

ОТЗЫВ

официального оппонента на диссертационное исследование Лапикова Игоря Игоревича на тему «Построение и реализации алгоритмов решения систем целочисленных неравенств в методе разделяющих плоскостей», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Актуальность темы исследования

Диссертация Лапикова И.И. посвящена разработке и реализации новых алгоритмов решения систем линейных целочисленных неравенств в задачах информационной безопасности. Можно указать два современных направления в проблематике защиты информации, делающих актуальной выбранную тему исследований.

Во-первых, увеличение объемов и совершенствование структуры информационного обмена в современных сетях связи, способствующее переходу на новые высокоскоростные методы обработки и передачи информации, в частности – оптические. Оптическая элементная база позволяет с высокой быстротой и эффективностью реализовывать операции вычисления скалярного произведения и сравнения, лежащие в основе синтеза пороговых функций в двоичной и k -значной логике. Функционирование узлов обработки информации в пороговом базисе объективно описывается системами линейных неравенств, анализу и решениям которых посвящена диссертация.

Во-вторых, с этим тесно связана и общая проблематика анализа узлов защиты информации, работа которых сводится к системам линейных неравенств либо естественно, благодаря их реализации в пороговом базисе, либо искусственно путем целенаправленного сведения реализуемых операций к системам линейных неравенств. Как показано в работе, к системам линейных неравенств может быть сведено описание значительного числа различающихся по своей архитектуре современных узлов и блоков защиты информа-

ции. Актуальность результатов диссертации также следует рассматривать с этих двух позиций: обоснованию надежности вновь разрабатываемых систем защиты информации к анализу уже существующих, а также перспективных, и их защиты от компрометации.

Основные задачи исследования

Представленная диссертация направлена на разработку принципиально нового метода решения систем линейных неравенств на базе развития и адаптации полиномиального алгоритма эллипсоидов, предложенного Л.Г. Хачияном в 1979 году. Поставленная цель потребовала от автора решения целого ряда взаимосвязанных математических и алгоритмических задач. В результате в построенном алгоритме удалось перейти от нахождения действительных решений, как это предусмотрено в алгоритме Хачияна, к получению целочисленных, что обеспечивается разработкой оригинальных процедур локализации множества решений и остановки алгоритма.

Прикладная направленность диссертационного исследования определяется непосредственным приложением вновь разработанного алгоритма для анализа целого ряда конкретных узлов защиты информации, прежде всего генераторов псевдослучайных последовательностей (ПСП). В результате обнаружены возможности компрометации систем в тех случаях, когда их функционирование приводит к формированию эффективно решаемых разработанным методом систем линейных неравенств.

Тема диссертации, направленность проведенных исследований и полученных результатов в полной мере соответствует паспорту научной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Теоретические положения и прикладные результаты в целом ориентированы на повышение информационной безопасности систем обработки и сетей передачи информации.

Характеристика работы

Во введении аргументирована актуальность темы исследования, сформулированы цели и задачи работы, перечислены используемые методы исследования, обоснованы научная новизна и практическая значимость полученных результатов, приведены сведения о результатах внедрения.

В первой главе подробно рассмотрены и обобщены результаты Никонова В.Г. и других авторов по направлению построения метода разделяющих плоскостей и его развития для k -значного случая – метода разделяющих поверхностей. Показана важность обозначенных методов в сведении прикладных задач к системам пороговых ограничений.

Во второй главе автором на основе углубленного изучения метода эллипсоидов в алгоритме Хачияна построены адаптивный алгоритм эллипсоидов решений систем линейных неравенств с k -значными неизвестными и его модификация – ПД-алгоритм на базе декомпозиции пространства поиска решений, проведено сравнение параметров их работы с эвристическими алгоритмами, в частности с алгоритмом Балаша и имитации отжига.

В третьей главе автором рассмотрены задачи компрометации генераторов ПСП, используемых при построении систем защиты информации, сводимые к решению СЛН с k -значными неизвестными, для решения которых применяются построенные алгоритмы. Отдельно отмечена важность полученной оценки расстояния единственности задачи восстановления линейной рекурренты по знакам старшего разряда.

В заключении подводятся итоги и обсуждаются некоторые направления для дальнейших исследований.

Новизна исследования и полученных научных результатов

Из анализа содержания диссертации можно сделать следующие выводы.

Автором на основании глубокого анализа структуры алгоритма Хачияна Л.Г. построен принципиально новый адаптивный алгоритм, позволяющий находить целочисленные решения систем линейных неравенств. Для

сокращения временной сложности реализации адаптивного алгоритма предложен метод геометрического распараллеливания, для которого дан расчет сложностных параметров.

Новыми результатами являются все рассмотренные приложения адаптивного алгоритма для решения задач анализа конкретных генераторов ПСП. Особого внимания заслуживает рассмотренная в диссертации задача нахождения начального заполнения ЛРС с трехчленным законом обратной связи, реализующим линейную рекуренту над кольцом $Z/2^m$, по последовательности подряд идущих знаков старшего разряда и полученная эмпирическая оценка расстояния единственности задачи.

Новым следует признать применение метода эллипсоидов Хачияна в задаче распознавания принадлежности булевой или k -значной функции к классу пороговых с обоснованием вывода о том, что эта задача имеет полиномиальную сложность.

Отмеченные положения позволяют сделать заключение о высоком уровне научной новизны представленной диссертации.

Обоснованность и достоверность положений и выводов диссертации

В основе работы лежит строгий математический подход к формализации поставленной задачи и ее последующему решению. Теоретические положения нашли свое экспериментальное подтверждение благодаря практической реализации разработанного адаптивного алгоритма. Его применение в конкретных прикладных задачах анализа генераторов ПСП позволило сделать вывод о его корректности и логической обоснованности.

Теоретическая значимость и практическая ценность работы

Теоретическое значение для развития методической базы построения и анализа систем защиты информации имеет и сам построенный в диссертации адаптивный алгоритм решения систем линейных целочисленных неравенств, так и все полученные в диссертации оценки сложности.

Практическая ценность диссертации заключается в разработанных направлениях применения адаптивного алгоритма для решения задач анализа различных схем генераторов ПСП. Высокую прикладную значимость подтверждают два свидетельства о регистрации программ для ЭВМ, полученные автором.

Недостатки работы

1. С практической точки зрения в диссертации основное внимание уделено выявлению генераторов ПСП, для которых может быть эффективно применен адаптивный алгоритм эллипсоидов и практически ничего не сказано о методах построения схем, защищенных от применения этого алгоритма.
2. Класс генераторов ПСП, для которых применим адаптивный алгоритм эллипсоидов может быть существенно расширен за счет специального их построения. Такие искусственно построенные схемы представляли бы интерес, как максимально удобные для данного алгоритма
3. Наряду с полученными в диссертации оценками временной сложности алгоритмов представляло бы интерес детальное рассмотрение параметров емкостной сложности.
4. На стр. 71 в описании алгоритма используется обозначение «Т», которое в алгоритме не определено, на стр. 125 ошибка в нумерации рисунка.

Тем не менее, указанные недостатки не снижают общего благоприятного впечатления от представленной работы.

Подводя итогу, можно заключить, что диссертация Лапикова Игоря Игоревича «Построение и реализация алгоритмов решения целочисленных неравенств в методе разделяющих плоскостей» удовлетворяет всем требованиям «Положения о порядке присуждения ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.12 №842, написана на высоком научном уровне, отличается логической целостностью, глубиной проведенных исследований, результаты которых имеют теоретическое и прикладное значение при решении актуальных задач защиты информации и дискретной математики.

Автор представленной диссертации Лапиков И.И. достоин присуждения ученой степени кандидата технических наук по научной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

Профессор кафедры «Прикладные и информационные технологии» Института комплексной безопасности и специального приборостроения Федерального государственного бюджетного учреждения высшего образования «МИРЭА – Российский технологический университет», доктор технических наук (специальность 20.02.12), профессор; 119454, город Москва, пр-т Вернадского, д.78; Тел. +7-911-987-88-19; электронная почта: mael@rambler.ru



Еремеев Михаил Алексеевич

«26» апреля 2019 г.

Подпись доктора технических наук, профессора Еремеева М.А. заверяю
Директор Института комплексной безопасности и специального приборостроения Федерального государственного бюджетного учреждения высшего образования «МИРЭА – Российский технологический университет»

кандидат технических наук, доцент

«30» апреля 2019 г.



А.Б. Снедков