предикатом являются параметрами данного метода и подбираются для каждой конкретной задачи отдельно. От того, насколько удачно они подобраны, зависит объем вычислений и скорость решения задачи.

Формально эта технология решения комбинаторных задач изложена в книге [15], где можно найти и алгоритмы решения многих конкретных задач, разработанные с её применением. На момент разработки они были лучшими среди известных алгоритмов решения тех же задач.

В дальнейшем обход дерева поиска с возвращением был распараллелен для выполнения на многопроцессорной вычислительной системе кластерного типа, о чём см. в отдельной статье [56] этого номера.

3. Наша «гражданская» криптография

С развитием в стране «гражданской» криптографии наши криптографические исследования испытали второе рождение. Оно случилось на стыке двух тысячелетий в непосредственной связи с открытием в ТГУ специальности «Компьютерная безопасность» со специализацией криптографической направленности. Научная школа прикладной дискретной математики ТГУ стала базой для подготовки кадров по новой специальности. Криптографию в ТГУ мы начали преподавать ещё раньше и задолго до того, как в стране появилась первая книжка по этому предмету. Именно результаты наших собственных научных исследований в области криптографии прошлых лет стали основой для постановки в ТГУ и криптографических дисциплин, и криптографической специализации в целом. Ныне в этом деле, наряду с фундаментальными теоремами криптографии [30], значимое место занимает и научная продукция наших современных криптографических исследований, проводимых с активным участием молодёжи, в том числе студентов и аспирантов.

Предмет этих исследований составляют кодовые шифрсистемы [20], системы полиномиальных уравнений над конечным полем и их применение в криптоанализе симметричных шифров [21, 23, 26, 27, 36, 37, 39, 45, 47, 52], криптографические протоколы [19, 22], булевы функции с криптографическими свойствами и их применение в синтезе поточных шифров [24, 34, 35, 40], вероятностные схемы поточного шифрования [31, 43, 49], инволютивные шифры [32, 42], теоретико-числовые алгоритмы, применяемые в анализе и синтезе криптосистем с открытым ключом, [19, 33, 38, 48], генераторы ключевого потока [25, 41, 46, 54], шифрующие автоматы [51], итеративные блочные шифры с аддитивным раундовым ключом [52], схемы разделения секрета [50, 53], параллельная генерация сочетаний, перестановок и разбиений для криптографических применений [28, 44] и др.

3.1. Криптоанализ кодовых шифрсистем [20]

Рассматриваются кодовые шифрсистемы над полем GF(2). Они строятся на основе двоичных кодов, исправляющих ошибки, и, как все шифрсистемы, делятся на два класса — симметричные, или с закрытым ключом, и несимметричные, или с откры-

тым ключом. Для первых предложен вероятностный алгоритм криптоанализа с целью нахождения ключа при возможности выбора сообщений, для вторых — детерминированный алгоритм криптоанализа с целью нахождения сообщения при известных открытом ключе и криптограмме.

Шифрование в симметричной кодовой шифрсистеме описывается уравнением

$$y = xG \oplus e, \tag{3}$$

где x — булев вектор с k компонентами, являющийся сообщением; y — булев вектор с n компонентами, являющийся криптограммой; G — булева матрица размера $k \times n$, которая является закрытым ключом и представляет собой порождающую матрицу некоторого двоичного линейного (n, k)-кода, исправляющего ошибки кратности до $t \geqslant 1$; e — случайный булев вектор ошибки с n компонентами, который содержит не более t единиц. Задача криптоанализа, решаемая в этом случае, — так выбрать значения вектора x, чтобы по ним и соответствующим значениям вектора $y = xG \oplus e$ при случайных и неизвестных значениях вектора e можно было найти матрицу G.

Выберем в качестве значений x единичные векторы длиной k, беря каждый из них некоторое число $s \geqslant 3$ раз. Тогда рассматриваемая задача криптоанализа сводится к решению k раз следующей частной задачи: пусть булевы векторы g, $y_1, \ldots, y_s$, $e_1, \ldots, e_s$ длины n удовлетворяют системе уравнений $y_i = g \oplus e_i$, $i = 1, \ldots, s$, где в j-й раз для $j = 1, \ldots, k$ вектор g есть j-я строка искомой матрицы G и векторы $e_1, \ldots, e_s$ случайные веса $\leqslant t$; требуется, зная $y_1, \ldots, y_s$, найти вектор $g = g_1 \ldots g_n$.

Эта частная задача решается следующим образом: пусть $y_i = y_{i1} y_{i2} \ldots y_{in}$ для $i = 1, \ldots, s$; тогда для каждого $j = 1, \ldots, n$ подсчитываем вес w_j вектора $y_{1j} y_{2j} \ldots y_{sj}$ и полагаем $g'_j = 1$, если $w_j > s/2$, и $g'_j = 0$ в противном случае; вектор $g' = g'_1 \ldots g'_n$ принимаем за решение. Если $t < n/2$, $s = 2r + 1$, $r \geqslant 1$ и p — вероятность принятия компонентой векторов e_i значения 1, то вероятность совпадения g' с искомым g равна $P = \sum_{i=0}^{r} C_s^i p^i (1-p)^{s-i}$. Например, при $n = 19$, $s = 29$ и $t \leqslant 4$ имеем $P = 0,999$.

В эксперименте на компьютере построены зависимости от n и t максимального и среднего арифметического значений числа s, при котором $g' = g$. Из них следует, что с ростом n отношение s/n убывает. Например, при $t = n/4$ и $n = 32, 64, 128, 256, 512$ среднее значение такого s равно 4, 5, 5, 6, 8 соответственно.

В случае несимметричной кодовой шифрсистемы в уравнении шифрования (3) матрица G является открытым ключом, и решаемая задача криптоанализа в этом случае состоит в решении уравнения (3) с известными G и y относительно неизвестного $x = x_1 x_2 \ldots x_k$ при неизвестном булевом векторе e веса, не превосходящего заданного числа t. Это есть задача декодирования для кода, порождённого матрицей G, и в общем случае (для произвольной матрицы G) не решаема за полиномиальное время.

Булев вектор $\alpha = a_1 a_2 \ldots a_i$, где $i \leqslant k$, называется её *частичным решением*, если не превышает величины t вес вектора $e(\alpha) = y \oplus a_1 g_1 \oplus \cdots \oplus a_i g_i$, где g_j для $j = 1, \ldots, k$ есть j-я строка матрицы G; в этом случае вектор $x = \alpha 0^{k-i}$ есть (полное) решение задачи.

Поиск частичного решения осуществляется обходом дерева поиска с возвращением, в котором последовательно порождаются в качестве кандидатов на место префикса в нём булевы векторы длиной не больше k. Это делается при помощи алгоритма ветвления, выбирающего вслед за вектором $a_1 a_2 \ldots a_{i-1}$ поочерёдно всевозможные векторы $a_1 a_2 \ldots a_i$, и условия возвращения, при котором выбранный вектор $\alpha = a_1 a_2 \ldots a_i$ для $i < k$ не может быть префиксом частичного решения. Последнее выполняется, если

истинен оценочный предикат $t_0 + t' > t$, где t_0 есть число номеров одновременно единичных компонент вектора $e(\alpha)$ и нулевых столбцов матрицы H, равной матрице G без первых i строк, и t' вычисляется следующим образом. Пусть m есть число классов равных ненулевых столбцов в H, и s-й из них, $s = 1, \ldots, m$, состоит из столбцов с номерами $r_1, \ldots, r_p$. Обозначим t_{s0} и t_{s1} количество нулей и единиц соответственно среди компонент вектора $e(\alpha)$, имеющих номера $r_1, \ldots, r_p$. Пусть $t_s = \min(t_{s0}, t_{s1})$. Тогда $t' = \sum_{s=1}^{m} t_s$.

Эффективость этого алгоритма в значительной степени зависит от порядка компонент в векторе x. Его оптимизация в каждом конкретном случае является отдельной задачей.

3.2. Системы уравнений над конечным полем

Возможность применения решений систем алгебраических уравнений в криптоанализе шифров обусловлена возможностью описания ими (системами) зависимостей в шифрах между символами известных открытого и шифртекстов и неизвестного закрытого ключа. В криптоанализе генераторов ключевого потока в поточных шифрах система уравнений связывает известные символы потока с неизвестными символами ключа. Основными средствами в решении систем уравнений над конечным полем в наших исследованиях служат дерево поиска с возвращением и метод его сокращённого обхода, составляющие основу созданной нами ранее технологии решения комбинаторно-логических задач [15]. Таким путём построены, в частности, алгоритмы криптоанализа сжимающего и самосжимающего генераторов ключевого потока [23], а для сжимающего генератора, кроме того, получены экспериментальные оценки его теоретической стойкости [26]. Эффективность этой технологии применительно к другим (не криптографическим) комбинаторным задачам демонстрируется в обзорной статье [55] этого номера.

Обход дерева поиска допускает эффективные процедуры распараллеливания на многопроцессорных вычислительных системах кластерного типа [29]. Как это делается в общем виде, а также для конкретных комбинаторных задач, имеющих криптографические применения, в том числе и для решения систем уравнений над конечным полем, демонстрируется в ещё одной обзорной статье [56] данного номера.

Для решения систем уравнений над конечным полем предложен метод *линеаризационного множества* [21, 39]. Последнее — это подмножество переменных системы со свойством: при фиксации любых их значений система уравнений превращается в линейную. Метод состоит в поочерёдной подстановке в систему всевозможных наборов значений переменных линеаризационного множества и в решении получающейся в каждом случае линейной системы методом Гаусса. Его сложность оценивается экспонентой от числа переменных в линеаризационном множестве. Предложен алгоритм построения линеаризационного множества наименьшей мощности обходом дерева поиска с возвращением; разработаны, реализованы и исследованы параллельные алгоритмы решения этой задачи и задачи решения системы линейных уравнений [27, 36, 37, 47, 56].

3.3. Линеаризационная атака

Определение неизвестного ключа криптоалгоритма как решение его системы уравнений методом линеаризационного множества назвается *линеаризационной атакой* [21]. В двоичном случае её вычислительная сложность оценивается числом 2^k, где k — мощность используемого линеаризационного множества. Так, для генератора ключевого потока Geffe линеаризационное множество образуют компоненты ключа, составляющие начальное состояние одного из его регистров, и k совпадает с длиной

этого регистра. Это значит, что фактическим ключом генератора Geffe является состояние только одного его регистра. Эти утверждения верны и для ряда других генераторов ключевого потока, в том числе для генераторов с альтернативным управлением, скалярного умножения и мультиплексорного. Известно, что корреляционная атака на генератор Geffe с длинами регистров n_1, n_2, n_3 имеет сложность $2^{n_1} + 2^{n_2} + 2^{n_3}$, в то время как сложность линеаризационной атаки на него равна одному из слагаемых последней суммы. Показано также, что сложность линеаризационной атаки на пороговый генератор ключевого потока не превосходит 2^m, где m — его расстояние единственности.

3.4. Вероятностные схемы симметричного поточного шифрования

Предложены два класса вероятностных схем симметричного поточного шифрования над конечным полем [31]. Генератор ключевого потока в них функционирует как фильтрующий генератор на основе LFSR максимального периода. В схемах первого класса в качестве функции фильтрации выступает комбинация линейной и нелинейной функций так, что первые n символов ключевого потока, где n — длина регистра, являются значениями линейной функции, а остальные символы — значениями нелинейной функции (на соответствующих состояниях регистра). Линейная функция служит ключом шифра (или определяется по нему), а начальное состояние s_0 регистра — случайным параметром шифрования. Расшифрование сводится к нахождению s_0 путем решения системы линейных уравнений и воспроизведению ключевого потока, а дешифрование требует для этого решения системы нелинейных уравнений. В схемах второго класса, в отличие от первого, случайное начальное состояние генератора ключевого потока складывается покомпонентно с ключом шифра, как в одноразовом блокноте.

Дано общее определение вероятностной поточной шифрсистемы — PSC [43], охватывающее все известные шифрсистемы этого класса. В её составе — ключевая система и блоки рандомизации и шифрования. Первая предназначена для выработки ключей инициализации, свидетельства и генератора. Блок рандомизации состоит из источника (множества) рандомизаторов и узлов свидетельства и инициализации. Формально узел свидетельства является некоторым шифром и предназначен для создания свидетельства рандомизатора в зависимости от ключа свидетельства. Формально узел инициализации является функцией и предназначен для выработки вектора инициализации для блока шифрования в зависимости от рандомизатора и ключа инициализации. Блок шифрования состоит из конечно-автоматного генератора ключевого потока, создаваемого в зависимости от ключа генератора и вектора инициализации, и шифра, предназначенного для зашифрования открытого текста и расшифрования шифртекста по ключевому потоку. При фиксированных ключах системы процесс шифрования выполняется в следующем порядке: выбирается случайно рандомизатор и последовательно вычисляются его свидетельство, вектор инициализации, ключевой поток и шифртекст. В канал связи передаются свидетельство рандомизатора и шифртекст. При расшифровании последнего вычисляются рандомизатор, вектор инициализации, ключевой поток и открытый текст. Выбирая различными способами компоненты системы PSC, можно получить многочисленные примеры вероятностных схем поточного шифрования как известных, так и ранее не встречавшихся.

В литературе по криптографии самосинхронизирующиеся поточные шифры представлены только примерами так называемых регистровых шифров, в которых свойство

самосинхронизации достигается за счет использования в генераторе ключевого потока (ГКП) регистра сдвига, через который пропускается шифртекст, и нет определения самосинхронизирующегося поточного шифра в общем виде, что, понятно, служит тормозом в развитии теории таких шифров. В работе [49], для преодоления этого недостатка, формализовано понятие самосинхронизирующегося с задержкой τ поточного (коротко: с/п-τ) шифра, в котором на каждом ключе в роли ГКП служит конечный автомат Мура, и доказано, что в случае сильной связности последнего всякий такой шифр функционально неотличим от некоторого регистрового шифра — (с/п-τ)-шифра на регистре сдвига длиной τ. Регистровый шифр определён так, что может использоваться как вероятностный (с/п-τ)-шифр. В этом случае шифртекст вычисляется в нём как функция ключа и случайного состояния регистра и передаётся вместе с этим состоянием получателю, который получает открытый текст после отбрасывания первых τ символов из результата расшифрования принятого сообщения по ключу и любому состоянию регистра дешифратора.

3.5. Булевы функции с криптографическими свойствами

Показано, каким образом можно построить все булевы функции, сохраняющие линейную сложность произвольной линейной рекуррентной последовательности (ЛРП) над полем из двух элементов, и оценивается их число, которое для m-последовательности порядка n равно $2(2^n-1)\varphi(2^n-1)/n$ [24]. Доказано, что булевы функции, тождественные своим переменным или отличающиеся от них только на нулевом наборе значений их всех, сохраняют линейную сложность любой двоичной ЛРП, а линейные булевы функции, не тождественные нулю и своим переменным, и функции, отличающиеся от них только на нулевом наборе, сохраняют линейную сложность всякой m-последовательности над полем из двух элементов [34].

Установлено, что булевы функции, линейные по первой или последней из своих существенных переменных, не имеют запрета, и найдено выражение для их числа; предложен графический тест на отсутствие у булевой функции запрета заданной длины l, и на его основе сформулированы алгоритмы порождения всех запретов длины l данной функции и всех функций без запрета данной длины l [35].

Доказана теорема о связи порядка устойчивости булевой функции с порядками устойчивости коэффициентов её разложения Шеннона, и на её основе сформулирован рекурсивный метод построения булевых функций от заданного числа переменных с заданным максимальным порядком устойчивости [40].

3.6. Теоретико-числовые алгоритмы в криптографии

Исследованы два варианта реализации алгоритма Адлемана дискретного логарифмирования в $\mathbb{Z}_p^*$ для простого p [33]. В первом варианте в систему сравнений для логарифмов простых чисел из факторной базы не включаются сравнения с ненулевыми необратимыми в $\mathbb{Z}_{p-1}^*$ коэффициентами на диагонали треугольной матрицы системы, так что система имеет единственное решение, а во втором — в систему включаются все возможные сравнения, но из её многочисленных решений отбирается только то, которое состоит из всех требуемых логарифмов. Варианты сравнивались по скорости логарифмирования на компьютере при разных размерах модуля и факторной базы. Эксперименты показали в пользу второго варианта. Доказана корректность алгоритма Адлемана для дискретного логарифмирования по простому модулю p в любой циклической подгруппе G группы $\mathbb{Z}_p^*$ с факторной базой, не обязательно целиком содержащейся в G. В действительности факторная база в этом случае вместе с элементом $x \in \mathbb{Z}_p^*$ может содержать и все корни s-й степени из x^s по модулю p, где s находится из

условий: $p = sq + 1$ и q — простое число. Такое расширение факторной базы упрощает применяемое в алгоритме разложение чисел в $\mathbb{Z}_p^*$ на множители из факторной базы и не увеличивает размерности решаемой системы сравнений.

В эксперименте на компьютере исследовались [19] следующие алгоритмы факторизации чисел RSA $n = pq$: Div1 — последовательным делением n на простые числа от 2 до $n^{1/2}$, Div2 — последовательным делением n на простые числа от $n^{1/2}$ до 2, Olv — методом Дж. Г. Олвея и Fer — методом Ферма. Установлено, что на числах длиной до 64 бит среди этих алгоритмов наиболее медленный алгоритм Olv и наиболее быстрые — Fer и Div2, и, кроме того, время работы каждого из последних двух растёт линейно с ростом $|p - q|$.

В [19] представлены также результаты экспериментального исследования на персональном компьютере прошлого века длительности некоторых известных атак на шифр RSA — с общим модулем, циклической и обобщённой циклической, с малой экспонентой шифрования и адаптивной атаки с выбором шифртекста. Как показал эксперимент, последние две атаки выполняются за пренебрежимо малое машинное время, первая — на числах длиной до 1500 бит за время в пределах нескольких минут, а циклические атаки нередко приводят к результату за приемлемое машинное время (на числах длиной в несколько десятков бит — в пределах от долей секунд до получаса).

Предложены параллельные реализации на суперкомпьютере кластерного типа двух алгоритмов факторизации чисел — ρ-метода Полларда и квадратичного решета [38]. В обоих случаях распараллеливается процедура порождения последовательности необходимых пар чисел, а именно: каждый процессор, кроме управляющего, порождает свою подпоследовательность независимо от других. Кроме того, в первом случае процессор осуществляет разложение порождаемых им вторых чисел по факторной базе и результат разложения вместе с порождёнными парами отсылает управляющему процессору. Для обоих алгоритмов произведено сравнение последовательных и параллельных реализаций на кластере с 9 двухпроцессорными компьютерами, работающими с тактовой частотой 650 МГц. Обнаружено, что ускорение (отношение времени работы последовательной программы ко времени работы параллельной) с ростом числа процессоров заметно отстаёт от него. Самое большое число, которое удалось факторизовать по ρ-методу Полларда параллельной программой на 12-процессорном кластере, имеет длину 128 бит. На это ушло 103 часа машинного времени.

Проведено экспериментальное сравнение двух алгоритмов генерации доказуемо простых чисел — алгоритма Маурера и алгоритма из Российского стандарта электронной цифровой подписи (ГОСТ Р34.10-94) и выявлен следующий недостаток обоих: иногда они ошибочно пропускают простые числа как не прошедшие проверку по основанию 2, но признаваемые простыми проверкой по основанию 3 [48]. Кроме того, в [19] установлено, что алгоритм из стандарта ГОСТ Р34.10-94 несколько проигрывает по скорости алгоритму генерации сильных простых чисел Гордона, что объясняется применением в последнем более быстрой процедуры проверки числа на простоту по вероятностному алгоритму Миллера — Рабина.

3.7. Генераторы ключевого потока

Представлены два варианта системы логических уравнений сжимающего генератора [25]. Уравнения в первом варианте рекуррентные, во втором — моделируют алгоритм сортировки «пузырёк». В эксперименте на компьютере исследованы различные варианты программной реализации генератора Fish. Наиболее быстрый вариант, в котором обращение к массивам регистров генератора осуществляется через указатели

без использования смещения, на компьютере с частотой 700 МГц порождает ключевой поток длиной 100 Мбит за 0,441 с.

В экспериментах на современных компьютерах более тщательно исследована [41] эффективность алгоритмов A и B криптоанализа конечно-автоматного генератора G ключевого потока с функцией выхода в качестве ключа (см. п. 1.3). Выяснено, в частности, что при известном числе k существенных переменных ключевой функции длина отрезка ключевого потока, требуемого для ее определения, сравнительно не велика, в то время как при известной только верхней границе k_0 для k длина требуемого отрезка ключевого потока много больше первой и быстро растет с ростом k_0. Это объясняется тем, что во втором случае, особенно если $k_0 >> k$, велико количество ложных ключей, для отсева которых как раз и требуется длинный отрезок ключевого потока. Кроме того, в этом случае возможны эквивалентные ключи, и тогда проверяемое алгоритмом B условие единственности не выполняется при любой длине ключевого потока. Этот недостаток алгоритма B преодолевается в следующем алгоритме C, решающем задачу криптоанализа G в тех же предположениях, что и B. Его применение предваряется этапом предвычислений, на котором в компьютерном эксперименте с генератором G с заданными параметрами n и $k = 1, 2, \ldots, k_0$ определяется ожидаемое максимальное значение $l(n, k)$ длины кратчайшего отрезка ключевого потока, по которому алгоритм A находит решение своей задачи — ключевую функцию g при известном числе k ее существенных аргументов. Затем алгоритм C определяет ключевую функцию g применением алгоритма B к отрезку ключевого потока длиной $l(n, k) + \delta$ для небольшого $\delta \geqslant 0$: сначала в предположении, что $k = k_0$, затем в предположении, что $k = k_0 - 1$, и так далее. Если при очередном предполагаемом k алгоритм B не находит g по отрезку ключевого потока длиной $l(n, k) + \delta$, то k уменьшается на 1. Экспериментальные результаты компьютерного моделирования алгоритма C свидетельствуют о том, что алгоритм C в десятки раз эффективнее алгоритма B — и по длине требуемого ключевого потока, и по времени выполнения.

Предложен алгоритм с вычислительной сложностью $O(2^n/n)$, позволяющий по задаваемым значениям параметра (ключа) путем склеивания циклов, порожденных циклически минимальными числами, строить двоичные нормальные рекуррентные последовательности порядка n так, что при разных значениях ключа с равной вероятностью строятся попарно неэквивалентные последовательности из множества большой мощности [54]. В случае простого n последняя равна числу $\prod_{n-1}^{m=1} m^{C_m^n/n}$, а длина ключа в битах — числу $((2^n-2)[\log(n-1)]/(n-1)$. Основной инструмент в этом построении — *циклически минимальное число* — определяется как всякое такое целое неотрицательное число, которое не уменьшается при любом циклическом сдвиге влево его двоичного представления.

3.8. Инволютивные шифры [32, 42]

Инволютивный шифр определяется как пара $C = (X, Q)$, где X — конечное множество сообщений и криптограмм и Q — подмножество множества *инволюций на* X, т. е. подстановок $q\colon X \to X$ со свойством $q(q(x)) = x$ для каждого $x \in X$. В нём каждая инволюция $q \in Q$ является одновременно ключом и операциями шифрования и расшифрования по ключу q.

Известно, что любая инволюция разлагается в произведение независимых циклов длиной не более 2. Кроме того, доказано, что количество r_p всех инволюций на множестве X мощности p подсчитывается по рекуррентной формуле $r_p = r_{p-1} + (p-1)r_{p-2}$, где $r_1 = 1$, $r_2 = 2$.

Подмножество $Z \subseteq X$ называется *тестом* для $q \in Q$, если для любого $s \in Q - \{q\}$ найдётся $z \in Z$, что $q(z) \neq s(z)$. Его можно получить, взяв по одному элементу из каждого цикла длины 2 в разложении q. Его мощность не более $|X|/2$. Тест для каждого $q \in Q$ называется *тестом для* C. Тест с наименьшим числом элементов называется *кратчайшим*. Такой тест для C можно построить как подмножество в X наименьшей мощности, которое пересекается с каждым циклом длины 2 в любой инволюции из Q. Эта задача решается как задача о кратчайшем покрытии булевой матрицы [11].

Любой ключ q шифра C однозначно определяется значениями $q(x)$ для всех x из теста для C, поэтому криптоанализ шифра C с целью раскрытия его ключа атакой с выбором открытого текста сводится к построению теста для C.

Пусть $4|p = |X|$, α — эквивалентность на X со всеми двухэлементными классами и $C_\alpha = (X, Q_\alpha)$ — инволютивный шифр, где для инволюции q на X

$$q \in Q_\alpha \Leftrightarrow \forall x, y \in X(x \alpha y \Rightarrow (q(x) \neq x \wedge q(y) \neq y \wedge q(x) \alpha q(y))).$$

Доказано, что число всех инволюций в C_α равно $r_\alpha = (p/2)!/(p/4)!$ и что мощность теста для любой из них равна $p/4$.

Произвольная инволюция $q \in Q_\alpha$ индуцирует на множестве X/α всех классов эквивалентности α инволюцию q' по правилу $q'(\{x, y\}) = \{q(x), q(y)\}$. Тест для C_α можно построить, выбрав по одному классу из каждого цикла в подстановке q' для всех $q \in Q_\alpha$ и взяв из каждого выбранного класса по одному элементу. Этот тест будет кратчайшим при наименьшем числе различных выбранных классов. Такой выбор можно осуществить опять же как решение задачи о кратчайшем покрытии булевой матрицы.

Пусть далее $X = A^n$ для некоторых натурального n и алфавита A и для всех $q \in Q$ и $i \in \{1, 2, \ldots, n\}$ определены функции $q_i \colon X \to A$ так, что $q(x) = q_1(x)q_2(x) \ldots q_n(x)$ для любого $x \in X$. Пусть также $B = \{i_1, \ldots, i_k\} \subset \{1, 2, \ldots, n\}$, $i_1 < \cdots < i_k$ и $q_B(x) = q_{i_1}(x) \ldots q_{i_k}(x)$. Инволюции q и s на X называют *B-неотличимыми* и пишут $q \approx_B s$, если $q_B(x) = s_B(x)$ для всех $x \in X$. Говорят, что инволюция $q \in Q$ *определяется в C множеством B однозначно*, или *B-определима в C*, если $\forall s \in Q(s \approx_B q \Rightarrow s = q)$.

Смысл последних понятий следующий. Если V есть число всех инволюций в Q, B-неотличимых от $q \in Q$, то $1/V$ есть вероятность, с которой ключ q шифра C определяется своими компонентами с номерами в B. Ключ q можно считать слабым в C, если найдётся подмножество B, при котором число V близко к 1, в частности когда B определяет q в C однозначно.

Таким образом, встают задачи: 1) найти V для заданных Q, $q \in Q$ и $B \subset \{1, \ldots, n\}$; 2) найти (если возможно) хотя бы одно $B \subset \{1, \ldots, n\}$, для которого B-определим в C ключ $q \in Q$; 3) для заданного B оценить число всех B-определимых в C ключей $q \in Q$ в зависимости от параметров шифра и мощности B. Решения этих задач для шифра, содержащего всевозможные инволюции на множестве сообщений, и для шифра со всеми инволюциями, разложимыми в произведение циклов длины 2, представлены в работе [42].

3.9. Схемы разделения секрета

Предложена схема разделения секрета, в которой в качестве секретов используются инволюционные подстановки на декартовой степени конечного множества, определяемые однозначно проекциями последней, включающими авторизованные группы участников, представленных своими номерами, а в качестве долей секрета — проекции набора функций, которыми задается секрет [50].

Базовые понятия (структура доступа — сд, схема разделения секрета — срс, совершенная срс, скорость срс, идеальная срс, сд и срс Брикелла и др.), а также основополагающие теоремы теории совершенных схем разделения секрета (о связи идеальных совершенных срс с матроидами, об условиях реализуемости сд схемой Брикелла, о соотношении между параметрами пороговой сд и реализующей ее схемы Брикелла и др.) вместе с оригинальными доказательствами систематизированы в [53].

3.10. Шифрующие автоматы

В эксперименте на компьютере исследована стойкость автоматного шифра с закрытым ключом к атакам на основе шифртекста, с известным открытым текстом и с выбором открытого текста [51]. Атаки применяются к шифрам 1-го типа, где ключом служит только начальное состояние автомата, и к шифрам 2-го типа, где в ключ входят одновременно начальное состояние и некоторое подмножество переходов в автомате. Первые две атаки осуществляются «грубой силой», третья атака на автоматы 1-го типа проводится как простой безусловный диагностический эксперимент, а на автоматы 2-го типа — как простой безусловный установочный эксперимент над прямым произведением доопределений заданного частичного автомата с последующим проведением диагностического эксперимента, как в предыдущем случае. Компьютерное моделирование данных атак демонстрирует нестойкость шифров 1-го типа к атакам с выбором открытого текста — по той простой причине, что почти все шифрующие автоматы допускают короткую диагностическую последовательность.

3.11. Дифференциальный криптоанализ

Среди научных достижений последних 15 – 20 лет в области криптоанализа важное место занимает дифференциальный криптоанализ. Применительно к шифрам он используется для построения атак с выбором открытого текста, имеющих целью (полное или частичное) раскрытие ключа шифра. Его название происходит от английского difference — разность и связано с тем, что в нем рассматриваются зависимости не между открытыми и шифртекстами, но между разностями пар открытых текстов и разностями пар соответствующих шифртекстов при фиксированном неизвестном ключе. Со времени выхода в свет первых работ по дифференциальному криптоанализу появились десятки, если не сотни, публикаций, в которых предлагаются конкретные атаки на конкретные шифры (или другие криптосистемы), разработанные на основе этой его идеи. К сожалению, среди них нет или слишком мало работ теоретического характера, которые содержали бы изложение дифференциального криптоанализа как метода в общем виде, а именно так, как это принято в вычислительной математике — с определением основных его понятий, с формулировкой и доказательством его базовых теорем, с определением классов шифров, к которым он применим, с формулировкой его алгоритма для какого-либо из этих классов или, хотя бы, четких правил (технологии) разработки такого алгоритма. Ничего подобного, к сожалению, на данный момент в криптографии нет. Известные атаки дифференциального криптоанализа на конкретные шифры носят совершенно частный характер и не применимы к другим шифрам, даже близким по классу.

В работе [52] предпринимается попытка хотя бы частично восполнить этот пробел. В ней дифференциальный криптоанализ рассматривается применительно к произвольным итеративным блочным шифрам, в которых блок открытого текста преобразуется в блок шифртекста за несколько раундов с применением на каждом раунде одной и той же операции преобразования, осуществляемой в зависимости от аддитивного раундового ключа. Изложению метода в общем виде предшествуют введение необхо-

димых элементов теории функций на конечных абелевых группах, определение класса рассматриваемых шифров, их классификация по свойствам раундовой функции, установление необходимых вспомогательных предложений, а также формулировка альтернативного метода для одного частного случая, а именно для шифров с функцией раунда, разделимой по Фейстелю. Этот частный метод основан на теореме об аддитивном раундовом ключе и фактически повторяет классический подход дифференциального криптоанализа к DES с присущими ему недостатками. Общий же метод дифференциального криптоанализа, сформулированный как алгоритм для всех итеративных блочных шифров с аддитивным раундовым ключом, в своей основе сводится к решению системы полиномиальных уравнений над конечным полем для последнего раунда шифра с известными значениями на его выходе, с известной с ненулевой вероятностью разностью значений на его входе, с неизвестными компонентами раундового ключа и с неизвестными значениями на его входе. Для r-раундового шифра разность на входе r-го раунда берется из $(r-1)$-раундовой дифференциальной характеристики этого шифра. Все построения общего характера проиллюстрированы на примере DES, взятого без операций начальной и заключительной перестановок и без расписания раундовых ключей.

3.12. Криптографические протоколы идентификации и цифровых денег

Показано [19], что в протоколе Фиата — Шамира доказывающий проходит идентификацию перед проверяющим, не зная закрытого ключа $(s_1, \ldots, s_k)$ последнего, если выполнено следующее *условие некорректности*: «в открытом ключе проверяющего $(v_1, \ldots, v_k)$ есть такое число v_j, что $u^2 v_j^{-1} \mod n = c^2$ для некоторых натуральных u и c», и, кроме того, ответ проверяющего является единичным вектором с 1 в j-й компоненте. Равенство в условии некорректности выполняется, например, если $us_j \mod n \in [0, \sqrt{n}] \cup [n-\sqrt{n}, n]$ и $c = \sqrt{u^2 v_j^{-1} \mod n}$ для некоторого u.

На базе криптографического протокола цифровых денег Шаума разработана платёжная компьютерная система для проведения расчётов между продавцом, покупателем и банком посредством электронной наличности в режиме реального времени через Internet с гарантией неотслеживаемости действий покупателя и невозможности повторного использования электронных денег участниками платежа [22].

4. Организационные мероприятия

В настоящее время исследования по криптографии в ТГУ служат научной базой для подготовки математиков по специальности 090102 «Компьютерная безопасность» со специализацией «Математические методы защиты информации». В ТГУ эта специальность открыта приказом МОПО РФ № 1219 от 18 мая 1998 г. Содержание подготовки специалистов по ней с перечнем преподаваемых дисциплин можно найти на сайте fpmk.tsu.ru.

Организацию учебного процесса по специальности и преподавание её дискретно-математических, общепрофессиональных и специальных дисциплин осуществляет кафедра защиты информации и криптографии, созданная для этой цели приказом ректора ТГУ от 7 апреля 1999 г.

Результаты проводимых научных исследований апробируются на Сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография» — SibeCrypt, которую кафедра, начиная с 2002 г., ежегодно проводит в сентябре в различных городах Сибири. В ней регулярно участвуют до 70 учёных,

студентов и аспирантов из учебных и научных учреждений России, Украины, Беларуси.

С целью профориентации томских школьников и для подготовки их к поступлению в ТГУ на специальность «Компьютерная безопасность» при кафедре открыта бесплатная школа юного криптографа, в которой с помощью ведущих специалистов кафедры учащиеся знакомятся с историей криптографии, овладевают необходимыми элементами дискретной математики, изучают простейшие криптографические системы и получают навыки решения криптографических задач.

ЛИТЕРАТУРА

1. *Агибалов Г. П.* САК-ЛЯПАС — система алгоритмов теории кодирования на основе языка ЛЯПАС // Логический язык для представления алгоритмов синтеза релейных устройств / Под ред. М. А. Гаврилова и А. Д. Закревского. М.: Наука, 1966. С. 326–341.
2. *Агибалов Г. П., Левашников А. А.* Статистическое исследование задачи опознания булевых функций одного класса // Тез. докл. к предстоящему Всесоюзному коллоквиуму по автоматизации синтеза дискретных вычислительных устройств, 20 – 25 сентября 1966 г., Новосибирск, 1966. С. 40–45.
3. *Агибалов Г. П., Левашников А. А.* Программа синтеза регистров сдвига, порождающих нормальные периодические последовательности // Тез. докл. к предстоящему Всесоюзному коллоквиуму по автоматизации синтеза дискретных вычислительных устройств, 20 – 25 сентября 1966 г., Новосибирск, 1966. С. 28–31.
4. *Агибалов Г. П.* Распознавание операторов, реализуемых в автономных автоматах // Конф. по теории автоматов и искусственному интеллекту. Аннотации докладов и программа. М.: ВЦ АН СССР, 1968. С. 7–8.
5. *Agibalov G. P.* SAK-LYaPAS — a system of coding theory algorithms in LYaPAS // LYaPAS, a Programming Language for Logic and Coding Algorithms. New York; London: Academic Press, 1969. P. 690–720.
6. *Агибалов Г. П.* Распознавание операторов, реализуемых в линейных автономных автоматах // Изв. АН СССР. Техническая кибернетика. 1970. № 3. С. 99–108.
7. *Агибалов Г. П.* О некоторых доопределениях частичной булевой функции // Труды Сибирского физико-технического института. Проблемы кибернетики. Вып 49. Томск: Изд-во Том. ун-та, 1970. С. 12–19.
8. *Агибалов Г. П.* Отождествление нормальных периодических последовательностей начальными отрезками // Труды Сибирского физико-технического института. Проблемы кибернетики. Вып 49. Томск: Изд-во Том. ун-та, 1970. С. 20–37.
9. *Агибалов Г. П., Левашников А. А.* Статистические оценки сложности булевых функций, порождающих нормальные периодические последовательности // Труды Сибирского физико-технического института. Проблемы кибернетики. Вып 51. Томск: Изд-во Том. ун-та, 1970. С. 6–8.
10. *Агибалов Г. П.* Распознавание операторов, вычисляющих нормальные периодические последовательности // Изв. АН СССР. Техническая кибернетика. 1971. № 6. С. 165–173.
11. *Закревский А. Д.* Алгоритмы синтеза дискретных автоматов. М.: Наука, 1971. 512 с.
12. *Агибалов Г. П., Юфит Я. Г.* О простых экспериментах для линейных инициальных автоматов // Автоматика и вычислительная техника. 1972. № 2. С. 17–19.
13. *Агибалов Г. П., Ванина Н. В.* Точная верхняя оценка степени различимости произвольной нормальной периодической последовательности // Изв. АН СССР. Техническая кибернетика. 1973. № 1. С. 131–136.

14. *Агибалов Г. П.* Синтез автоматов по конечно-определённым словарным функциям // Алгоритмы решения задач дискретной математики. Томск: Изд-во Том. ун-та, 1979. С. 160–164.

15. *Агибалов Г. П., Беляев В. А.* Технология решения комбинаторно-логических задач методом сокращённого обхода дерева поиска. Томск: Изд-во Том. ун-та, 1981. 125 с.

16. *Агибалов Г. П., Оранов А. М.* Лекции по теории конечных автоматов. Томск: Изд-во Том. ун-та, 1984. 184 с.

17. *Агибалов Г. П., Евтушенко Н. В.* Декомпозиция конечных автоматов. Томск: Изд-во Том. ун-та, 1985. 128 с.

18. *Евтушенко Н. В.* О принадлежности последовательности множеству контрольных последовательностей автомата // Алгоритмы решения задач дискретной математики. Вып. 2. Томск: Изд-во Том. ун-та, 1987. С. 130—133.

19. *Агибалов Г. П., Дирко Д. В., Казаков С. А., Коршиков Е. М.,* Компьютерное моделирование и исследование некоторых криптологических алгоритмов с открытым ключом // Новые информационные технологии в исследовании дискретных структур. Томск: ТНЦ СО РАН, «Спектр», 2000. С. 64–70.

20. *Пронина И. В., Агибалов Г. П.* Некоторые алгоритмы криптоанализа для кодовых криптосистем // Вестник Томского госуниверситета. Июнь 2000. № 271. С. 115–118.

21. *Агибалов Г. П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского госуниверситета. Приложение. Сентябрь 2003. № 6. С. 31–41.

22. *Михалёва М. А.* Электронная платёжная система на базе криптографического протокола цифровых денег // Вестник Томского госуниверситета. Приложение. Сентябрь 2003. № 6. С. 42–49.

23. *Агибалов Г. П.* Логические уравнения в криптоанализе сжимающего и самосжимающего генераторов // Вестник Томского госуниверситета. Приложение. Август 2004. № 9(I). С. 49–54.

24. *Колегов Д. Н.* О булевых функциях, сохраняющих линейную сложность линейной рекуррентной последовательности // Вестник Томского госуниверситета. Приложение. Август 2004. № 9(I). С. 18–20.

25. *Стефанцов Д. А.* Логическое и компьютерное моделирование криптоалгоритма Fish // Вестник Томского госуниверситета. Приложение. Август 2004. № 9(I). С. 82–84.

26. *Тимошевская Н. Е.* Экспериментальное исследование стойкости сжимающего генератора // Вестник Томского госуниверситета. Приложение. Август 2004. № 9(I). С. 84–88.

27. *Тимошевская Н. Е.* Параллельные вычисления в решении систем логических уравнений методом линеаризации // Материалы XV Междунар. школы-семинара «Синтез и сложность управляющих систем» / Под ред. О. Б. Лупанова. Новосибирск: Изд-во Института математики, 2004. С. 97–102.

28. *Тимошевская Н. Е.* Параллельная генерация сочетаний и перестановок // Вторая Сибирская школа-семинар по параллельным вычислениям. Томск: Изд-во Том. ун-та, 2004. С. 55–59.

29. *Тимошевская Н. Е.* Параллельные методы обхода дерева // Математическое моделирование. 2004. Т. 16. № 1. С. 105–114.

30. *Агибалов Г. П.* Избранные теоремы начального курса криптографии. Томск: Изд-во НТЛ, 2005. 116 с.

31. *Агибалов Г. П.* Вероятностные схемы симметричного поточного шифрования над конечным полем // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 39–42.

32. *Андреева Л. Н.* К криптоанализу шифров инволюционной подстановки // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 43–44.

33. *Белов А. Г.* Исследование алгоритма дискретного логарифмирования Адлемана // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 45–49.

34. *Колегов Д. Н.* О некоторых классах булевых функций, сохраняющих линейную сложность линейных рекуррентных последовательностей // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 57.

35. *Колегов Д. Н.* О булевых функциях без запрета // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 58–60.

36. *Тимошевская Н. Е.* Задача о кратчайшем линеаризационном множестве // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 79–83.

37. *Тимошевская Н. Е.* О линеаризационно эквивалентных покрытиях // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 84–91.

38. *Худяшов И. И.* Применение параллельных вычислений в методах факторизации // Вестник Томского госуниверситета. Приложение. Август 2005. № 14. С. 96–98.

39. *Агибалов Г. П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского госуниверситета. Приложение. Август 2006. № 17. С. 4–9.

40. *Панин А. Н.* Генерация булевых функций зданного порядка устойчивости // Вестник Томского госуниверситета. Приложение. Август 2006. № 17. С. 47–52.

41. *Агибалов Г. П., Сунгурова О. Г.* Криптоанализ конечно-автоматного генератора ключевого потока с функцией выходов в качестве ключа // Вестник Томского госуниверситета. Приложение. Август 2006. № 17. С. 104–108.

42. *Андреева Л. Н.* К криптоанализу инволютивных шифров с частично известными инволюциями // Вестник Томского госуниверситета. Приложение. Август 2006. № 17. С. 109–112.

43. *Колегов Д. Н.* Общая схема вероятностной поточной шифрсистемы // Вестник Томского госуниверситета. Приложение. Август 2006. № 17. С. 109–112.

44. *Тимошевская Н. Е.* Параллельное перечисление разбиений множества методом нумерации // Вестник Томского госуниверситета. Приложение. Август 2006. № 17. С. 260–264.

45. *Худяшов И. И., Семёнов В. В.* Применение параллельных вычислений для решения систем логических уравнений методом линеаризационного множества // Вестник Томского госуниверситета. Приложение. Август 2006. № 17. С. 267–272.

46. *Агибалов Г. П.* Нормальные рекуррентные последовательности // Вестник Томского госуниверситета. Приложение. Август 2007. № 23. С. 4–11.

47. *Тимошевская Н. Е.* Оценки числа покрытий с линеаризационными множествами заданной мощности // Вестник Томского госуниверситета. Приложение. Август 2007. № 23. С. 60–64.

48. *Белов А. Г., Панкратова И. А.* Сравнительный анализ двух алгоритмов генерации простых чисел // Вестник Томского госуниверситета. Приложение. Август 2007. № 23. С. 77–80.

49. *Панкратов И. В.* К определению понятия самосинхронизирующегося поточного шифра // Вестник Томского госуниверситета. Приложение. Август 2007. № 23. С. 114–117.

50. *Андреева Л. Н.* Инволюционные схемы разделения секрета // Вестник Томского госуниверситета. Приложение. Август 2007. № 23. С. 99.

51. *Треньkаев В. Н., Колесников Р. Г.* Автоматный подход к атакам на симметричные шифры // Вестник Томского госуниверситета. Приложение. Август 2007. № 23. С. 77–80.

52. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1. С. 34–42.

53. *Парватов Н. Г.* Совершенные схемы разделения секрета // Прикладная дискретная математика. 2008. № 2. С. 50–57.

54. *Поздеев А. Г.* Построение нормальных периодических последовательностей из циклически минимальных чисел // Прикладная дискретная математика. 2008. № 2. С. 15–17.

55. *Андреева Л. Н.* Технология решения задач кратчайшего разбиения // Прикладная дискретная математика. 2009. № 2. С. 79–95.

56. *Тимошевская Н. Е.* Разработка и исследование параллельных комбинаторных алгоритмов // Прикладная дискретная математика. 2009. № 2. С. 96–103.

57. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2. С. 127–137.