На правах рукописи

Подколзин Вадим Владиславович

МОДЕЛИРОВАНИЕ СИСТЕМ НА ОСНОВЕ ОДНОСТОРОННИХ РЮКЗАЧНЫХ ОТОБРАЖЕНИЙ

Специальность 05.13.18 – математическое моделирование, численные методы и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание учёной степени кандидата физико-математических наук

Краснодар – 2011

Работа выполнена на кафедре информационных технологий ГОУ ВПО «Кубанский государственный университет»

Научный руководитель:	доктор физико-математических наук, доцент Осипян Валерий Осипович
Официальные оппоненты:	доктор физико-математических наук, доцент Зеленков Геннадий Анатольевич
	кандидат физико-математических наук Василенко Вера Викторовна
Ведущая организация:	Южный федеральный университет (г. Ростов-на-Дону)

Защита состоится 14 октября 2011 г. в 14-00 на заседании диссертационного совета Д 212.101.17 в Кубанском государственном университете по адресу: 350040, Краснодар, ул. Ставропольская, 149, ауд. 231.

С диссертацией можно ознакомиться в научной библиотеке Кубанского государственного университета, с авторефератом – на сайте http://www.kubsu.ru

Автореферат разослан 12 сентября 2011 г.

Учёный секретарь
диссертационного совета В.Ю. Барсукова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

С момента возникновения в начале 1970-х гг. понятие «*NP*-полная задача» определяет трудности, с которыми приходится сталкиваться разработчикам алгоритмов при решении задач постоянно возрастающей размерности и усложняющейся структуры. Большинство таких задач, часто встречающихся в математике, теоретическом программировании и исследовании операций, являются *NP*-полными.

Первые результаты о труднорешаемости задач – классические результаты о неразрешимости – были получены А. Тьюрингом. Он доказал, что для некоторых задач не существует алгоритма их решения. Основными объектами теории являются: класс *NP* всех переборных задач и класс *P* переборных задач, разрешимых за полиномиальное время на машине Тьюринга.

Большой практический мировой опыт решения дискретных задач дает основание считать, что *NP*-полные задачи и задачи из класса *P* сильно отличаются по трудоемкости решения, но в строгом смысле до сих пор это различие не доказано. Это, в частности, объясняется тем, что классы *P* и *NP* определяются с помощью понятия времени работы вычислительного устройства с потенциально неограниченной памятью. Основополагающий характер различий между классами *P* и *NP* впервые обсуждался в работах А. Кобхэма и Д. Эдмондса. В частности, Д. Эдмондс, отождествляя полиномиальные алгоритмы с «хорошими» алгоритмами, высказал предположение, что некоторые задачи целочисленного программирования невозможно решить такими «хорошими» алгоритмами.

В классе *NP* выявлены так называемые универсальные *NP*-полные задачи, к которым полиномиально сводится любая задача из *NP*. В этом смысле универсальные задачи определяют эталон сложности. В настоящее время установлена универсальность многих задач, эквивалентных между собой относительно полиномиальной сводимости. Если бы удалось доказать, что некоторая *NP*-полная задача принадлежит классу *P*, то тем самым было бы доказано, что $P = NP$, и можно было бы надеяться на построение эффективных алгоритмов для различных классов дискретных задач. Если же классы *P* и *NP* различны, то

необходимо разрабатывать эффективные алгоритмы для все более узких классов задач.

Проблеме вычислительной сложности, представления и преобразования данных в современной научной литературе посвящены исследования А. Тьюринга, С. Кука, А. Кобхэма, Д. Эдмондса, В. Кли, Г. Минти, Н. Заде, М. Гэри, Д. Джонсона, Д. Хартманиса, Р. Стирза, А. Майера, Л. Стокмейера, М. Фишера, М. Рабина, У. Диффи, М. Хеллмана, Р. Меркле, А. Шамира, К. Вилиамса, Р. Карпа, В. Чора, Р. Райвеста, Е. Брикеля, А. Ростовцева, Е. Маховейко, Р. Лидла, Г. Нидеррайтера, Л. Адлемана и др. По мнению авторов, применение *NP*-полных задач для моделирования систем доступности, целостности и безопасности данных является обоснованным. Качество таких систем существенно зависит как от самой задачи, так и от способа ее применения.

В силу теоретических положений построения математических моделей в диссертационной работе не рассматриваются конкретная физическая природа, содержание и назначение объектов, а они заменяются соответствующими моделями. Под моделью понимается способ описания объекта, процесса или явления, отражающий существенные с точки зрения решаемой задачи факторы или параметры.

Отметим, что проблема теоретической информатики о существовании класса *NP*-полных задач тесно связана с вопросом о существовании односторонних функций. Под односторонней понимается функция, значение которой для любого входного значения вычисляется за полиномиальное время, но не существует полиномиального алгоритма нахождения аргумента при заданном значении функции. Ни для одной функции не удалось доказать, что она трудна для обращения, хотя многие функции кажутся таковыми. Найден ряд комбинаторных и алгебраических задач, которые являются в среднем полными при равномерном распределении входов.

Использование в основе многих моделей и систем односторонних функций позволило эффективно решать задачи в областях теории кодирования, алгоритмизации, WEB-программирования, баз данных и защиты информации. Для практического применения алгоритмов таких моделей важна их

безопасность, т.е. сложность обращения, которая зачастую определяется некоторой вычислительно трудной задачей, лежащей в ее основе. Подобные задачи имеют решения, однако их нахождение требует больших вычислительных ресурсов и временных затрат. Следовательно, выбор подходящей трудно решаемой задачи, в частности, *NP*-полной задачи, позволяет моделировать систему на должном уровне безопасности.

К числу таких задач относится рассматриваемая в данном исследовании *NP*-полная задача о рюкзаке.

Основным аспектам использования *NP*-полной задачи о рюкзаке в преобразовании информации посвящены работы М. Хеллмана, Р. Меркле, А. Шамира, Н. Заде, В. Чора, Р. Райвеста, Е. Брикеля, В. Осипяна и др. Анализ трудов отечественных и зарубежных авторов показывает, что наиболее распространенными моделями, основанными на рюкзачных векторах, являются ассиметричные модели с открытым ключом.

Безопасность алгоритмов связана со сложностью решения трудных задач, лежащих в их основе, и вероятностью нахождения ранее неизвестных эффективных методов их решения. Данное понятие включает два аспекта – трудоемкость восстановления методов отображения данных на основе использования лучшего известного метода, например лучшего известного метода решения трудной задачи, и вероятность появления ранее неизвестных эффективных способов решения этой задачи. Первое значение должно быть достаточно большим, а второе – достаточно малым.

Один из способов повышения качества систем на основе односторонних функций – построение моделей, анализ (поиск методов нахождения обратного преобразования) которых требует одновременного решения нескольких независимых вычислительно трудных задач. В этом случае вероятность появления эффективных способов их компрометации резко уменьшается, что существенно повышает их применимость. Увеличение уровня безопасности становится возможным за счет использования полиалфавитных отображений, позволяющих уменьшить эффективность частотного и статистического анализа. Совместное использование нескольких односторонних функций и основанных на них моделей позволяет увеличить срок эффективного применения соответствующих систем.

В связи с изложенным диссертационное исследование, посвященное построению моделей односторонних отображений, основанных на *NP*-полных задачах с использованием методов хеш-функций, блочных преобразований, полиалфавитных и симметричных систем, относится к своевременным и **актуальным.**

Целью диссертационной работы является разработка математических моделей, методов и механизмов одностороннего отображения числовых данных на основе рюкзачных векторов, обращение которых требует одновременного решения нескольких *NP*-полных задач, задач дискретной интерполяции и разбиений числовых значений при условии многократного изменения параметров отображения в рамках одного набора данных, что обеспечивает повышение качества систем, в которых они применяются.

Для достижения указанной цели в диссертационной работе были поставлены и решены следующие частные задачи:

1) изучить свойства рюкзачных векторов и множества числовых значений, разбиение которых по компонентам вектора допустимо;

2) исследовать применимость использования рюкзачного вектора для представления элементов заданного множества;

3) определить верхнюю оценку сложности решения задачи о рюкзаке для рюкзачного вектора, обладающего заданными свойствами;

4) разработать математические модели односторонних числовых рюкзачных отображений, обладающих свойствами блочных, полиалфавитных и симметричных отображений;

5) разработать математические модели полиалфавитных систем преобразования данных с открытым ключом на основе односторонних рюкзачных отображений.

Методы исследования. В исследовании использованы аппарат и методы линейной алгебры, теории чисел, теории сложности, математического анализа, математической статистики, теории вероятности и теории информационной безопасности.

Научная новизна. В процессе выполнения диссертационной работы получены следующие научные результаты:

1) предложены методы анализа и определены свойства рюкзачного вектора на основе его вариации;

2) разработан численный метод построения инъективных рюкзачных векторов заданной размерности, в компонентах которого выражаются элементы базового числового множества;

3) разработаны математические модели инъективных односторонних отображений на основе динамически генерируемых рюкзачных векторов и построены алгоритмы функционирования систем на их основе;

4) предложены математические модели инъективных односторонних отображений на основе динамически генерируемых рюкзачных векторов для обратной задачи о рюкзаке и построены алгоритмы функционирования систем на их основе.

Обоснованность и достоверность научных положений обеспечены анализом современных исследований в данной области, подтверждены математическими доказательствами, результатами вычислительных экспериментов, а также апробацией основных теоретических достижений в печатных трудах и докладах на всероссийских и международных научно-практических конференциях.

Теоретическая и практическая значимость работы. Основные результаты, полученные в работе, являются достоверными и имеют как теоретическую, так и практическую значимость.

Теоретическая значимость работы состоит в следующем:

1) предложены математические методы анализа свойств рюкзачных векторов заданной размерности;

2) разработаны методы построения инъективных рюкзачных векторов с заданными условиями;

3) определены способы задания односторонних рюкзачных отображений на основе функциональных и процедурных зависимостей;

4) разработаны математические модели систем преобразования числовой информации на основе функционально и процедурно-определяемых рюкзачных векторов.

Практическая значимость исследования определяется:

1) применимостью предложенных методов к решению задачи анализа рюкзачных односторонних отображений;

2) применимостью предложенных математических моделей и методов к решению задач построения систем на основе односторонних функций с заданными характеристиками;

3) разработкой программной системы с открытым ключом и динамическим рюкзачным вектором.

На защиту выносятся:

1. Математическая модель описания элементов множества числовых значений, выражаемых в рюкзачном векторе.

2. Оценка значения верхней границы решений задачи о рюкзаке для векторов с заданными свойствами.

3. Численный метод построения инъективного рюкзачного вектора с заданными свойствами.

4. Математические модели односторонних отображений на основе динамически генерируемых рюкзачных векторов.

5. Модели системы преобразования числовой информации, основанные на моделях с динамически генерируемыми рюкзачными векторами, и алгоритмы их функционирования.

Апробация и внедрение результатов исследования проходили на базе Кубанского государственного университета, осуществлялись в форме научных докладов на XI Всероссийском симпозиуме по прикладной и промышленной математике (Кисловодск, 2010), VII Международной конференции «Алгебра и теория чисел: современные проблемы» (Тула, 2010), VI Всероссийской научно-практической конференции «Математические методы и информационно-технические средства» (Краснодар, 2010), I Всероссийской молодежной конференции по проблемам информационной безопасности «Перспектива-2009» (Таганрог, 2009), XIII Международной научной конференции им. Решетнева, (Красноярск, 2009), X Всероссийском симпозиуме по прикладной и промышленной математике (Санкт-Петербург, 2009), V Всероссийской научно-практической конференции «Математические методы и информационно-технические средства» (Краснодар, 2009), III Международной научно-практической конференции «Актуальные проблемы безопасности информационных технологий» (Красноярск, 2009), Международной научной конференции «Современные проблемы математики, информатики и управления» (Алматы, 2008).

Результаты исследования внедрены и используются в рамках учебного процесса в Кубанском государственном университете, Краснодарском университете МВД России, а также в программных системах ЗАО «ЭкоГрин».

На основе разработанных моделей и алгоритмов реализовано программное приложение преобразования данных «Программный комплекс преобразования информации «РСЗИ ДГВ[ц]», зарегистрированное в Реестре программ для ЭВМ под номером 2011610789 от 14 января 2011 г.

Публикации. Основные результаты диссертационной работы изложены в 20 публикациях, 7 из которых опубликованы в ведущих рецензируемых журналах, входящих в перечень рекомендуемых ВАК, в докладах и тезисах докладов на международных и всероссийских научно-практических конференциях.

Структура и объем работы. Диссертационная работа изложена на 155 машинописных страницах, включает 3 главы, 18 рисунков, 5 таблиц, список литературы (105 наименования).

Тема и содержание диссертационного исследования **соответствует требованиям паспорта специальности 05.13.18 –** математическое моделирование, численные методы и комплексы программ и соответствуют следующим областям исследования паспорта специальности: 2. Развитие качественных и приближенных аналитических методов исследования математических моделей; 4. Реализация эффективных численных методов и алгоритмов в виде комплексов проблемно-ориентированных программ для проведения вычислительного эксперимента; 5. Комплексные исследования научных и технических проблем с применением современной технологии математического моделирования и вычислительного эксперимента; 8. Разработка систем компьютерного и имитационного моделирования.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснованы важность и актуальность темы диссертации, сформулированы цели исследования и решаемые задачи, определена научная новизна и приведено краткое содержание диссертационного исследования по главам.

В **первой главе** проведён анализ известных теоретических и практических решений проблем, основанных на *NP*-полных задачах, рассмотрены основные проблемы теории и практики односторонних функций. Подчёркнуто, что в основе большинства задач теории сложности, алгоритмизации, WEB-программирования, баз данных, передачи и защиты информации лежит односторонняя функция. Под односторонней функцией понимается отображение, значение которого для любого входного значения вычисляется за полиномиальное время, но поиск обратного отображения связан либо с *NP*-полной задачей, либо эффективный алгоритм, реализующий обратное отображение, еще не известен.

В главе дан обзор наиболее известных способов использования *NP*-полной задачи о рюкзаке, а именно систем с открытым ключом. В рюкзачных системах с открытым ключом в качестве открытого ключа используют рюкзачный вектор преобразованный секретным методом. Метод поиска векторов, описывающих отображение исходных данных во множество значений для таких систем определяется прежде всего сложностью модификации рюкзачного вектора. В частности, для системы Меркле–Хеллмана найден эффективный метод анализа, а для системы Чор–Райвестра – нет.

Дальнейшее развитие рюкзачные системы получили в работах В. О. Осипяна, где используется расширение значений коэффициентов до значений из Z_p. Показано, что обобщенные рюкзачные вектора имеют свойства, аналогичные стандартным (с коэффициентами из множества {0, 1}) рюкзакам. Но для модели M_G с обобщенным рюкзачным вектором требуются дополнительные затраты при анализе, а общее решение задачи о рюкзаке K_G имеет оценку сложности p^n. Развитие данного подхода позволило определить системы на основе так называемых универсальных рюкзаков, для каждого компонента которых определяется свой диапазон значений коэффициентов, и функциональных рюкзаков, представляющих собой набор целочисленных функций.

Определение рюкзачного вектора как набора функциональных зависимостей является наиболее интересным, но мало изученным направлением моделирования систем на основе рюкзачных векторов. Основная сложность в данном направлении заключается

в определении функций, составляющих вектор, с целью достижения заданных свойств.

Несмотря на простоту реализации алгоритмов на основе задачи о рюкзаке, ее использование вне систем с открытым ключом практически отсутствует. Методы применения рюкзачного вектора к исходному набору данных по своим характеристикам близки к блочным системам преобразования информации, а использование сверхрастущих рюкзачных векторов позволяет говорить и о признаках симметричных моделей.

Подобно хешированию, выражение числовых значений в компонентах стандартного рюкзачного вектора представляет собой отображение входного набора данных произвольной длины в выходную битовую последовательность фиксированной длины. В рамках главы анализируются свойства хеш-функций и их применение. Хеш-функции представляют собой «почти» инъективные отображения в том смысле, что если у двух наборов данных хеш-коды разные, то эти наборы различны, а если хеш-коды одинаковые – наборы, возможно, одинаковы. В общем случае однозначного соответствия между исходными данными и хеш-кодом нет в силу того, что количество значений хеш-функций меньше, чем мощность множества наборов данных. Первоначально хеш-функции предназначались для организации методов поиска. Развитие информационного обмена по каналам связи привело к использованию хеш-функций в задачах контроля целостности переданных данных, а также в области криптографии.

Способность системы противостоять методам поиска функции, лежащей в ее основе, называется стойкостью. Количественно стойкость измеряется как сложность наилучшего алгоритма, приводящего к успеху с приемлемой вероятностью. В главе приводится описание наиболее распространенных методов поиска функций преобразований числовых значений.

Во **второй главе** приводятся результаты исследования автора рюкзачных векторов и множества числовых значений, в них представляемых.

Обобщенная задача о рюкзаке K_G для заданных $w \in N$ и вектора $A=(a_1, a_2, \ldots, a_n)$, где $a_i \in N$, $i = 1, \ldots, n$, имеет решение в Z_p, если существует решение x уравнения

$$Ax^T = w,\ x \in Z_p^n. \qquad (1).$$

Рюкзачный вектор $A = (a_1, a_2, \ldots, a_n)$ – инъективен, если для любого натурального w уравнение (1) имеет не более одного решения. Такие рюкзачные вектора наиболее перспективны для исследования, так как допускают однозначность нахождения решения x и выражения w в условиях (1).

Определение 2.1. Вариацией вектора $A = (a_1, a_2, \ldots, a_n)$ $(a_i \in N, i = 1, \ldots, n)$ в Z_p называется вектор $\Delta A = (\delta_1, \delta_2, \ldots, \delta_n)$, для компонентов которого выполняются соотношения

$$\delta_1 = a_i, \delta_i = a_i - \sum_{i=1}^{j-1}(p-1)a_i, j=2, \ldots, n.$$

Обозначим через $\mu_p(A)$ множество значений w, для которых уравнение (1) имеет решение в Z_p.

Определение 2.2. Последовательность $W_{\mu_p(A)} = (w_0, w_1, w_2, \ldots, w_{p^n-1})$, где $w_i = Ax_i^T$, $x_i = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $i = \sum_{j=1}^{n} \alpha_j p^{j-1}$, $i = 0, \ldots, p^n-1$, называется последовательностью значений вектора A в Z_p.

Обозначим как $\Delta W_{\mu_p(A)}$ последовательность $(m_1, m_2, \ldots, m_{p^n-1})$, где $m_i = w_i - w_{i-1}$ $(w_i \in W_{\mu_p(A)}, i=1, \ldots, p^n-1)$. Пусть $A_n = (a_1, a_2, \ldots, a_n)$ – рюкзачный вектор. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ получен из A_n добавлением компонента a_{n+1}. Тогда в последовательности $\Delta W_{\mu_p(A_{n+1})} = (\Delta W_{\mu_p(A_n)}, \delta_{n+1}, \Delta W_{\mu_p(A_n)}, \delta_{n+1}, \Delta W_{\mu_p(A_n)}, \ldots, \delta_{n+1}, \Delta W_{\mu_p(A_n)})$ подпоследовательность $\delta_{n+1}, \Delta W_{\mu_p(A_n)}$ повторяется $p-1$ раз.

В диссертационной работе исследуются свойства стандартных рюкзачных векторов и множества их значений, как наиболее широко используемые на практике. Сформулированы и доказаны теоремы:

Теорема 2.1. Пусть $A_n = (a_1, a_2, \ldots, a_n)$ – инъективный возрастающий рюкзачный вектор в Z_2 размерности n $(n \geq 2)$. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ – вектор, полученный из A_n добавлением компонента a_{n+1}, и $\Delta A_{n+1} = (\delta_1, \delta_2, \ldots, \delta_n, \delta_{n+1})$ – вариация вектора A_{n+1}. Тогда если $\delta_{n+1} > 0$, то $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ является инъективным возрастающим рюкзачным вектором в Z_2 размерности $n+1$.

Теорема 2.2. Пусть $A_n = (a_1, a_2, \ldots, a_n)$ – инъективный возрастающий рюкзачный вектор в Z_2 размерности n $(n \geq 2)$. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ – вектор, полученный из A_n добавлением

компонента a_{n+1}, и $\Delta A_{n+1} = (\delta_1, \delta_2, \ldots, \delta_n, \delta_{n+1})$ – вариация вектора A_{n+1}.

Тогда $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ является инъективным возрастающим рюкзачным вектором в Z_2 размерности $n + 1$, если выполняются следующие условия:

a) $-\sum_{j=1}^{n-1} \alpha_j < \delta_{n+1}$;

b) $|\delta_{n+1}| \notin W_{\mu_3(A_{n-1})}$.

Обобщение полученных результатов на пространство Z_p позволило описать свойства $\mu_p(A)$, $W_{\mu_p(A)}$ и $\Delta W_{\mu_p(A)}$, а также сформулировать и доказать критерии построения инъективных рюкзачных векторов в Z_p.

Теорема 2.3. Пусть $A_n = (a_1, a_2, \ldots, a_n)$ – инъективный рюкзачный вектор в Z_p размерности n $(n \geq 2)$, где $a_i \in N$, $i = 1, \ldots, n$. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ получен из A_n добавлением компонента $a_{n+1} \in N$, $\Delta A_{n+1} = (\delta_1, \delta_2, \ldots, \delta_n, \delta_{n+1})$ – вариация вектора A_{n+1}. Тогда если $\delta_{n+1} > 0$, то $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ – инъективный рюкзачный вектор в Z_p.

Теорема 2.4. Пусть $A_n = (a_1, a_2, \ldots, a_n)$ – инъективный возрастающий рюкзачный вектор в Z_p размерности n $(n \geq 2)$, где $a_i \in N$, $i = 1, \ldots, n$. Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ получен из A_n добавлением компонента $a_{n+1} \in N$, $\Delta A_{n+1} = (\delta_1, \delta_2, \ldots, \delta_n, \delta_{n+1})$ – вариация вектора A_{n+1} и $\delta_{n+1} < 0$.

Вектор $A_{n+1} = (a_1, a_2, \ldots, a_n, a_{n+1})$ является инъективным возрастающим рюкзачным в Z_p, если выполняются условия:

a) $a_n - \sum_{j=1}^{n} (p-1)\alpha_j < \delta_{n+1}$;

b) $|\delta_{n+1}| \notin W_{\mu_{2p-1}(A_n)}$.

В диссертации исследуются взаимные свойства векторов: определяются и исследуются понятия совместимости, несовместимости, несовпадения и сравнения рюкзачных векторов. Два вектора A и B совместимы, если $\mu_p(A) \cap \mu_p(B) \neq \emptyset$. Коэффициент совместимости $\|(A, B)\|$ двух различных совместимых в Z_p рюкзачных векторов A и B определяет наибольшее возможное значение количества выражений произвольного значения w в Z_p при их совместном использовании. Вводится понятие подрюкзака (операция $\prec$), когда всякий компонент одного вектора является компонентом другого.

Исследуются свойства таких рюкзаков, формулируется и доказывается критерий неинъективности.

Лемма 2.1. Рюкзачный вектор $A = (a_1, a_2, \ldots, a_n)$ размерности n, все компоненты которого различны ($\forall i, j\ a_i \neq a_j, i \neq j$), не является инъективным тогда и только тогда, когда существуют два различных совместимых в Z_p вектора B и C таких, что $B \prec A$ и $C \prec A$.

Определение 2.3. Два возрастающих рюкзачных вектора $A = (a_1, a_2, \ldots, a_n)$ и $B = (b_1, b_2, \ldots, b_k)$, векторы вариаций ΔA и ΔB которых отличаются только значением первого компонента, называются изоморфными и обозначают $A \approx B$, если существует изоморфизм f: $\mu_p(A) \rightarrow \mu_p(B)$.

Изоморфизм рюкзачных векторов является отношением эквивалентности. В каждом классе существует базовый вектор, для которого коэффициент изоморфизма ε с любым другим вектором этого класса неотрицательный. Произвольному отображению на основе рюкзачного вектора A можно поставить в соответствие отображение на основе базового вектора его класса эквивалентности с целью оптимизации ресурсов в практической реализации.

В главе сформулированы требования к модификации множества значений с целью увеличения сложности задачи поиска параметров рюкзачного отображения исходя из заданной размерности вектора. Сформулирована и доказана:

Лемма 2.2. Пусть $A = (a_1, a_2, \ldots, a_n)$ – инъективный рюкзачный вектор в Z_p размерности n и $t \neq 0$ – целое число. Тогда не существует инъективного рюкзачного вектора размерности n, посредством компонентов которого в Z_p выражаются все элементы множества $\{w+t \mid w \in \mu_p(A)\}$.

Определение 2.4. Два рюкзачных вектора $A = (a_1, a_2, \ldots, a_n)$ и $B = (b_1, b_2, \ldots, b_k)$ подобны, будем обозначать $A \cong B$, если существует взаимно однозначное отображение f: $A \rightarrow B$ такое, что:

1) $\forall a \in A\ f(Ca) = Cf(a)$, где $C \in Z$;

2) $\forall a', a'' \in A$ выполняется $f(a'+a'') = f(a') + f(a'')$.

Показана равнозначная стойкость математических моделей на основе подобных рюкзачных векторов.

Существенной характеристикой любой системы на основе односторонней функции является величина затрат времени и ресурсов при ее анализе, которая прежде всего определяется множеством возможных решений задачи обращения. Сформулирована и доказана следующая лемма:

Лемма 2.3. Пусть для возрастающего вектора $A_n = (a_1, a_2, \ldots, a_n)$ размерности n множество $\Lambda = \{(B_k, C_k)\}$ образует множество всех пар различных совместимых в Z_p рюкзаков B_k и C_k таких, что $B_k \prec A$, $C_k \prec A$ и $B_k \leq C_k$. Тогда для рюкзачного вектора A уравнение (1) в Z_p имеет не более чем $\max(1, \prod_{i=1}^{|\Lambda|} \| B_i, C_i \|)$ решений.

Обобщение полученных результатов позволило определить верхнюю границу количества решений задачи о рюкзаке для векторов произвольного вида и доказать следующую теорему:

Теорема 2.5. Пусть для рюкзачного вектора $A_n = (a_1, a_2, \ldots, a_n)$ размерности n множество $\Lambda = \{(B_k, C_k)\}$ образует множество пар различных совместимых в Z_p рюкзаков B_k и C_k таких, что $B_k \prec A$, $C_k \prec A$ и $B_k \leq C_k$. Кроме того, вектор A имеет r различных повторяющихся компонентов, причем первый из них повторяется m_1 раз, второй – m_2, …, r-й – m_r. Тогда уравнение (1) для рюкзачного вектора A имеет решений не более чем

$$\max\left(1, \prod_{i=1}^{|A|} \| B_i, C_i \|\right) \prod_{j=1}^{r} \left(\sum_{k=0}^{\left\lfloor \frac{m_j \cdot (p-1)}{2} \right\rfloor} (-1)^k C_{m_j}^{k} C_{m_j - k \cdot \left\lfloor \frac{m_j \cdot (p-1)}{2} \right\rfloor - kp}^{m_j - 1} \right).$$

Результатом исследования свойств $\Delta W_{\mu_p(A)}$ является численный метод поиска рюкзачного вектора по заданному множеству значений соответствующей односторонней функции, в основе которого лежат статистические свойства подпоследовательностей $\Delta W_{\mu_p(A)}$.

Для заданной размерности рюкзачного вектора A определяется последовательность специального вида $S_n = ((k_1, s_1), (k_2, s_2), \ldots)$, где s_i – сумма элементов подпоследовательности $\Delta W_{\mu_p(A)}$, где k_i – количество вхождений подпоследовательности элементов s_i в $\Delta W_{\mu_p(A)}$, $k_i \leq k_j$, $i<j$. Для заданной последовательности значений $W' = \{w_1', \ldots, w_m'\}$ определяется множество $\Delta W' = \{\omega_i' \mid \omega_i' = w_i' - w_{i-1}', i = 1, \ldots, m\}$, где

$w_0' = 0$. На основе $\Delta W'$ аналогично S_n задается последовательность $S'=((k_i',s_i'))$. Сопоставляя выборки из n элементов последовательностей S' и S_n осуществляется поиск вариации ΔA. Применимость предложенного метода определяется тем фактом, что чем раньше элемент встречается в S_n, тем больше вероятность найти соответствующий ему элемент в S'.

Показано, что для восстановления рюкзачного вектора нет потребности в большом объеме информации о результатах отображения, существенным является количество различных значений. Предложенный численный метод позволяет уменьшить объем вычислений при поиске рюкзачного вектора – параметра одностороннего рюкзачного отображения – на основе различных значений $\mu_p(A)$. Обоснованы методы оптимизации численного метода для случая Z_2.

В **третьей главе** диссертации представлены результаты исследования вопросов использования рюкзачных векторов для определения односторонних функций, рассмотрены разработанные автором математические модели, описывающие односторонние отображения, и вопросы приложения полученных моделей в различных системах.

В основе методов поиска данных с использованием хеш-функций, хеш-таблиц, декартова дерева, фильтра Блума лежат отображения числовых значений во множество числовых цепочек (или чисел с заданными свойствами). Основным методом преобразования открытого текста в блочных системах защиты информации является «взбалтывание и перемешивание», в частности посредством перестановочной функции. В главе описываются математические модели односторонних рюкзачных отображений и систем на их основе, представляющие преобразование исходных значений, которое проводится аналогично описанным системам. Предложены системы, использующие рюкзачный вектор в качестве аналога перестановочной функции блочных систем защиты информации и хеш-функций. Определен способ задания рюкзачного вектора некоторой функциональной или процедурной зависимостью – генератором векторов – с относительно небольшим количеством параметров, часть которых общедоступна. Предложены модели

систем для такого способа задания вектора, сложность поиска отображения которых позволяет говорить об их практичности.

Определение 3.1. Произвольную всюду определенную функцию $F : R^t \to Z_p^n$ будем называть генератором векторов размерности n (ГВ^n) в Z_p.

Вектор $A = (a_1, a_2, \ldots, a_n) \in Z_p^n$ определяется генератором векторов F, если существует $\lambda \in R^t$, $F(\lambda) = A$ и будем говорить, что A задается F в точке λ. В качестве ГВ^n могут выступать алгоритм, аналитическая функция или их совокупность. Здесь важно то, что $F(\lambda)$ может быть найдено за приемлемое (в том или ином смысле) время.

Вектор $F(\lambda)=A \in Z_p^n$ рассматривается как рюкзачный вектор размерности n. Однако возможна интерпретация $F(\lambda)$ как вариация вектора ΔA, на основе которого возможно получение вектора A. В обоих случаях будем говорить, что $F(\lambda)$ задает вектор A, обозначим его $F(\lambda) \Rightarrow A$. Требование инъективности вектора $F(\lambda)$ обеспечивается применением теорем 2.1, 2.2, 2.3, 2.4 при определении генератора.

С целью увеличения сложности анализа разработана модель преобразования числовой последовательности с динамически изменяющимся рюкзачным вектором (ДГВ^n):

1) ГВ^n $F: R^t \to Z_p^n$ является частью системы, недоступной для сторонних пользователей;

2) значение $t \in N$ общедоступно и определяется пользователем в качестве параметра отображения;

3) значение i принимается равным 1;

4) значение j принимается равным 1;

5) значение $\lambda_j \in R^t$ общедоступно и определяется в качестве параметра отображения;

6) результат отображения $(A,v) = F_{np}(v_i) = w_i$ для очередного значения v_i последовательности исходных данных определяется на основе рюкзачного вектора A, где $F(\lambda_j) \Rightarrow A$;

7) значения i и j увеличиваются на 1;

8) если $i \leq s$ и $j \leq t$, то следует перейти к п.6;

9) если $i \leq s$, то следует перейти к п.4;

10) последовательность (t, λ_1, w_1, …, w_i, λ_2, w_{i+1}, w_{2i}, …, w_s) является результатом отображения системой последовательности числовых значений (v_1, v_2, …, v_s).

Восстановление значений (v_1, v_2, …, v_s) определяется функцией $F_{об}(w_i) = v_i$ для соответствующих векторов $F(\lambda_j) \Rightarrow A$.

Для предложенной модели доказана следующая теорема:

Теорема 3.1. При одинаковой верхней границе значений выходов w_{max} сложность нахождения параметров модели с ДГВ^m не меньше сложности нахождения параметров модели с ГВ^n, если количество рюкзачных векторов C_L, используемых в модели с ДГВ^n, не меньше $n - m + 1$.

Сложность поиска односторонего отображения на основе ДГВ^{44} в Z_2 превышает сложность поиска одностороннего отображения на основе ГВ^{256} в Z_2 уже при преобразовании набора данных объемом *2* килобайта в условиях теоремы 3.1. Данный факт показывает практическую значимость предложенных моделей в силу возможности оптимизации ресурсов при реализации систем на их основе.

В соответствии с правилом Кергхоффса в диссертационном исследовании модифицированы модели односторонних отображений на основе генераторов векторов в части анонимности определения генератора. Проанализированы методы задания генератора рюкзачных векторов, секретных и открытых параметров в целях увеличения сложности поиска функции отображения. Приведены примеры ГВ^n на основе одной или нескольких аналитических функций. Показана возможность определения рюкзачных векторов на основе рекуррентных зависимостей. Исследована стойкость таких моделей. Результаты исследования свидетельствуют о неэффективности большинства известных методов анализа таких отображений.

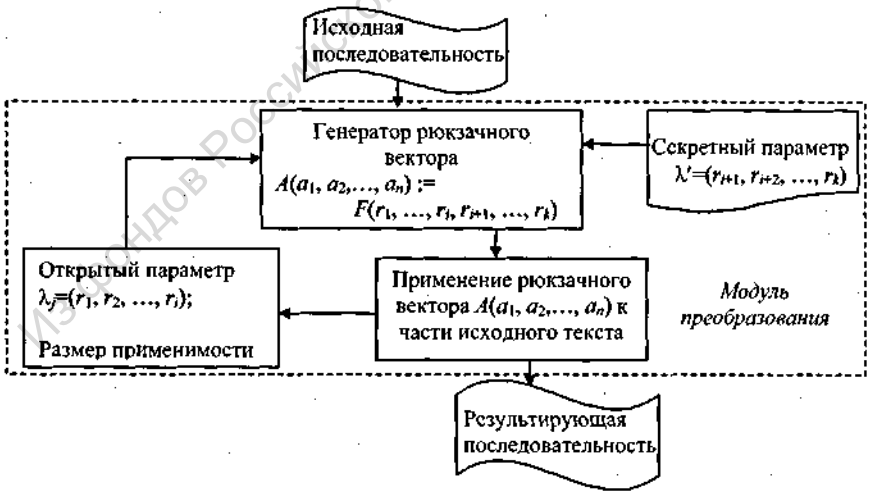
Показано, что, используя системы с ДГВ^n, можно минимизировать возможность применения статистических методов анализа, а при достаточно большом n – и алгебраических процедур анализа. Метод анализа на основе вариации существенно зависит от распределения известных значений $\mu_p(A)$. Но модификация результатов отображения путем изменения числового значения текста посредством корректирующей функции, свойства которой описаны в работе, приводит к невозможности получения

рюкзачного вектора отображения этим методом, так как последний будет искать вектор по заведомо ложным данным.

Проведен сравнительный анализ характеристик моделей односторонних отображений на основе ГВ^n и ДГВ^n. Предложены методы их использования, в частности, приведены примеры рюкзачных систем защиты информации.

В рамках исследования созданы различные системы преобразования данных на основе моделей с ГВ^n и ДГВ^n с различными способами определения генератора векторов. Показана высокая сложность восстановления параметров преобразования таких систем даже при небольших размерах рюкзачного вектора. Существенной характеристикой моделей с ДГВ^n является значение размера применимости рюкзачного вектора, которое определяет прежде всего количество различных рюкзачных векторов в рамках одного преобразования массива исходных данных. Указание в модели значения размера применимости рюкзачного вектора меньше размера последнего приводит к невозможности использовать неперебoрные методы анализа. Свойства получаемых отображений близки к полиалфавитным с малой вероятностью повторения результата для одного и того же исходного значения.

Общая блок-схема функционирования систем на основе ДГВ^n представлена на рисунке.



В рамках диссертационного исследования определена математическая модель односторонней функции, основанной на обратной задаче о рюкзаке (ОДГВ^n) для рюкзачного вектора $A = (a_1, a_2, \ldots, a_n)$. Результирующее значение ω такого отображения в Z_p представляет собой последовательность значений $(\alpha_1, \alpha_2, \ldots, \alpha_n, \eta_0, \eta_1, \ldots, \eta_s)$, где $s = [\log_p(a_1 - 1)] + 1$. Первые n элементов определяются разбиением по компонентам рюкзачного вектора согласно соотношений

$$\alpha_n = \omega \, div \, a_n, \qquad \alpha_i = \left(\omega - \sum\nolimits_{j=i+1}^{n} \alpha_j a_j\right) div \, a_i.$$

Последовательность $\eta_0\eta_1\ldots\eta_s$ определяет представление значения $\omega - \sum_{j=1}^{n} \alpha_j a_j$ в системе счисления с основанием p. В целях оптимизации затрат на реализацию и уменьшения вероятности эффективного анализа значение p определяется на основе рюкзачного вектора A по правилу

$$p = 1 + max_{i=1,n-1}(2, (a_{i+1} - 1) div \, a_i).$$

Приводятся различные математические модели ОДГВ^n.

Для данной модели характерна линейная сложность прямого и обратного преобразования, значение p не постулируется в системе, размер результата зависит от компонент рюкзачного вектора и меняется в процессе отображения. Показано, что анализ такого рода моделей односторонних отображений требует одновременного решения нескольких *NP*-полных задач, а информация, доступная для поиска параметров рюкзачного отображения, минимальна.

На основе предложенных математических моделей разработаны соответствующие алгоритмы функционирования систем. Создано программное приложение, реализующее возможность использования модели с ДГВ^n в системах защиты информации. Проанализированы результаты для различных ГВ^n. Описаны прикладные аспекты функционирования таких систем.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационной работе исследованы односторонние функции и способы их реализации на основе рюкзачных векторов. Разработаны и теоретически обоснованы математические модели односторонних функций с динамически определяемым рюкзачным вектором и системы на их основе.

В процессе выполнения диссертационной работы получены следующие основные научные и практические результаты.

1. Дано математическое описание элементов множества числовых значений, выражаемых в рюкзачном векторе.

2. Определено значение верхней границы решений задачи о рюкзаке для векторов с заданными свойствами.

3. Предложен численный метод построения рюкзачного вектора с заданными свойствами.

4. Построены модели односторонних отображений на основе динамически генерируемых рюкзачных векторов.

5. Разработаны модели систем на основе односторонних рюкзачных отображений и описаны алгоритмы их функционирования.

Список основных трудов по теме диссертации

1. *Подколзин В.В., Осипян В.О.* О свойствах рюкзачных систем защиты информации с открытым ключом в Z_p // Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2010 . Вып. 3(29). С. 51–55.

2. *Подколзин В.В.* Построение инъективных рюкзачных векторов на основе структурных и частотных свойств числовых множеств // Экологический вестник научных центров Черноморского экономического сотрудничества. 2010. №4. С. 64–67.

3. *Подколзин В.В.* Модель системы защиты информации с открытым ключом на основе динамической генерации рюкзачного вектора // Обозрение прикладной и промышленной математики. М.: Изд-во ОПиПМ, 2009. Т. 16, вып. 5. С. 913–914.

4. *Подколзин В.В., Осипян В.О.* Об одном методе определения верхней границы числа входов для рюкзачных систем защиты информации // Вестник Воронежского института МВД России. 2010. №4. С. 83–90. г. Воронеж, 2010

5. *Осипян В.О., Подколзин В.В.* Модели на основе рюкзачного вектора с обратным преобразованием // Экологический вестник научных центров Черноморского экономического сотрудничества. 2010. №4. С. 59–63.

6. *Осипян В.О., Подколзин В.В.* Об одной модификации задачи защиты информации с открытым ключом на основе обобщенного

рюкзака // Обозрение прикладной и промышленной математики. М.: Изд-во ОПиПМ, 2009. Т. 16, вып. 5. С. 905.

7. *Подколзин В.В.* Построение инъективного рюкзачного вектора для заданного множества значений на основе вариации // Обозрение прикладной и промышленной математики. М.: Изд-во ОПиПМ, 2010. Т. 17, вып. 3. С. 451–452.

8. *Подколзин В.В.* Модель системы защиты информации на основе обратной задачи о рюкзаке // Математические методы и информационно-технические средства: труды V Всерос. науч.-практ. конф. Краснодар: Краснодарский ун-т МВД России, 2009. С. 139–141.

9. *Подколзин В.В.* Об одном определении рюкзачной СЗИ с открытым ключом на основе динамически создаваемого вектора. Верхняя оценка количества решений // Материалы I Всероссийской молодежной конференции по проблемам информационной безопасности «Перспектива-2009». Таганрог: Изд-во ТТИ ЮФО, 2009. С 265–269.

10. *Подколзин В.В., Осипян В.О.* Алгоритм построения инъективного возрастающего рюкзачного вектора // Математические методы и информационно-технические средства: труды V Всерос. науч.-практ. конф. Краснодар: Краснодарский ун-т МВД России, 2009. С. 141–145.

11. *Подколзин В.В., Осипян В.О.* Верхняя граница числа решений обобщенной задачи о рюкзаке на заданном входе // Актуальные проблемы безопасности информационных технологий: материалы III Междунар. науч.-практ. конф. / под общ. ред. О. Н. Жданова, В. В. Золотарева. Красноярск: Сибирский гос. аэрокосмический ун-т, 2009. С. 28–32.

12. *Подколзин В.В., Осипян В.О., Арджанов А.А.* Изоморфизм рюкзачных систем защиты информации с открытым ключом // Материалы XIII Международной научной конференции им. Решетнева. Красноярск: Сибирский гос. аэрокосмический ун-т, 2009. С. 569–571.

13. *Осипян В.О., Подколзин В.В.* Моделирование рюкзачных систем защиты информации на основе динамически изменяемого рюкзачного вектора // Математические методы и информационно-технические средства: труды VI Всерос. науч.-практ. конф. Краснодар: Краснодарский ун-т МВД России, 2010. С. 128–132.

14. *Осипян В.О., Подколзин В.В.* Системы защиты информации с генератором рюкзачных векторов // Труды академии связи : научно-технический сборник № 76. С. 53-55. г. Краснодар, 2010.

15. *Осипян В.О., Подколзин В.В., Арджанов А.А.* О сложности задачи о плотной укладке рюкзака для выходов систем защиты информации на основе ГРВ // Математические методы и информационно-технические средства: труды V Всерос. науч.-практ. конф. Краснодар: Краснодарский ун-т МВД России, 2009. С. 136–139.

16. *Осипян В.О., Подколзин В.В., Арджанов А.А.* Об одной кодовой криптосистеме на основе кода Варшамова // Материалы XIII Международной научной конференции им. Решетнева Красноярск: Сибирский гос. аэрокосмический ун-т, 2009. С. 568–569

17. *Осипян В.О., Спирина С.Г., Подколзин В.В., Шевцова М.А.* Разработка методов построения и оценка числа перестановочных целых функций над полем Галуа // Вестник КазНУ. 2008. №4 (59). С. 178–183.

18. *Осипян В.О., Спирина С.Г., Подколзин В.В., Арутюнян А.С.* Моделирование ранцевых криптосистем, содержащих диофантовую трудность // Чебышевский сборник Т. XI, вып. 1(33): труды VII Междунар. конф. Алгебра и теория чисел: современные проблемы. Тула: Изд-во Тул. гос. пед. ун-та им. Ломоносова, 2010. С. 209–217.

19. *Осипян В.О., Спирина С.Г., Подколзин В.В.* Моделирование перестановок на основе перестановочных целых функций // Современные проблемы математики, информатики и управления: материалы Междунар. науч. конф. Алматы: Институт проблем информатики и управления, 2008. С. 284–287.

20. Свидетельство о государственной регистрации программ для ЭВМ № 2011610789. Программный комплекс преобразования информации «РСЗИ ДГВ[n]» // Подколзин В.В., Осипян В.О. ; заявитель и правообладатель ГОУ ВПО КубГУ – № 2010617352; заявл. 23.10.2010; опубл. 14.01.2011, Реестр программ для ЭВМ.

Подколзин Вадим Владиславович

МОДЕЛИРОВАНИЕ СИСТЕМ НА ОСНОВЕ ОДНОСТОРОННИХ РЮКЗАЧНЫХ ОТОБРАЖЕНИЙ

Автореферат

Бумага тип. № 2. Печать трафаретная.
Тираж 100 экз. Заказ № 859

350040 г. Краснодар, ул. Ставропольская, 149,
Центр "Универсервис", тел. 21-99-551.