Московский государственный университет имени М.В.Ломоносова

На правах рукописи

Мелузов Антон Сергеевич

ПОСТРОЕНИЕ И АНАЛИЗ ЭФФЕКТИВНЫХ КОМБИНАТОРНЫХ АЛГОРИТМОВ РЕШЕНИЯ СИСТЕМ БУЛЕВЫХ УРАВНЕНИЙ

Специальность **05.13.19.** —
Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2012

Работа выполнена на
кафедре Математической кибернетики
факультета Вычислительной математики и кибернетики
Московского государственного университета имени М.В.Ломоносова

Научный руководитель: *кандидат физико-математических наук,*
старший научный сотрудник
Логачев Олег Алексеевич;

Официальные оппоненты:
доктор физико-математических наук
профессор Бабаш Александр Владимирович;

кандидат физико-математических наук
Сергеев Игорь Сергеевич.

Ведущая организация: *Российский государственный*
гуманитарный университет

Защита диссертации состоится «29» февраля 2012 года в 16^{45} на заседании диссертационного совета *Д.501.002.16* при Московском государственном университете имени М.В. Ломоносова по адресу: РФ, 119991, Москва, ГСП-1, Ленинские горы, д. 1, МГУ, Главное здание, механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке Механико-математического факультета МГУ имени М.В. Ломоносова (Главное здание, 14 этаж).

Автореферат разослан «__» _____ 2012 г.

Ученый секретарь диссертационного совета Д 501.002.16 при МГУ,
доктор физико-математических наук,
профессор

А.А. Корнев

Общая характеристика работы

Актуальность темы. В ходе разработки, анализа и совершенствования средств и механизмов защиты информации возникают задачи формального описания процессов обработки информации на основе математических моделей. Процессы, протекающие в информационных системах могут моделироваться системами булевых уравнений. При этом задачи анализа эффективности систем обеспечения информационной безопасности, аудита состояния объекта, находящегося под воздействием угроз информационной безопасности, задачи анализа рисков нарушения информационной безопасности, уязвимости процессов обработки информации и другие задачи в сфере защиты информации могут быть переформулированы в терминах поиска решений систем булевых уравнений и анализа трудоемкости, других характеристик этого поиска.

Задача решения систем булевых уравнений возникает во многих разделах математики, в том числе, в криптологии, теории кодирования, теории автоматов, в алгебраических приложениях. Под задачей решения систем булевых уравнений, будем иметь ввиду задачу поиска всех решений системы.

Среди известных методов решения систем булевых уравнений можно выделить несколько направлений, по которым велись исследования различными авторами. Универсальным методом решения систем полиномиальных уравнений, который может быть применен и для решения булевых систем, является метод построения минимального редуцированного базиса Грёбнера идеала, образованного полиномами, входящими в систему уравнений. Для построения базиса Грёбнера идеала известны алгоритм Бухбергера[1] и алгоритмы F_4, F_5, предложенные Ж.-К. Фажере[2][3].

Другим направлением в решении систем булевых уравнений являются методы, связанные с линеаризацией. Линеаризация — метод решения систем, состоящий в замене всех мономов степени выше первой новыми переменными, решении полученной линейной системы и последующей проверке полученных решений на корректность.

[1] *B. Buchberger.* **Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory.** Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985.

[2] *J.-C. Faugère.* **A new efficient algorithm for computation Gröebner bases (F_4).** Journal of pure and applied algebra, 1999.

[3] *J.-C. Faugère.* **A new efficient algorithm for computation Gröebner bases without reduction to zero (F_5).** Proceedings of the 2002 international symposium on Symbolic and algebraic computation, p.75–83, 2002.

Группой ученых под руководством Н. Куртуа были предложены усовершенствования XL[4] и XSL[5] метода линеаризации для случаев, когда количество уравнений в системе недостаточно для эффективного применения линеаризации в классическом виде. Суть данных методов состоит в дополнении системы новыми уравнениями, которые не меняют множества решений системы, но увеличивают размер системы и ранг линеаризованной системы. Позднее Н. Куртуа и Г.В. Бардом был предложен еще один метод, основанный на методе линеаризации — ElimLin[6].

Поскольку задача выполнимости конъюнктивной нормальной формы (КНФ) является актуальной и её исследованию посвящено значительное количество научных работ, кроме того постоянно совершенствуются алгоритмы решения задачи выполнимости КНФ, важным направлением в решении систем булевых полиномиальных уравнений стало сведение задачи поиска решения системы к задаче выполнимости КНФ[7] [8] [9] [10] [11].

Семейство комбинаторных методов решения разреженных систем булевых уравнений было предложено И. Семаевым и Г. Рад-

[4] *N. Courtois, A. Klimov, J. Patarin, A. Shamir.* **Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations.** Advances in Cryptology, EUROCRYPT 2000, p. 392–407, 2000.

[5] *N. Courtois, J. Pieprzyk.* **Cryptanalysis of block chiphers with overdefined systems of equations.** Proc. 8th Int. Conf. on the Theory and Application of Cryptology and Information Security, Springer, p. 267–287, 2002.

[6] *N. Courtois, G. V. Bard* **Algebraic cryptanalysis of the data encryption standard.** IMA International Conference on Cryptography and Coding Theory, Lecture Notes in Computer Science, Springer-Verlag, p. 152—169, 2007.

[7] *F. Massacci, L. Marraro.* **Logical Cryptanalysis as a SAT Problem.** Journal of Automated Reasoning, Springer Netherlands, p. 165-203, 2000.

[8] *C. Fiorini, E. Martinelli, F. Massacci.* **How to fake an RSA signature by encoding modular root finding as a SAT problem.** Discrete Applied Mathematics, p. 101-127, 2003.

[9] *A. K. Abdel, Y. M. Amr.* **Applications of SAT Solvers to AES key Recovery from Decayed Key Schedule Images.** Cryptology ePrint Archive, http://eprint.iacr.org/, vol. 324, 2010.

[10] *I. Mironov, L. Zhang.* **Applications of SAT Solvers to Cryptanalysis of Hash Functions.** Cryptology ePrint Archive, http://eprint.iacr.org/, vol. 254, 2006.

[11] *О. А. Логачев, С. В. Смышляев.* **Логический криптоанализ потокового шифра LILI-128.** Материалы 8-й Общероссийской конференции МаБИТ–09, МЦНМО, 2009.

думом[12] [13] [14]. Принципиальным отличием методов данного семейства от известных ранее является то, что объектами рассмотрения являются множества решений отдельных уравнений системы, из которых, путем последовательного согласования и склеивания, строится множество решений исходной системы.

Для всех известных алгоритмов решения систем булевых уравнений отсутствуют доказанные оценки трудоемкости по порядку меньшие, чем $2^{O(n)}$, где n — число булевых переменных в системе. В такой ситуации актуальными направлениями исследований являются: поиск классов систем булевых уравнений, которые могут быть решены с субэкспоненциальной от числа переменных трудоемкостью; разработка методов и алгоритмов, позволяющих эффективно решать системы уравнений определеленного вида.

Эффективные методы решения систем булевых уравнений позволяют уточнять оценку уязвимости систем защиты информации. Подобный анализ уязвимости может быть проведен в отношении программных или программно–аппаратных компонентов системы информационной безопасности, работа которых может быть описана системами булевых уравнений. При разработке новых методов и средств противодействия угрозам нарушения информационной безопасности, необходимо учитывать возможности применения эффективных методов решения систем булевых уравнений потенциальным нарушителем.

Целью диссертационной работы является разработка и исследование эффективных алгоритмов решения систем булевых уравнений, а также поиск классов систем булевых уравнений, допускающих сокращение трудоемкости их решения по сравнению с методом полного перебора. Это научное направление соответствует областям исследований, перечисленным в пп. 7, 9, 10 и 14 Паспорта специальности 05.13.19 — методы и системы защиты информации, информационная безопасность.

Для достижения поставленных целей были решены следующие новые задачи.

1. Разработка методов решения систем булевых уравнений с ис-

[12] *H. Raddum, I. Semaev.* **New technique for Solving Sparse Equation Systems.** Cryptology ePrint Archive, http://eprint.iacr.org/2006/475, 2006.

[13] *I. Semaev.* **Sparse Boolean equations and circuit lattices.** Designs, Codes and Cryptography, Springer Netherlands, p.349-364, 2011.

[14] *I. Semaev.* **Improved Agreeing-Gluing algorithm.** Proceedings of SCC'10, Royal Holloway, University of London, p.73–88, 2010.

пользованием ассоциативных принципов обработки информации.

2. Разработка методов решения систем булевых полиномиальных уравнений с использованием частичного опробования переменных и промежуточных критериев истинности решений.

3. Получение асимптотических оценок трудоемкости алгоритмов, реализующих разработанные методы, в общем случае и для систем специального вида.

4. Применение полученных результатов в криптографическом анализе потокового шифра LILI-128.

5. Разработка программной библиотеки для эмуляции работы ассоциативных вычислителей и проведение экспериментальных исследований трудоемкости разработанного алгоритма решения систем булевых уравнений при различных параметрах систем.

Методологической основой и научно-теоретической базой диссертации являются работы Б. Бухбергера, Ж.-К. Фажере, Н. Куртуа, И. Семаева о методах решения систем булевых уравнений, а также работы В.Ф. Колчина, В.Н. Сачкова и Г.В. Балакина, посвященные исследованию случайных систем булевых уравнений.

В диссертации применялись методы теории булевых функций, линейной алгебры, комбинаторного анализа, теории вероятностей и математической статистики.

Научная новизна исследования заключается в следующем. В диссертации предложены новые подходы к решению систем булевых уравнений. Впервые предложено использовать для решения систем булевых уравнений специальные ассоциативные вычислители. Помимо адресной организации памяти вычислительных машин, возможна организация доступа к ячейкам памяти по их содержимому. Организованная таким образом память называется ассоциативной (Content-addressable memory, CAM), когда операции с ячейками памяти осуществляются в зависимости от записанной в них информации. Такой подход к организации памяти эффективен, например, в задачах поиска. Подобные устройства активно используются в современных информационных технологиях. Например, в сетевых коммутаторах, позволяя за одну операцию по IP–адресу определять физический порт, по которому следует передать пакет.

Кроме того, ассоциативная память используется в диспетчерах кэша центрального процессора, базах данных, искусственных нейронных сетях, системах обнаружения вторжений и аппаратуре сжатия данных. Существуют различные современные подходы к технической реализации принципов ассоциативной памяти[15].

Для поиска решений системы булевых уравнений с использованием преимуществ ассоциативных вычислителей разработан алгоритм ассоциативного обхода дерева решений (АОДР). Предложена теоретико–вероятностная модель случайной системы булевых уравнений, характерная для систем, моделирующих работу блочных шифров. В рамках этой модели получена оценка математического ожидания трудоемкости решения систем булевых уравнений с использованием ассоциативных вычислителей, основанная на «связности» уравнений системы по переменным и зависящая от характера этой «связности». Найдены множества типов систем булевых уравнений на которых асимптотика математического ожидания трудоемкости решения систем булевых уравнений является субэкспоненциальной.

Разработан алгоритм частичного опробования и мономиальной совместности (ЧОМС) для решения систем булевых полиномиальных уравнений, основанный на опробовании части переменных системы и решении только тех систем булевых уравнений, полученных в результате опробования, которые удовлетворяют критерию мономиальной совместности. Предложена теоретико–вероятностная модель случайной системы булевых уравнений, характерная для систем, моделирующих работу потоковых шифров. В рамках данной модели для алгоритма ЧОМС получены оценки асимптотики математического ожидания трудоемкости решения систем булевых полиномиальных уравнений в общем виде и для квадратичных систем булевых уравнений.

Разработан метод восстановления ключа потокового шифра LILI-128 по известной шифрующей последовательности, оценены его трудоемкость и другие параметры. Определенным преимуществом предложенного метода, по сравнению с известными ранее методами восстановления ключа потокового шифра LILI-128, является возможность его применения в широком диапазоне длин известных шифрующих последовательностей.

[15] *K. Pagiamtzis, A. Sheikholeslami.* **Content-addressable memory (CAM) circuits and architectures: A tutorial and survey.** IEEE Journal of Solid-State Circuits, vol. 41, no. 3, 2006.

Для проведения экспериментальных исследований поведения ассоциативных вычислителей при решении систем булевых уравнений с различными параметрами была разработана программная библиотека, эмулирующая работу ассоциативных вычислителей. По результатам проведенных экспериментов проведено статистическое исследование работы ассоциативных вычислителей при решении систем булевых уравнений с различными параметрами.

На защиту выносятся:

— алгоритм АОДР поиска всех решений систем булевых уравнений с использованием ассоциативных вычислителей и верхняя оценка математического ожидания трудоемкости поиска решений системы булевых уравнений с помощью алгоритма АОДР, а также модифицированный алгоритм АОДР(S) поиска всех решений систем булевых уравнений с использованием ассоциативных вычислителей, размеры ячеек которых меньше числа переменных в системе уравнений;

— верхние асимптотические оценки средней трудоемкости алгоритма АОДР поиска всех решений систем булевых уравнений из множеств типов, выделяемых функциями специального вида, ограничивающими рост числа переменных в этих системах;

— алгоритм, реализующий метод ЧОМС решения систем булевых полиномиальных уравнений с опробованием переменных и исследованием редуцированных систем на мономиальную совместность и верхняя асимптотическая оценка математического ожидания трудоемкости поиска всех решений систем булевых полиномиальных уравнений, а также верхняя асимптотическая оценка математического ожидания трудоемкости поиска всех решений для квадратичных систем булевых полиномиальных уравнений;

— метод ЧОМС(L) определения ключа потокового шифра LILI–128 по известным открытому и шифрованному текстам и оценки его трудоемкости для различных объемов исходных данных;

— программная библиотека для эмуляции работы ассоциативных вычислителей и результаты экспериментальных исследований трудоемкости алгоритмов решения систем булевых уравнений с использованием ассоциативных вычислителей.

Теоретическая и практическая значимость. Диссертационная работа имеет теоретический характер. Полученные в диссертации результаты могут найти применение:

— при анализе и синтезе средств обеспечения информационной безопасности;

— при разработке методов криптографического анализа и оценки их эффективности;

— в учебном процессе для студентов–математиков в рамках специализации «Математическое и программное обеспечение защиты информации»;

— в научных центрах, занимающихся исследованиями в области обеспечения информационной безопасности.

Апробация работы. Основные результаты диссертации докладывались на следующих научных конференциях и семинарах:

— VI Молодежной научной школе по дискретной математике и её приложениям;

— XVII Международной научной конференции студентов, аспирантов и молодых ученых «Ломоносов–2010»;

— Научной конференции «Тихоновские чтения–2010»;

— Семинаре кафедры Математической кибернетики ВМК МГУ им. М.В. Ломоносова «Дискретная математика и математическая кибернетика», неоднократно (2010–2011гг.);

— Семинаре кафедры Математической кибернетики ВМК МГУ им. М.В. Ломоносова «Математические проблемы криптографического анализа», 2011г.;

— Семинаре по криптографии Института проблем информационной безопасности МГУ им. М.В. Ломоносова, 2011г.

Публикации. Основные положения и выводы диссертации опубликованы в 7 печатных работах [1–7], из них 2 статьи [1, 2] в изданиях из перечня ВАК РФ ведущих рецензируемых журналов.

Личный вклад автора. Все представленные в диссертации результаты получены лично автором.

Структура работы. Диссертация состоит из введения, 4 глав, библиографии и 3 приложений. Объем диссертации 116 страниц, включая 14 рисунков. Объем приложений 48 страниц, включая 3 рисунка. Библиография включает 62 наименования.

Содержание работы

Во ***введении*** обосновывается актуальность темы, формулируются цель и задачи исследования, указывается научная новизна, структура и практическая значимость работы, приведены основные результаты, полученные в работе, указаны публикации и апробация работы.

В главе 1 приводится обзор существующих подходов, методов и алгоритмов решения систем булевых уравнений. Рассмотрены теоретические вопросы сложности задачи решения системы булевых уравнений, перечислены различные задачи, возникающие в связи с системами уравнений, показана связь между такими задачами и их иерархия. Приведены варианты формулировок обобщения задачи поиска всех решений систем булевых уравнений.

Кратко описан метод решения систем полиномиальных уравнений, основанный на построении минимального редуцированного базиса Грёбнера идеала, описываемого системой уравнений. Приведены известные оценки трудоемкости классического алгоритма Бухбергера построения базиса Грёбнера, а также метод оценки трудоемкости построения базиса Гребнера идеала для почти всех систем булевых полиномиальных уравнений с помощью нового алгоритма F_5, предложенного Ж.–К. Фажере.

Другим важным направлением является решение систем булевых полиномиальных уравнений с помощью линеаризации и с помощью методов, основанных на линеаризации (XL, FXL и XSL). Описан метод линеаризации, состоящий в замене всех мономов степени выше первой новыми переменными и решении полученной линейной системы уравнений одним из известных методов (например, методом Гаусса) с последующей проверкой полученных решений на корректность (с точки зрения исходной системы). Обозначены основные приемы, предложенные Н. Куртуа с соавторами, позволяющие решать системы булевых уравнений в случае, когда количество уравнений в системе недостаточно для эффективного применения метода линеаризации.

Кратко рассмотрены возможности применения алгоритмов решения задач выполнимости КНФ (SAT) для решения систем булевых уравнений. Приведены примеры использования существующих SAT–решателей для решения систем булевых уравнений в работах отечественных и зарубежных ученых.

Далее в первой главе приведено краткое описание методов решения систем булевых уравнений с помощью согласования и склеивания специальных «комплексов» — объектов, описывающих наборы решения отдельных уравнений, входящих в систему. Определено понятие комплекса, а также операции над комплексами, применяемые в методах решения систем булевых уравнений с помощью согласования и склеивания. Приведен простейший вариант алгоритма, позволяющего решать системы булевых уравнений с помощью склеивания комплексов. Рассмотрены особенности операции склеивания комплексов с точки зрения трудоемкости.

В главе 2 рассмотрены вопросы применения специальных ассоциативных вычислителей для решения систем булевых уравнений. Описана математическая модель ассоциативного вычислителя — специализированного устройства, позволяющего производить операции над ячейками памяти в зависимости от содержимого данных ячеек, и приведено краткое описание модели такого устройства. Разработан использующий ассоциативные вычислители алгоритм АОДР поиска всех решений систем булевых уравнений, эффективно использующий преимущества ассоциативной организации памяти.

Поскольку для любого алгоритма поиска всех решений системы булевых уравнений в «худшем случае» число решений равно 2^n, то есть даже их перечисление может требовать экспоненциального от числа переменных в системе числа операций, то в качестве параметра, характеризующего эффективность предложенного алгоритма, была выбрана трудоемкость алгоритма в среднем, в рамках естественной теоретико–вероятностной модели со случайными функциями в системе уравнений. Предложенная теоретико–вероятностная модель описывает случайную систему булевых уравнений с заданными количеством уравнений, числом переменных и множествами существенных переменных для каждого из уравнений системы. При этом функции, определяющие уравнения системы выбираются случайно равновероятно из множества всех булевых функций с заданными параметрами. Такая теоретико–вероятностная модель может быть использована, например, для систем булевых уравнений, опи-

сывающих функционирование блочных шифров.

Для каждого множества $B(X_1, X_2, \ldots, X_m)$ всех систем булевых уравнений с заданными количеством уравнений m, количеством переменных $n = |\bigcup_{i=1}^{m} X_i|$ и множествами $X_1, X_2, \ldots, X_m$ существенных переменных для каждого уравнения системы может быть однозначно определена последовательность $\{d_1, d_2, \ldots, d_m\}$, задающая количество переменных в каждом уравнении, от которых не зависело ни одно из предыдущих уравнений системы. Каждое множество $B(X_1, X_2, \ldots, X_m)$ задает тип систем булевых уравнений с такими параметрами.

Доказана Лемма 2.5, утверждающая, что если в случайной системе булевых уравнений последовательность $\{d_1, d_2, \ldots, d_m\}$ является невозрастающей и, кроме того, число уравнений системы превышает число переменных, то существует номер $k_0 \in [1, m)$ такой, что математическое ожидание количества решений системы уравнений, составленной из первых $k = k_0$ уравнений исходной системы, является наибольшим для всех возможных k. В утверждении Леммы 2.6 определено максимальное значение математического ожидания количества решений системы уравнений, составленной из первых $k = k_0$ уравнений исходной системы, через функцию $\delta(x)$, ограничивающую сверху последовательность $\{d_1, d_2, \ldots, d_m\}$ и принимающую значение 1 хотя бы в одной точке x_0 отрезка $[1, m)$, как

$$\int_0^{x_0} \delta(x)\, dx - x_0.$$

С использованием лемм 2.5 и 2.6 доказано следующее утверждение.

Теорема 2.7. *Пусть множество $B(X_1, X_2, \ldots, X_m)$ таково, что: $d_1 > 1$, $m \geqslant n$, последовательность $d_1, d_2, \ldots, d_m$ невозрастает, существует невозрастающая функция $\delta(x)$: $\delta(x) \geqslant d(x), x \in (0, k_0]$ и существует x_0: $\delta(x_0) = 1$.*

Тогда математическое ожидание трудоемкости поиска всех решений случайной системы булевых уравнений из такого множества $B(X_1, X_2, \ldots, X_m)$ с помощью алгоритма АОДР не превосходит

$$c \cdot m \cdot 2^{\int_0^{x_0} \delta(x)\, dx - x_0},$$

где c — константа, которая не зависит от параметров системы.

Далее во второй главе определены классы множеств типов систем уравнений (Определения 2.8 и 2.9), для которых функция $\delta(x)$ такова, что становятся верны верхние субэкспоненциальные асимптотические оценки математического ожидания трудоемкости решения систем из такого набора типов систем уравнений (Теоремы 2.10 и 2.11) при стремлении числа переменных и количества уравнений в системе к бесконечности. Доказанные верхние оценки асимптотики математического ожидания трудоемкости составляют $O(n \cdot 2^{C^2 \cdot \frac{n}{\log n}})$ и $O(n \cdot 2^{D\sqrt{n}(\log D + \log n - 1)})$ при $n \to \infty$ для ограничивающих последовательность $\{d_1, d_2, \ldots, d_m\}$ функций $\delta(x) = C \cdot \sqrt{\frac{n}{\log n}} \cdot \frac{1}{\sqrt{x}}$ и $\delta(x) = D \cdot \frac{\sqrt{n}}{x+1}$ соответственно. Здесь C и D — любые константы.

Также в главе 2 рассмотрен алгоритм АОДР(S), являющийся модификацией алгоритма АОДР, предназначенной для применения в случаях ограниченности ёмкостных характеристик ассоциативных вычислителей. Получено Следствие 2.14 из Теоремы 2.7, доказывающее верхнюю оценку математического ожидания трудоемкости для модифицированного алгоритма АОДР(S), равную

$$c' \cdot n \cdot l \cdot m \cdot 2^{\int_0^{x_0} \delta(x)\,dx - x_0},$$

где c' — константа, которая не зависит от параметров системы, а l — максимальное количество переменных в одном уравнении.

В конце главы 2 описаны экспериментальные исследования средней трудоемкости алгоритмов АОДР, АОДР(F) и алгоритма полного перебора на ассоциативных вычислителях. Алгоритм АОДР(F) отличается от АОДР только тем, что после каждого шага алгоритма проводится проверка согласованности полученного частичного решения не только со следующим блоком, но и со всеми последующими ассоциативными блоками. Выбранный подход к экспериментальным исследованиям алгоритмов решения систем булевых уравнений с использованием ассоциативных вычислителей состоит в решении сформированных с использованием генератора псевдослучайных чисел систем булевых уравнений при различных параметрах решаемых систем. В рамках экспериментальных исследований получены статистические оценки математического ожидания трудоемкостей решения систем булевых уравнений с различными исходными параметрами для трех исследованных алгоритмов.

По результатам экспериментов удалось продемонстрировать, что трудоемкость в среднем при решении разреженных по переменным

систем булевых уравнений у алгоритмов АОДР и АОДР(F) ниже, чем у алгоритма полного перебора. Полученные экспериментальные данные не противоречат теоретическим результатам, полученным в диссертации.

В главе 3 исследованы вопросы построения эффективного алгоритма решения систем полиномиальных булевых уравнений. Введено понятие мономиальной совместности (Определение 3.1) как совместность линеаризованной системы и предложен метод ЧОМС поиска всех решений систем булевых полиномиальных уравнений, а также алгоритм ЧОМС, его реализующий. Метод ЧОМС состоит в опробовании части переменных системы, применении к получаемым при опробовании редуцированным системам уравнений промежуточного критерия мономиальной совместности для отбрасывания части редуцированных систем булевых полиномиальных уравнений и последующего решения только тех редуцированных систем, которые удовлетворяют критерию. Проверка мономиальной совместности проводится на основе известных алгоритмов решения систем линейных уравнений.

Трудоемкость алгоритма ЧОМС, в «худшем случае» является экспоненциальной от количества переменных системы, поэтому был выбран подход к оценке эффективности алгоритма ЧОМС, состоящий в оценке математического ожидания трудоемкости решения случайной системы полиномиальных булевых уравнений. Для получения такой оценки, в главе 3 введена теоретико–вероятностная модель, предполагающая равновероятный выбор системы булевых полиномиальных уравнений из всех возможных систем булевых полиномиальных уравнений заданной степени d от заданного количества переменных s и включающих в себя заданное количество уравнений m. Множество всех систем с такими параметрами $\Omega(m, s, d)$ образует множество элементарных исходов вероятностного пространства.

Такая теоретико–вероятностная модель, является моделью систем булевых полиномиальных уравнений со случайными коэффициентами при мономах и характерна, например, для систем булевых полиномиальных уравнений, описывающих работу фильтрующих генераторов. В рамках данной математической модели, доказано следующее утверждение.

Теорема 3.6. *Все коэффициенты при мономах в случайной системе, полученной из системы, случайно равновероятно выбранной из множества элементарных исходов $\Omega(m, s, d)$, в результате*

опробования переменных из множества X значениями некоторого двоичного вектора $\tilde{a}$, являются независимыми в совокупности случайными величинами, принимающими значения 0 *и* 1 *с вероятностью* $p = \frac{1}{2}$.

С помощью известного критерия Кронекера–Капелли совместности систем линейных алгебраических уравнений, а также доказанных в работах В.Ф. Колчина [16], В.Н. Сачкова [17] и Г.В. Балакина [18] утверждений, характеризующих распределение ранга случайной системы линейных булевых уравнений и вероятность совместности случайной системы линейных булевых уравнений, доказано следующее утверждение о характере изменения вероятности совместности случайной системы линейных булевых уравнений, при изменении размеров системы.

Лемма 3.10. *Для любых целых* $z \geqslant 0, l \geqslant 1, T \geqslant 1$ *верно:*

$$\mathcal{P}_T(l+z) \leqslant \frac{1}{2^{z-2}} \cdot \mathcal{P}_T(l),$$

где $\mathcal{P}_T(x)$ *— вероятность совместности системы линейных алгебраических уравнений, заданной матрицей* $[A|b]$*, причем* A *— случайная двоичная матрица с размерами* $T \times (T+x)$*, а* b *— случайный двоичный вектор–столбец правых частей длины* T.

Поскольку понятие мономиальной совместности системы булевых полиномиальных уравнений определено через совместность соответствующей линейной системы булевых уравнений, утверждение Леммы 3.10 может быть применено для оценки изменения вероятности мономиальной совместности случайных систем булевых полиномиальных уравнений при изменении параметров таких систем.

Для определения оптимального числа k опробуемых в алгоритме ЧОМС переменных используется выражение $k = s - n$, где n — наибольшее не превосходящее s целое положительное решение неравенства $m - \sum_{i=1}^{d} \binom{n}{i} > n + 2$, m — количество уравнений в системе, s — количество переменных в системе, а d — наибольшая алгебраическая степень полиномов системы. Доказано следующее утверждение, задающее верхнюю асимптотическую оценку матема-

[16] *В.Ф. Колчин.* **Случайные графы.** Москва:Физматлит, 2006, С. 256.

[17] *В.Н. Сачков.* **Системы случайных уравнений над конечными полями.** Труды по дискретной математике, № 8, 2004.

[18] *Г.В. Балакин.* **Системы случайных уравнений над конечным полем.** Труды по дискретной математике, № 2, 1998.

тического ожидания трудоемкости алгоритма ЧОМС поиска всех решений систем булевых полиномиальных уравнений.

Теорема 3.11. *Пусть, в условиях Теоремы 3.6, задана случайная система булевых полиномиальных уравнений из m полиномиальных уравнений степени не выше d от s неизвестных. Пусть n — наибольшее не превосходящее s целое положительное решение неравенства*

$$m - S_{n,d} > n + 2.$$

Пусть γ — случайная величина, равная трудоемкости решения с помощью алгоритма ЧОМС случайной системы булевых уравнений при опробовании $k = s - n$ переменных, заданных множеством X, $|X| = k$.

Тогда математическое ожидание случайной величины γ имеет верхнюю асимптотическую оценку $O(2^k \cdot m^3)$ при $m \to \infty$.

На основании утверждения Теоремы 3.11 доказана верхняя асимптотическая оценка математического ожидания трудоемкости поиска всех решений квадратичных систем булевых уравнений, равная $O(2^{s-\lfloor \frac{\sqrt{8m-7}-3}{2} \rfloor} \cdot m^3)$ при $m \to \infty$, где s — число неизвестных, а m — число уравнений в квадратичной системе булевых полиномиальных уравнений (Теорема 3.13).

В главе 4 рассмотрен потоковый шифр $LILI-128$, построенный на основе фильтрующего генератора с нерегулярным движением. Для него разработан комбинаторный метод определения ключа ЧОМС(L) основанный на использовании алгоритма ЧОМС. Получены оценки трудоемкости восстановления ключа шифра $LILI-128$ по известным открытому и шифрованному тексту. При длине известной шифрующей последовательности $2^{17,5}$ бит, трудоемкость в среднем восстановления ключа составляет 2^{100} битовых операций, а необходимый для этого объем памяти составляет $2^{42,6}$ бит. При этом, наилучший известный на сегодняшний день алгебраический метод анализа требует 2^{102} битовых операций и 2^{40} бит памяти, а количество бит известной шифрующей последовательности не должно быть меньше, чем 2^{18}.

В отличие от известных ранее методов анализа потокового шифра $LILI-128$, предложенный в главе 4 метод ЧОМС(L) применим при меньших объемах известной шифрующей последовательности. Кроме того, при соответствующем изменении подготовительного этапа, на котором формируется система булевых полиномиальных уравнений, метод ЧОМС(L) может быть применен для криптографического анализа любого потокового шифра данного вида.

В приложении А приведен алгоритм АОДР(VS), являющийся модификацией алгоритма АОДР для применения в случаях, когда размеры ячеек ассоциативных вычислителей меньше, чем максимальное количество переменных, задействованных в отдельном уравнении решаемой системы. Также в приложении А приведен алгоритм ЧОМС(А) поиска всех решений систем булевых полиномиальных уравнений. Алгоритм ЧОМС(А) повторяет подход, реализованный в алгоритме ЧОМС, но помимо опробования переменных и использования промежуточных критериев истинности решений, дополнительно использует возможности ассоциативных вычислителей.

В приложении Б приведены численные результаты экспериментов по исследованию средней трудоемкости работы алгоритмов полного перебора, АОДР и АОДР(F).

Приложение В содержит тексты программной библиотеки для эмуляции работы ассоциативного вычислителя и проведения экспериментальных оценок трудоемкости различных алгоритмов поиска решений систем булевых уравнений.

Заключение

В диссертации получены следующие основные результаты.

1. Разработан алгоритм АОДР поиска всех решений систем булевых уравнений, эффективно использующий преимущества ассоциативных вычислителей, получена верхняя оценка математического ожидания трудоемкости поиска решений системы булевых уравнений с помощью алгоритма АОДР, предложен алгоритм АОДР(S) поиска всех решений систем булевых уравнений с использованием ассоциативных вычислителей, размеры ячеек которых меньше числа переменных в системе уравнений и получена верхняя оценка математического ожидания трудоемкости поиска решений системы булевых уравнений с помощью алгоритма АОДР(S).

2. Получены верхние асимптотические оценки средней трудоемкости алгоритма АОДР поиска всех решений систем булевых уравнений из множеств типов, выделяемых функциями специального вида, ограничивающими рост числа переменных в этих системах.

3. Разработана программная библиотека для эмуляции работы ассоциативных вычислителей и исследования алгоритмов решения систем булевых уравнений, получены результаты экспериментальных исследований трудоемкости алгоритмов решения систем булевых уравнений с использованием ассоциативных вычислителей, которые не противоречат теоретическим результатам, полученным в диссертации.

4. Разработан метод и алгоритм ЧОМС решения систем булевых полиномиальных уравнений с опробованием переменных и исследованием редуцированных систем на мономиальную совместность, получены верхняя асимптотическая оценка математического ожидания трудоемкости поиска всех решений систем булевых полиномиальных уравнений и верхняя асимптотическая оценка математического ожидания трудоемкости поиска всех решений для квадратичных систем булевых полиномиальных уравнений.

5. Разработан метод ЧОМС(L) определения ключа потокового шифра LILI–128 по известным открытому и шифрованному текстам и получены оценки его трудоемкости для различных объемов исходных данных.

Полученные в диссертационной работе результаты могут быть использованы при решении и оценке трудоемкости решения систем булевых уравнений, моделирующих процессы, протекающие в информационных системах, что, в свою очередь, позволит решать задачи анализа эффективности систем обеспечения информационной безопасности, задачи аудита состояния объекта, находящегося под воздействием угроз информационной безопасности, задачи анализа рисков нарушения информационной безопасности и уязвимости процессов обработки информации и другие задачи в сфере защиты информации.

Благодарности. Автор благодарит научного руководителя к.ф.-м.н, с.н.с Логачева Олега Алексеевича за постановку задачи, постоянное внимание и помощь в работе. Автор выражает глубокую благодарность заведующему кафедрой Математической кибернетики профессору Алексееву Валерию Борисовичу и всем сотрудникам кафедры за творческую атмосферу, способствующую научной работе.

Список литературы

[1] ***А.С. Мелузов*. Использование ассоциативных принципов обработки информации для построения алгоритмов решения систем булевых уравнений. Журнал вычислительной математики и математической физики, 50, № 11, 2010, С.2028–2044.**

[2] ***А.С. Мелузов*. Построение эффективных алгоритмов решения систем полиномиальных булевых уравнений методом опробования части переменных. Дискретная математика, 23, № 4, 2011, С.66–79.**

[3] *А.С. Мелузов*. Оценка сложности применения символьных методов в криптоанализе алгоритма ГОСТ 28147-89. Сборник работ молодых ученых факультета ВМК МГУ, № 4, 2007, С.109–112.

[4] *А.С. Мелузов*. Сложность применения символьных методов в криптоанализе алгоритма ГОСТ 28147-89. Материалы VI научной школы по дискретной математике и её приложениям (Москва, 16-21 апреля 2007 г.), 2007, С.20–26.

[5] *А.С. Мелузов*. Алгоритмы решения систем булевых уравнений с использованием ассоциативных принципов обработки информации. Материалы Международного молодежного научного форума «ЛОМОНОСОВ-2010», 2010, С.35–36.

[6] *А.С. Мелузов*. Построение эффективных алгоритмов решения систем полиномиальных уравнений над полем GF(2) методом частичного опробования переменных. Научная конференция Тихоновские чтения, 2010, С.12–13.

[7] *А.С. Мелузов*. О криптоанализе LILI-128, основанном на частичном опробовании и мономиальной совместности систем полиномиальных уравнений. Сборник работ молодых ученых факультета ВМК МГУ, № 8, 2011, С.99–107.