

ОТЗЫВ

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

Актуальность темы работы

Проблема решения систем неравенств наряду с проблемой решения систем уравнений по праву может быть отнесена к числу важнейших в теоретической и прикладной математике. В настоящее время очевидный алгоритмический аспект этой проблематики дополняется активно развиваемым теоретико-сложностным подходом с разбиением задач на условно сложные и простые, для которых может быть предложен алгоритм с полиномиальной оценкой сложности. С этой точки зрения появление в 1979 году алгоритма Хачияна решения систем линейных неравенств в действительной области с полиномиальной оценкой сложности стало важным событием в этой научной области. Основным недостатком алгоритма Хачияна являлось то, что он позволял находить решения именно в действительной области и не был приспособлен к нахождению решений дискретных. Устранению этого недостатка путем построения нового адаптивного алгоритма для нахождения уже дискретных решений с сохранением рационального алгоритмического ядра – метода эллипсоидов – посвящена представленная диссертация. Можно констатировать, что успешная разработка автором адаптивного алгоритма эллипсоидов для решения систем линейных неравенств относительно дискретных неизвестных вносит значимый вклад в развитие данной актуальной проблематики в целом. Кроме того, необходимо подчеркнуть, что тема диссертации представляется актуальной и в связи с рассмотренными в ней важными приложениями

разработанного алгоритма в задачах анализа конкретных узлов защиты информации.

Научная и практическая новизна результатов работы

Разработанный в диссертации адаптивный алгоритм линейных неравенств относительно дискретных неизвестных является новым. Применение этого алгоритма в задачах анализа узлов защиты информации и генераторов псевдослучайных последовательностей (ПСП) открывает новые возможности нахождения уязвимостей в этих системах путем анализа и решения порождаемых ими систем линейных неравенств.

Достоверность и степень обоснованности научных положений и выводов

Достоверность результатов диссертации обосновывается корректным использованием математических методов исследования с привлечением теории булевых и k -значных функций, математического анализа, теории алгоритмов. Практические положения и выводы подтверждаются экспериментальными методами исследования с реализацией на ЭВМ разработанных алгоритмов и их применения в конкретных задачах анализа узлов защиты информации.

Характеристика работы

Во введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследования, показаны теоретическая и практическая значимости, представлены основные положения, выносимые на защиту.

В первой главе рассмотрено псевдобулево направление в дискретной математике. В параграфе 1.1 рассмотрены свойства булевых и k -значных функций. В параграфах 1.3-1.4 проведен анализ методов сведения булевых и k -значных уравнений к системам линейных равенств.

Во второй главе построены алгоритмы решения систем линейных неравенств на основе идей метода эллипсоидов Хачияна. В параграфах 2.1-2.2 выделены направления развития алгоритма Хачияна для его применения

в дискретной области. В параграфах 2.3.-2.5 построены адаптивный алгоритм эллипсоидов и пространственно-декомпозиционный алгоритм, проведено сравнение параметров их работы с альтернативными алгоритмами на модели случайных систем.

В третьей главе рассмотрены практические приложения разработанных алгоритмов. В параграфе 3.1 приведен обзор прикладных задач информационной безопасности, основанных на анализе генераторов ПСП. В параграфе 3.2 адаптивный алгоритм эллипсоидов применен для изучения классов функций с запретами и полузапретами, а в параграфе 3.3 для доказательства биективности произвольного отображения. В параграфах 3.4, 3.5 показана возможность восстановления начального состояния комбинирующих и фильтрующих генераторов на базе линейного регистра сведением задачи их анализа к системам линейных неравенств с дискретными неизвестными, для решения которых применен адаптивный алгоритм эллипсоидов. Особый интерес представляет полученная аппроксимирующая функция верхней оценки сложности задачи восстановления линейной рекурренты, реализованной ЛРС с трехчленным законом обратной связи по подряд идущим знакам ее старшей координатной последовательности. В параграфе 3.6 модифицированный алгоритм эллипсоидов Хачияна использован для решения задачи характеристики k -значной пороговой функции.

В заключении сформулированы основные научные и практические результаты диссертации.

В приложениях приведены акты о внедрении результатов диссертационного исследования, свидетельства о регистрации программ для ЭВМ и описания состава программных продуктов.

Публикации, реализации и апробации научных положений

Результаты диссертационного исследования опубликованы в 10 научных трудах, из которых 7 научных статей опубликованы в изданиях, входящих в перечень рецензируемых научных журналов ВАК РФ.

Публикации полностью отражают научные положения, выносимые на защиту. Ссылки на совместные работы и работы других авторов использованы корректно.

Основные результаты апробировались на XLIII Международной конференции, XIII Международной конференции молодых ученых «Информационные технологии в науке, образовании, телекоммуникации и бизнесе 'IT+SE15'» (2015 г.), Всероссийской конференции «Сибирская научная школа-семинар с международным участием 'Компьютерная безопасность и криптография' SIBECRYPT'17» (2017 г.), XI Всероссийской научной конференции ученых, специалистов и профессорско-преподавательского состава «Территориальные распределенные системы охраны» (2018 г.).

Результаты работы внедрены в образовательный процесс Балтийского Федерального университета им. И. Канта., практическую деятельность ООО «Ю-КОРП» и ООО «Лингвистические и информационные технологии». Автором получены два свидетельства о регистрации программ для ЭВМ.

Оценка содержания диссертации и степени ее завершенности.

Оценка содержания автореферата

По содержанию работа представляется завершенной научной работой, которая включает введение, три главы с выводами по каждой из них, заключение, список литературы и приложения. Она содержит 164 страницы, 19 рисунков и 16 таблиц и список литературы (125 наименований).

В целом диссертационная работа Лапикова И.И. представляет собой самостоятельно завершенную научно-квалификационную работу, в которой сформулирована и решена актуальная научная задача. Диссертационная работа обладает внутренним единством, содержит новые научные результаты и положения, свидетельствует о личном вкладе автора в науку и обладает практической значимостью. Из проведенного анализа материалов диссертационной работы следует, что автором получен ряд оригинальных

результатов, имеющих существенное значение для дискретной математики и информационной безопасности.

Полученные результаты достоверны и в достаточной степени обоснованы. Следует отметить целостность диссертационной работы. Материал изложен логично, содержание рисунков и таблиц хорошо продумано. Рукопись оформлена в соответствии с ГОСТ.

Тема и содержание диссертационной работы соответствуют паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Глубокое изучение автором сущности научной задачи нашло свое выражение в сформулированных им направлениях дальнейших исследований.

Автореферат правильно и достаточно полно передает основное содержание диссертации. Он оформлен в соответствии с требованиями ВАК РФ и ГОСТ. Стиль изложения в основном способствует пониманию содержания работы.

Наряду с вышеперечисленными достоинствами указанная работа не лишена недостатков, не влияющих на общее качество работы.

1. По мнению оппонента, некоторые вопросы, затронутые в диссертации, заслуживают более глубокого изучения, например, приложения построенного алгоритма к теории запретов и к задаче нахождения заполнения ЛРП над кольцом \mathbb{Z}_2^m по знакам старшего разряда. Развитию указанных направлений могли бы быть посвящены дальнейшие исследования по данной тематике.

2. Имеется неточность в определениях полузапретов I и II рода, в которых значность логики полагается равной $k \geq 2$. Однако отдельно случай при $k = 2$ не рассматривается.

3. В нескольких местах (стр. 50, 63, 65) используется понятие «шар», когда говорится об n -мерном пространстве.

4. Имеются опечатки на страницах 12, 66, 72, 123.

Заключение

Диссертационная работа содержит решение актуальной научной задачи, имеющей существенное значение для информационной безопасности и дискретной математики, соответствует требованиям «Положения о порядке присуждения ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.12 №842, предъявляемым к кандидатским диссертациям, а ее автор, Лапиков Игорь Игоревич, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

Начальник отдела криптографических исследований общества с ограниченной ответственностью «КРИПТО-ПРО», кандидат физико-математических наук (специальность 05.13.19– «Методы и системы защиты информации, информационная безопасность»), 127018, город Москва, ул. Сушевский Вал, д.18; Тел. +7-903-159-33-62; электронная почта: alekseev@cryptopro.ru

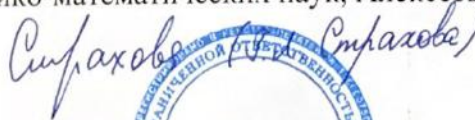


Алексеев Евгений Константинович

«7» мая 2019 г.

Подпись кандидата физико-математических наук, Алексева Е.К. заверяю

Специалист по кадрам



«7» мая 2019 г.