Федеральное государственное бюджетное учреждение науки
Институт динамики систем и теории управления имени В.М. Матросова
Сибирского отделения Российской академии наук
(ИДСТУ СО РАН)

На правах рукописи

Грибанова Ирина Александровна

Применение алгоритмов решения проблемы булевой выполнимости к задачам обращения криптографических хеш-функций

09.06.01 — Информатика и вычислительная техника

05.13.18 — Математическое моделирование, численные методы и комплексы программ

НАУЧНЫЙ ДОКЛАД
об основных результатах научно-квалификационной работы (диссертации)
на соискание ученой степени
кандидата технических наук

Иркутск — 2019

Работа выполнена в лаборатории 6.2. Логических и оптимизационных методов анализа сложных систем отделения 6. Методов невыпуклой и комбинаторной оптимизации ИДСТУ СО РАН.

Научный руководитель: **Семёнов Александр Анатольевич,**
к.т.н., доцент,
зав. лаб. 6.2 ИДСТУ СО РАН

Рецензенты: **Сидоров Денис Николаевич,**
д.ф.-м.н., профессор РАН,
в.н.с. ИСЭМ СО РАН

Ульянов Сергей Александрович,
к.т.н.,
зав. лаб. 5.2 ИДСТУ СО РАН

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Современные криптографические хеш-функции являются де-факто базовыми примитивами многих криптографических протоколов: процедуры проверки целостности данных, схемы электронной подписи, системы хранения паролей, криптовалюты. Стойкость криптографических хеш-функций определяется вычислительной трудностью задач их криптоанализа. К таким задачам относятся задачи поиска коллизий и задачи поиска прообразов. В этой связи актуальными являются исследования различных методов и алгоритмов решения таких задач.

В рамках настоящего исследования рассматриваются задачи криптоанализа известных хеш-функций семейства MD (MD4, MD5), построенных на основе конструкции Меркла–Дамгарда. Данная конструкция предполагает, что хешируемое сообщение разбивается на блоки некоторой фиксированной длины. Для вычисления хеш-значения к каждому блоку последовательно применяется специальная функция сжатия. Данная функция задается алгоритмом, который состоит из последовательности элементарных преобразований (шагов). На каждом шаге на основе результата предыдущих шагов обновляется значения одной из четырех 32-битных переменных. Данные переменные называются переменными сцепления (chaining variables) и формируют 128-битный хеш-регистр, в котором хранится промежуточное значение хеша. После обработки всех блоков сообщения хеш-регистр содержит итоговое значение хеш-функции.

В хеш-функциях MD4 и MD5, которые были предложены Р. Ривестом в 1990–1991 гг., длина одного блока составляет 512 бит, а длина хеш-значения — 128 бит. Основное отличие данных хеш-функций состоит в использовании различных алгоритмов задания функции сжатия. Так, алгоритм функции сжатия MD4 состоит из 48 шагов, которые условно делятся на три раунда по 16 шагов. В каждом раунде используются специальные раундовые функции и известные целочисленные константы. Функция сжатия MD5 состоит из 64 шагов, при этом раундовые функции первого и второго раунда совпадают с аналогичными раундовым функциям MD4.

Вскоре после того, как данные хеш-функции были сертифицированы, появились работы, в которых были описаны их первые уязвимости. Наиболее значимыми стали работы, опубликованные в 2005 г. коллективом криптографов под руководством С. Ванг, в которых был предложен эффективный метод нахождения коллизий для хеш-функций MD4[1] и MD5[2]. Данный метод представлял собой вариант «дифференциальной атаки», использующий разностные соотношения на пары хешируемых сообщений и промежуточные значения хеша. В контексте дифференциальной атаки множества таких соотношений, за-

[1] Wang X., Lai X., et al. Cryptanalysis of the Hash Functions MD4 and RIPEMD // Advances in Cryptology (EUROCRYPT 2005). Springer-Verlag, 2005. Vol. 3494. P. 1–18.

[2] Wang X., Yu H. How to Break MD5 and Other Hash Functions // Advances in Cryptology (EUROCRYPT 2005). Springer-Verlag, 2005. Vol. 3494. P. 19–35.

писанные в виде разностей (целочисленных или битовых), называют «дифференциальными» или «разностными» путями (differential paths). Позднее метод С. Ванг был значительно улучшен в ряде работ. В частности, для хеш-функции MD5 были найдены одноблоковые коллизии и построены примеры коллизий реальных документов (пара различных X.509 сертификатов, имеющих одинаковый хеш[3]). Для хеш-функции MD4 был предложен метод поиска коллизий, сложность которого сравнима со сложностью вычисления данной хеш-функции. В результате хеш-функции MD4 и MD5 были полностью скомпрометированы по отношению к задаче поиска коллизий.

Тем не менее, для хеш-функций семейства MD до сих пор не предложено эффективных методов решения задачи поиска прообраза, т. е. задачи поиска неизвестного входного сообщения по известному значению хеша. Даже для хеш-функции MD4, которая является менее криптографически стойкой по сравнению с MD5, предложена лишь теоретическая атака[4], оценка сложности которой составляет 2^{102} вычислений функции сжатия MD4. Лучшие «практические» результаты в данной области относятся к задачам поиска прообраза некоторых ослабленных версий данных хеш-функций.

Одной из первых работ в данном направлении стала работа Г. Доббертина, в которой было продемонстрировано, что задача поиска прообраза 32-шаговой версии хеш-функции MD4 не является вычислительно сложной задачей[5]. Ключевой для данной работы стала идея использования дополнительных ограничений, накладываемых на промежуточные значения хеш-функции. Более точно, было предложено зафиксировать значения переменных сцепления на определенных шагах алгоритма функции сжатия MD4 с помощью конкретной 32-битной константы. В 2007 г. был предложен вариант атаки Г. Доббертина[6], в котором алгоримы решения задачи о выполнимости булевых формул использовались для поиска прообразов 39-шаговой версии хеш-функции MD4.

В последние годы задачи, связанные с исследованием стойкости криптографических примитивов, все чаще рассматриваются в контексте алгебраического криптоанализа, в рамках которого данные задачи сводятся к решению систем алгебраических уравнений над конечными полями, например над полем $GF(2)$. При помощи данного подхода были построены алгебраические атаки с рекордной трудоемкостью для ряда алгоритмов блочного и поточного шифрования.

Одним из способов решения широкого круга комбинаторных задач является т. н. «SAT-подход», в рамках которого исходная задача сводится к задаче о булевой выполнимости (Boolean Satisfiability Problem), кратко обозначаемой

[3]Lenstra A., et al. Colliding X.509 Certificates // IACR Cryptology ePrint Archive. 2005. Vol. 2005. P. 67.

[4]Leurent G. MD4 is not one-way // Proc. of the 14th International Workshop on Fast Software Encryption (FSE 2008). Springer, 2008. Vol. 5086. P. 412–428.

[5]Dobbertin H. The first two rounds of MD4 are not one-way // Proc. of the 5th International Workshop on Fast Software Encryption (FSE 1998). Springer, 1998. Vol. 1372. P. 284–292.

[6]De D., et al. Inversion attacks on secure hash functions using SAT solvers // Theory and Applications of Satisfiability Testing (SAT 2007). Springer, 2007. Vol. 4501. P. 377–382.

как SAT. Данная задача заключается в ответе на вопрос о выполнимости произвольной булевой формулы в конъюнктивной нормальной форме (КНФ). Если КНФ выполнима, то требуется найти хотя бы один выполняющий ее набор (т. е. такой набор значений переменных данной КНФ, на котором она принимает значение «истина»). Многие современные алгоритмы и технологии решения SAT, разработанные с целью использования в распределенных вычислительных средах, успешно справляются даже с такими аргументированно трудными задачами, какими являются задачи криптоанализа. В целом ряде работ, из которых сошлемся лишь на монографию Г. Барда[7], для решения задач алгебраического криптоанализа используется именно SAT-подход.

Цель и задачи исследования. Основная цель состоит в разработке новых методов решения задач криптоанализа хеш-функций семейства MD, в основу которых положены алгоритмы и технологии решения проблемы булевой выполнимости (SAT).

Для достижения поставленной цели были решены следующие задачи:

- проанализированы существующие подходы к решению рассматриваемых задач;
- задачи поиска коллизий криптографических хеш-функций MD4 и MD5, а также задачи поиска прообразов неполнораундовых вариантов хеш-функции MD4 сведены к решению систем булевых уравнений;
- разработаны методы автоматического синтеза «эффективных» дополнительных ограничений, накладываемых на промежуточные значения хеш-функции MD4, с целью упрощения исходных уравнений криптоанализа;
- построены новые алгебраические атаки на неполнораундовые версии хеш-функции MD4;
- построены оценки сложности реализации предложенных данных атак в параллельных и распределенных вычислительных средах.

Методы и инструменты исследования. Теоретическая часть исследования базируется на методах дискретной математики, криптографии, теории вычислительной сложности, теории решения систем булевых уравнений, анализе предыдущего опыта криптоанализа хеш-функций семейства MD, в том числе с использованием SAT-подхода.

Для сведения задач криптоанализа хеш-функций семейства MD к решению систем булевых уравнений в форме «КНФ=1» применялся программный комплекс Transalg, разработанный в ИДСТУ СО РАН. Для выполнения вычислительных экспериментов использовались современные SAT-решатели (MiniSat2.2, CryptoMiniSat, Painless и др.), а также вычислительные ресурсы кластера ИДСТУ СО РАН «Академик В.М. Матросов».

Научная новизна. Новыми являются все полученные результаты, кратко сформулированные далее.

[7]Bard G. Algebraic cryptanalysis. Springer, 2009. 356 p.

1. Улучшены известные результаты поиска коллизий хеш-функций MD4 и MD5 с использованием SAT-подхода. Для хеш-функции MD5 выделен новый класс двухблоковых коллизий. Для хеш-функции MD4 построены новые дифференциальные пути, дающие более эффективную в сравнении с известными SAT-атаку поиска одноблоковых коллизий.
2. Разработан метод автоматической генерации дополнительных ограничений для задачи поиска прообразов неполнораундовых версий хеш-функции MD4. Процедура поиска таких ограничений сведена к решению задачи псевдобулевой оптимизации оценочной функции типа «черный ящик».
3. С использованием найденных наборов ограничений построена атака на 39-шаговую версию хеш-функции MD4 с рекордной трудоемкостью. В рамках построенной атаки удается решать задачи поиска прообразов для большой доли (65%) случайных значений данной хеш-функции в среднем менее чем за 1 минуту при помощи последовательного SAT-решателя.
4. Предложен новый класс атак на неполнораундовые версии криптографической хеш-функции MD4, аргументирующие отсутствие у них свойств односторонней функции. Для задачи поиска прообразов 40-шаговой версии хеш-функции MD4 построена алгебраическая атака из класса «угадывай-и-определяй» (guess-and-determine attack).
5. Найдены множества дополнительных ограничений, позволяющие выделить множества значений полнораундовой хеш-функции MD4, для которых задача поиска прообразов является вычислительно легкой.

Положения, выносимые на защиту:

1. Метод построения новых дифференциальных путей для задачи поиска одноблоковых коллизий хеш-функции MD4.
2. Метод поиска дополнительных ограничений для задачи обращения неполнораундовых версий хеш-функции MD4, реализованный при помощи алгоритмов псевдобулевой оптимизации.
3. Новый класс криптографических атак на неполнораундовые версии хеш-функции MD4, в рамках которых исходные задачи обращения рассматриваемых хеш-функций сводятся к задачам обращения функций специального вида.

Теоретическая и практическая значимость. Полученные результаты имеют важное теоретическое и практическое значение, поскольку разработанные методы и алгоритмы могут быть использованы в качестве средств тестирования базовых примитивов, лежащих в основе других криптографических хеш-функций, а также способствовать тем самым разработке новых таких функций.

Соответствие специальности. В соответствии с паспортом специальности 05.13.18 «Математическое моделирование, численные методы и комплексы программ» квалификационная работа охватывает такие направления, как раз-

работка, реализация и тестирование эффективных вычислительных методов в виде комплексов проблемно-ориентированных программ, а также проведение вычислительных экспериментов с применением современных компьютерных технологий для исследования актуальных научно-технических проблем. Отраженные в квалификационной работе положения соответствуют пунктам 3, 4, 5 области исследований специальности 05.13.18.

Достоверность результатов проведенных исследований. Достоверность подтверждается обоснованным использованием выбранных подходов к решению поставленных задач. Корректность предложенных методов и алгоритмов, а также эффективность их практической реализации подтверждается результатами вычислительных экспериментов.

Апробация результатов работы. Результаты, полученные в процессе выполнения научной работы, докладывались и обсуждались на следующих конференциях: «Параллельные вычислительные технологии (ПаВТ) 2019» (г. Калининград, 2019 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» — Sibecrypt'18 (г. Абакан, 2018 г.), International Convention on Information and Communication Technology, Electronics and Microelectronics — MIPRO 2018 (г. Опатия, Хорватия, 2018 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» — Sibecrypt'17 (г. Красноярск, 2017 г.), XVIII Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям (г. Иркутск, 2017 г.), «Параллельные вычислительные технологии (ПаВТ) 2017» (г. Казань, 2017 г.), Сибирская научная школа-семинар с международным участием «Компьютерная безопасность и криптография» — Sibecrypt'16 (г. Новосибирск, 2016 г.), «Ляпуновские чтения» (г. Иркутск, 2015–2018 гг.).

Основные научные результаты по теме исследования получены в рамках грантов РФФИ (№ 14-07-31172 мол_а, № 14-07-00403 А, № 15-07-07891), а также проекта РНФ (№ 16-11-10046).

Публикации и личный вклад автора. Результаты квалификационной работы опубликованы в 16 печатных работах, в том числе две статьи в рецензируемых журналах, входящих в перечень ВАК, три статьи в изданиях, индексируемых в международных системах научного цитирования (Web of Science, Scopus).

Концепции алгебраических атак, построенных с использованием IBS-метода (пп. 2.4, 2.6, 2.7), сформулированы совместно с научным руководителем А.А. Семёновым. Разработка методов решения задач криптоанализа хеш-функций MD4 и MD5 и все выносимые на защиту положения получены лично автором.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В **главе 1** рассматриваются базовые понятия, связанные с криптографическими хеш-функциями и задачами их криптоанализа.

В **п. 1.1** дается общая характеристика хеш-функций как базового криптографического примитива. Вводится понятие криптографической хеш-функции и описываются ее основные свойства (детерминированность, высокая скорость вычисления хеш-значения, стойкость к нахождению прообразов, стойкость к нахождению коллизий и др.).

В **п. 1.2** описан ряд примеров систем и приложений, в которых используются современные криптографические хеш-функции.

В **п. 1.3** стойкие криптографические хеш-функции рассматриваются как перспективные кандидаты на роль реальных прототипов идеального понятия «случайный оракул».

В **п. 1.4** рассматриваются криптографические атаки общего вида, которые могут быть применены к любым хеш-функциям. Данные атаки отличаются от атак специального вида, которые эксплуатируют недостатки определенного способа построения хеш-функции.

В **п. 1.5** приведено описание конструкции Меркла–Дамгарда, которая является базовой для многих криптографических хеш-функций, например хеш-функций семейства MD и SHA.

В **п. 1.6** описаны алгоритмы хеш-функций семейства MD, а именно хеш-функции MD4 и MD5.

В **п. 1.7** кратко описаны известные атаки на криптографические хеш-функции MD4 и MD5.

В **главе 2** задачи обращения криптографических функций рассматриваются в контексте концепции алгебраического криптоанализа, в рамках которой данные задачи сводятся к алгебраическим уравнениям над конечными полями, например над полем $GF(2)$. Для решения подобных уравнений могут быть использованы как алгебраические методы, так и алгоритмы решения проблемы булевой выполнимости (SAT). В роли криптографических функций могут выступать различные криптографические примитивы, например алгоритмы блочного и поточного шифрования, а также хеш-функции.

В **п. 2.1** отмечается, что для ряда криптографических примитивов алгебраические атаки имеют рекордные оценки трудоемкости в сравнении с другими методами криптоанализа[8].

В **п. 2.2** приводится известная теорема о существовании эффективной процедуры сведения задачи обращения произвольной дискретной функции к решению систем алгебраических уравнений E_f над полем $GF(2)$ (теорема 1). В рассматриваемой системе E_f присутствуют множества X^{in} и X^{out}, связанные с входом и выходом функции f. Если при подстановке в E_f произвольного

[8]Courtois N.T., Bard G.V. Algebraic Cryptanalysis of the Data Encryption Standard // Cryptography and Coding. Springer, 2007. Vol. 4887. P. 152–169.

$\gamma \in Range\ f$ полученную систему $E_f(\gamma)$ удастся решить, то из найденного решения можно эффективно выделить такой $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$.

В **п. 2.3** рассматривается постановка задачи булевой выполнимости (SAT) в отношении произвольной конъюнктивной нормальной формы (КНФ). Пусть C — произвольная КНФ, а $X, |X| = k,$ — множество всех булевых переменных из этой КНФ. Обозначим через $f_C : \{0,1\}^k \to \{0,1\}$ булеву функцию, которую задает КНФ C. Тогда SAT для КНФ C заключается в том, чтобы определить выполнима ли C. КНФ C называется выполнимой, если существует такой $\alpha \in \{0,1\}^k$, являющийся набором значений переменных из X, что имеет место $f_C(\alpha) = 1$. Если такого α не существует, то C называется невыполнимой.

Для задачи о булевой выполнимости (SAT), так же, как и для систем уравнений над полем $GF(2)$, справедлива теорема об эффективном сведении к ней задачи обращения произвольной дискретной функции (теорема 2). Процедура сведения, рассмотренная в теореме 2, в целом, аналогична процедуре из теоремы 1. КНФ, построенная в соответствии с этой процедурой по алгоритму, задающему рассматриваемую функцию, называется пропозициональной кодировкой задачи обращения данной функции. В настоящей работе для построения пропозициональных кодировок используется система TRANSALG[9], которая позволяет по алгоритмическому описанию произвольной дискретной функции построить т. н. «шаблонную» КНФ (template CNF), в которой выделены множества переменных X^{in} и X^{out}, кодирующие вход и выход рассматриваемой функции.

Для криптографически стойких функций задачи их криптоанализа являются вычислительно трудными. В таких случаях решение данных задач методом грубой силы (brute force attack) — это наименее эффективный метод. Для решения данных задач в **п. 2.4** рассматриваются алгебраические атаки из класса «угадывай-и-определяй» (guess-and-determine, G&D). Для многих криптографических функций удается построить G&D-атаки, которые существенно эффективнее атак методом грубой силы. Такие атаки обычно рассматриваются как свидетельство компрометации соответствующей функции.

Рассмотрим дискретную функцию $f : \{0,1\}^n \to \{0,1\}^m$, которая задана некоторым криптографическим алгоритмом. Пусть E_f — система алгебраических уравнений, построенная по схеме из функциональных элементов S_f, задающей функцию f. Через X^{in} и X^{out} обозначаются множества переменных, приписанных входам и выходам схемы S_f. Можно показать, что подстановка в E_f произвольного $\alpha \in \{0,1\}^n$ в качестве набора значений переменных из X^{in} приведет к выводу по простым правилам значений всех остальных переменных из E_f.

G&D-атака на основе множества угадываемых бит $B \subset X^{in}$, $|B| \ll n$, строится путем подстановки различных наборов значений переменных из B в исходную систему уравнений. Полученные таким образом упрощенные си-

[9]Otpuschennikov I., et al. Encoding cryptographic functions to SAT using TRANSALG system // Proc. of the 22nd European Conference on Artificial Intelligence (ECAI-2016). IOS Press, 2016. Vol. 285. P. 1594–1595.

стемы уравнений решаются при помощи некоторого алгоритма A, время работы которого ограничено некоторой величиной t. При этом общее время, которое тратится на поиск $\alpha : f(\alpha) = \gamma$ в результате перебора различных $\beta \in \{0,1\}^{|B|}$, может оказаться существенно меньше, чем время, которое требуется для атаки методом грубой силы.

В ряде работ описаны эффективные G&D-атаки, в которых ослабленные уравнения криптоанализа решались при помощи алгоритмов решения SAT.

В **п. 2.5** рассматриваются понятия SAT- и UNSAT-иммунности, предложенные Н. Куртуа[10], посредством которых делается попытка определить меру стойкости криптографического примитива (шифра) к алгебраическим атакам. Определения SAT- и UNSAT-иммунности Н. Куртуа дает через понятия SAT- и UNSAT-метода.

Для более точной формулировки данных понятий, а именно для определения меры стойкости криптографической функции к алгебраическим атакам (в том числе, к атакам, использующим алгоритмы решения SAT), применяется метод Монте-Карло.

В **п. 2.6** идеология данного метода используется для точного определения SAT-иммунности. С этой целью вводится специальный класс множеств угадываемых бит, т. н. «инверсные лазейки» (Inverse Backdoor Set, IBS)[11]. В данном пункте также устанавливается важное свойство шаблонной КНФ C_f (теорема 3), которое говорит о том, что применение только правила единичного дизъюнкта (Unit Propagation, UP) к КНФ

$$x_1^{\alpha_1} \wedge \ldots \wedge x_n^{\alpha_n} \wedge C_f,$$

где $\alpha \in \{0,1\}^n$, $\alpha = (\alpha_1, \ldots, \alpha_n)$ — произвольный набор значений переменных из множества X^{in}, приводит к выводу всех значений переменных из C_f.

Рассмотрим множество B, $|B| = s$. Вероятность того, что SAT в отношении КНФ $C_f(\gamma(\alpha), \beta(\alpha))$ решается алгоритмом A за время, не превосходящее t, есть

$$\rho_B = \frac{\#\{\alpha \in \{0,1\}^n : T_A(C_f(\gamma(\alpha), \beta(\alpha))) \leq t\}}{2^n},$$

где $\gamma(\alpha)$ и $\beta(\alpha)$ — наборы значений переменных из множеств X^{out} и B, выведенные по правилу UP в результате подстановки некоторого набора α в шаблонную КНФ C_f. Через $T_A(C_f(\gamma(\alpha), \beta(\alpha)))$ обозначено время, которое тратит алгоритм A на поиск набора, выполняющего КНФ $C_f(\gamma(\alpha), \beta(\alpha))$. Множество B с параметрами $s = |B|, t, \rho_B$ называется инверсной лазейкой (IBS).

G&D-атака на основе IBS B выглядит как анализ произвольных значений $\gamma_1, \ldots, \gamma_r$: для каждого $i \in \{1, \ldots, r\}$ перебираются наборы вида $\beta \in \{0,1\}^{|B|}$

[10] Courtois N.T., et al. Contradiction immunity and guess-then-determine attacks on GOST // Tatra Mountains Mathematical Publications. 2012. Vol. 53(1). P. 2–13.

[11] Semenov A., et al. On cryptographic attacks using backdoors for SAT // Proc. of the 32nd AAAI Conference on Artificial Intelligence (AAAI-2018). 2018. P. 6641–6648.

(т. е. наборы значений переменных из B) с лимитом t времени работы SAT-решателя A. При $r \approx \frac{3}{\rho_B}$ вероятность того, что хотя бы для одного $i \in \{1, \ldots, r\}$ при проверке соответствующего $\beta(\alpha)$ выполняющий набор будет найден алгоритмом A за время, не превышающее t, составит не менее 95%. Таким образом, трудоемкость такой G&D-атаки относительно множества B есть $2^{|B|} \cdot t \cdot \frac{3}{\rho_B}$.

Тогда SAT-иммунность шифра f определяется через G&D-атаку, построенную на основе IBS B, с наименьшей трудоемкостью. Чаще всего G&D-атаки строятся для случая, когда множеством альтернатив для B является множество X^{in}.

В **п. 2.7** приводятся теоретические результаты, аргументирующие точность оценок SAT-иммунности, получаемые при помощи IBS-метода.

Глава 3 содержит основные авторские результаты. Конкретно, приведены новые алгоритмы генерации коллизий для хеш-функций MD4 и MD5, а также эффективные алгоритмы поиска прообразов хеш-функций вида MD4-k, $k \geq 39$. Все построенные атаки используют SAT-подход для решения соответствующих систем алгебраических уравнений.

В **п. 3.1** содержится краткое описание особенностей задач, рассматриваемых в третьей главе. Во-первых, решаются задачи поиска коллизий криптографических хеш-функций MD4 и MD5. Во-вторых, рассматривается задача поиска прообразов неполнораундовых вариантов хеш-функции MD4, а именно задача обращения функции сжатия, которая использует $k, k \leq 48$, шагов базового алгоритма MD4: $f_{MD4-k} : \{0,1\}^{512} \to \{0,1\}^{128}$.

В **пп. 3.2–3.3** задача поиска коллизий хеш-функций семейства MD (с использованием дифференциальных путей С. Ванг) была сведена к проблеме булевой выполнимости при помощи системы TRANSALG. Были построены пропозициональные кодировки для задач поиска одноблоковых коллизий MD4 и двухблоковых коллизий MD5, в которые были подставлены условия из соответствующих дифференциальных путей. Новизна данной части состоит в использовании специальных процедур кодирования дополнительных условий (bit conditions), встроенных в систему TRANSALG. Для решения полученных SAT-задач использовались специальные алгоритмы решения SAT (SAT-решатели).

Для поиска коллизий хеш-функции MD4 использовался SAT-решатель CRYPTOMINISAT, который тратил на поиск 1000 одноблоковых коллизий около 200 секунд работы в однопоточном режиме. Данный результат по эффективности значительно превосходит известную SAT-атаку на хеш-функцию MD4, описанную в статье И. Миронова и Л. Чжана[12].

Задача поиска двухблоковых коллизий хеш-функции MD5, а именно задача поиска первой пары 512-битных блоков, оказалась вычислительно более трудной. Для ее решения использовались многопоточные SAT-решатели, которые запускались на кластере ИДСТУ СО РАН[13]. Каждый решатель запускался

[12] Mironov I., Zhang L. Applications of SAT solvers to cryptanalysis of hash functions // Theory and Applications of Satisfiability Testing (SAT 2006). Springer, 2006. Vol. 4121. P. 102–115.

[13] Иркутский суперкомпьютерный центр СО РАН. URL: http://hpc.icc.ru.

на одном вычислительном узле с лимитом времени в 30 часов. Как результат, была найдена пара искомых блоков, которая содержала 25 первых нулевых бит в каждом блоке сообщения.

Далее была проведена серия вычислительных экспериментов, которая показала, что максимально возможное количество первых нулевых бит, одновременно присутствующих в каждой паре первых блоков, составляет 85. Таким образом, был выделен новый класс двухблоковых коллизий, удовлетворяющих дифференциальному пути С. Ванг, в которых первые 85 бит являются нулевыми. Для задачи поиска пары блоков длиной 512 бит из выделенного класса среднее время поиска составило 9 часов на одном вычислительном узле при помощи SAT-решателя Painless. Задача поиска второй пары блоков решалась в среднем за 500 секунд работы многопоточного SAT-решателя на одном вычислительном узле кластера.

Работы, появившиеся вскоре после дифференциальной атаки С. Ванг, позволяют сделать вывод, что для нахождения коллизий хеш-функций семейства MD можно использовать альтернативные дифференциальные пути. Пример такого дифференциального пути для задачи поиска одноблоковой коллизии хеш-функции MD4 также представлен в п. 3.2.

В **п. 3.4** в контексте SAT-подхода рассматриваются задачи поиска прообразов функций вида $f_{MD4-k} : \{0,1\}^{512} \to \{0,1\}^{128}$. Для решения данных задач используется и развивается идея дополнительных ограничений, впервые предложенная Г. Доббертином для функции f_{MD4-32}. С каждым таким ограничением связывается новая переменная, называемая переменной переключения.

Пусть C_{MD4-k} — шаблонная КНФ для функции вида f_{MD4-k}. Множество X — множество всех булевых переменных в C_{MD4-k}. Предположим, что имеется некоторое множество дополнительных ограничений $R = \{R_1, \ldots, R_q\}$, в котором произвольное $R_j, j \in \{1, \ldots, q\}$, — это формула вида

$$\neg x_{j_1} \wedge \ldots \wedge \neg x_{j_{32}}, \tag{1}$$

где булевы переменные $x_{j_1}, \ldots, x_{j_{32}}$ кодируют 32-битную переменную сцепления на конкретном шаге алгоритма MD4. Везде далее применяются ограничения вида (1), для обозначения которых будет использоваться термин ослабляющие ограничения.

Рассмотрим новое множество булевых переменных (переменных переключения) $S = \{s_1, \ldots, s_q\}$, $S \cap X = \emptyset$. Переменная переключения s_j и ограничение R_j вида (1) связываются формулой

$$C_{R_j} = (\neg s_j \vee \neg x_{j_1}) \wedge \ldots \wedge (\neg s_j \vee \neg x_{j_{32}}).$$

Заметим, что из КНФ $s_j \wedge C_{R_j}$ по правилу UP будут выведены литералы $\neg x_{j_1}, \ldots, \neg x_{j_{32}}$. С другой стороны, очевидно, что $\neg s_j \wedge C_{R_j} \equiv \neg s_j$. В этом случае ограничение R_j не дает никакой дополнительной информации. Таким образом,

булевы переменные переключения, принимающие значение 1, задают некоторый набор «активных» ограничений вида (1).

В **п. 3.5** поиск новых наборов ослабляющих ограничений для задачи обращения функции f_{MD4-k} рассматривается в форме процедуры псевдобулевой оптимизации.

Множество значений переменных переключения из S — это булев гиперкуб $\{0,1\}^q$, следовательно, каждый ненулевой вектор $\lambda \in \{0,1\}^q$ задает некоторый набор ослабляющих ограничений. Рассмотрим КНФ

$$C_{MD4-k} \wedge (\wedge_{j\in\{h_1,\ldots,h_d\}} C_{R_j}), \tag{2}$$

в которой $\{\lambda_{h_1},\ldots,\lambda_{h_d}\}$ — множество компонент вектора λ, принимающих значение 1. Таким образом, КНФ (2) — это шаблонная КНФ C_{MD4-k}, к которой добавлены ослабляющие ограничения вида с номерами $\{h_1,\ldots,h_d\}$.

Мера эффективности набора ослабляющих ограничений, заданного вектором $\lambda \in \{0,1\}^q$, была определена следующим образом. Рассмотрим функцию $\mu : \{0,1\}^q \to \mathbf{N}$, значение которой для произвольного $\lambda \in \{0,1\}^q$ определяется следующим образом:

$$\mu(\lambda) = \#\{l(x) \mid l(x) \leftarrow_{UP} (C_{MD4-k} \wedge (\wedge_{j\in\{h_1,\ldots,h_d\}} C_{R_j})) : x \in X^{in}\}. \tag{3}$$

Запись $l(x) \leftarrow_{UP}$ означает факт вывода литерала $l(x)$ по правилу UP из соответствующей КНФ. Таким образом, значение функции $\mu(\lambda)$ равно числу литералов над переменными из X^{in}, которые выводятся по правилу UP из КНФ C_{MD4-k} после подстановки в нее набора ослабляющих ограничений, которые определяются вектором λ. Для исследования точек $\{0,1\}^q$, в которых значение μ близко к максимально возможному, решается задача максимизации функции (3) на гиперкубе $\{0,1\}^q$. Для этого используется вариант алгоритма поиска с запретами (Tabu Search)[14].

В **п. 3.6** приводятся вычислительные результаты поиска новых ослабляющих ограничений для задачи обращения функции f_{MD4-39} с использованием программной реализации предложенного алгоритма. Более точно, для поиска новых ослабляющих ограничений решалась задача максимизации функции вида (3) на булевом гиперкубе $\{0,1\}^{31}$. Как итог, был найден набор ослабляющих ограничений, заданный вектором значений соответствующих переменных переключения λ_1 из $\{0,1\}^{31}$:

$$\lambda_1 : 0000000001101110111011101000000.$$

Подстановка данного набора ограничений в КНФ для задачи обращения функции f_{MD4-39} в точках 0^{128} и 1^{128} дает вычислительно «легкие» КНФ, для решения которых требуется менее минуты работы однопоточного SAT-

[14] Glover F., Laguna M. Tabu Search. Kluwer Academic Publishers, 1997. 382 p.

решателя MiniSat2.2. Отличительной особенностью ослабляющих ограничений, заданных вектором λ_1, является возможность нахождения прообразов для случайных 128-битных векторов, рассматриваемых в качестве значений функции f_{MD4-39}. Для большинства таких векторов ($\approx 65\%$) среднее время нахождения одного прообраза при помощи решателя MiniSat2.2 составляет меньше 1 минуты. Для остальной части векторов ($\approx 35\%$) было доказано, что соответствующие MD4-39 прообразы, совместные с ограничениями, заданными вектором λ_1, не существуют.

В **п. 3.7** показано, что в ряде случаев задачи обращения функций вида f_{MD4-k} с использованием ослабляющих ограничений можно свести к задачам обращения специальных функций. Напомним, что, исходя из определения меры эффективности μ, в процессе поиска ослабляющих ограничений находятся такие ограничения, подстановка которых в шаблонную КНФ для функции f_{MD4-k} приводит к выводу большого количества значений переменных из множества входных переменных рассматриваемой функции. Например, ослабляющие ограничения, задаваемые вектором λ_1, выводят значения 288 переменных (из 512 возможных) из множества X^{in}.

Обозначим через X^*_λ подмножество в X^{in}, образованное переменными, значения которых не были выведены в результате применения правила UP к КНФ вида (2). Для некоторых λ в множестве X^*_λ можно выделить подмножество $\hat{X}_\lambda$, обладающее следующим важным свойством. Подстановка произвольных значений переменных из данного множества приводит к однозначному выводу значений всех остальных переменных в КНФ (2).

Все сказанное означает, что с произвольным λ, задающим некоторый набор ослабляющих ограничений, можно связать функцию следующего вида:

$$g^\lambda_{MD4-k} : \{0,1\}^{|\hat{X}_\lambda|} \to \{0,1\}^{128}. \quad (4)$$

Один из примеров семейства функций вида (4) дает вектор λ_1, для которого в множестве $X^*_{\lambda_1}$ удается выделить подмножество $\hat{X}_{\lambda_1}$, $|\hat{X}_{\lambda_1}| = 128$. В результате функция $g^{\lambda_1}_{MD4-k}$ имеет вид

$$g^{\lambda_1}_{MD4-k} : \{0,1\}^{128} \to \{0,1\}^{128}.$$

Тот факт, что задача обращения функций f_{MD4-k} сводится к обращению специальных функций вида (4), сформулирован в виде теоремы (теорема 4). При помощи найденных ослабляющих ограничений, заданных вектором λ_1, задача обращения f_{MD4-39} была сведена к обращению именно $g^{\lambda_1}_{MD4-39}$. Задачи обращения различных функций вида g^λ_{MD4-k}, $k > 39$, оказались, в том числе и для вектора λ_1, вычислительно более сложными даже для многопоточных SAT-решателей. Следовательно, для их решения необходимо использовать новые подходы и методы решения. В настоящей работе в роли такого подхода используются атаки из класса «угадывай-и-определяй».

В **п. 3.8** устанавливается ряд важных свойств, введенных выше функций вида (4). Более точно, с использованием вероятностных экспериментов оценивается доля векторов в $\{0,1\}^{128}$, имеющих $g^{\lambda_1}_{MD4-39}$-прообразы и $g^{\lambda_1}_{MD4-40}$-прообразы.

В **п. 3.9** описывается новый класс атак на криптографические хеш-функции вида f_{MD4-k}, которые аргументируют отсутствие у них свойств односторонней функции.

Во многих случаях для демонстрации того факта, что конкретная хеш-функция не удовлетворяет свойствам односторонней функции, достаточно построить атаку обращения (preimage attack), сложность которой существенно меньше, чем сложность атаки методом грубой силы.

Рассмотрим произвольную хеш-функцию вида

$$f : \{0,1\}^n \to \{0,1\}^m, \tag{5}$$

а также задачу поиска по $\gamma \in \{0,1\}^m$ такого $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$. Следствием базовых свойств криптографических хеш-функций является тот факт, что произвольный $\gamma \in \{0,1\}^m$ имеет приблизительно 2^{n-m} прообразов. В случае хеш-функции MD4 вероятность попадания в прообраз γ составляет около $\frac{1}{2^{128}}$. Таким образом, для задачи поиска прообразов криптографических хеш-функций в роли параметра, относительно которого определяется сложность алгоритмов обращения f, следует выбирать не длину входа функции, а длину ее хеш-значения.

Простейший вариант алгоритма поиска прообраза $\gamma \in Range\ f$ заключается в попытке подбора такого $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$. Обозначим через t_0 время вычисления функции f в произвольной точке $\alpha \in \{0,1\}^n$. Определим сложность решения задачи обращения f методом грубой силы как $2^m \cdot t_0$. Отметим, что для произвольной функции вида (5) могут существовать отдельные т. н. «легкие» выходы, задача обращения которых не является вычислительно трудной. Такая ситуация, конечно же, крайне нежелательна в отношении криптографических хеш-функций. Перечисленные выше неформальные соображения приводят к определению следующего типа атак на функции вида (5).

Рассмотрим множество входов $\alpha_1, \ldots, \alpha_r$, которые выбраны случайно (в соответствии с равномерным распределением на $\{0,1\}^n$), и множество соответствующих выходов $\gamma_j = f(\alpha_j)$, $j \in \{1, \ldots, r\}$. Пусть A — некоторый алгоритм, который тратит на решение задачи обращения произвольного $\gamma_j = f(\alpha_j)$, $j \in \{1, \ldots, r\}$, время, не превосходящее t. Если A не находит прообраз γ_j за время t, он прерывает работу и рассматривает следующий выход функции. Обозначим через $P_A(r)$ вероятность события, при котором хотя бы один из выходов γ_j, $j \in \{1, \ldots, r\}$, был обращен алгоритмом A за лимит времени t.

Будем говорить, что определена ALO-атака (от «At Least One») с параметрами $(r, t, P_A(r))$ на функцию вида (5). Скажем, что хеш-функция вида (5) не удовлетворяет свойствам односторонней функции относительно ALO-атаки,

если существует такая ALO-атака с параметрами $(r, t, 0{,}98)$, что $r \cdot t \ll 2^m \cdot t_0$. Существование ALO-атаки с указанными параметрами говорит о том, что среди относительно малого числа случайных входов есть такой, который дает относительно легко обратимый образ с вероятностью, близкой к 1.

В **п. 3.10** построена ALO-атака на функцию f_{MD4-40}. Напомним, что в соответствии с п. 3.9 задача обращения функции $f_{MD4-k} : \{0,1\}^{512} \to \{0,1\}^{128}$ может быть сведена к задаче обращения специальной функции вида

$$g^{\lambda}_{MD4-k} : \{0,1\}^d \to \{0,1\}^{128}, \ d \ll 512, \tag{6}$$

где λ задает некоторый набор ослабляющих ограничений. В рамках ALO-атаки задача обращения функции вида (6) разбивается на несколько подзадач:

1. Оценка доли векторов из $\{0,1\}^d$, на которых функция g^{λ}_{MD4-k} определена.
2. Оценка доли векторов в $\{0,1\}^{128}$, которые имеют прообразы при отображении вида (6).
3. Построение G&D-атаки для задачи обращения функции (6) с использованием IBS-метода. Сложность соответствующей G&D-атаки, построенной на основе множества B, определяется как $2^{|B|} \cdot t \cdot \frac{4}{\rho_B \cdot \delta}$, где δ — оценка доли векторов в $\{0,1\}^{128}$, являющихся образами функции g^{λ}_{MD4-k}.

С использованием описанного метода была построена ALO-атака для функции f_{MD4-40}. Опишем детали данной атаки. При помощи ослабляющих ограничений, заданных вектором λ_1, задача обращения f_{MD4-40} была сведена к задаче обращения $g^{\lambda_1}_{MD4-40}$. В п. 3.8 вероятность δ для $g^{\lambda_1}_{MD4-40}$ была оценена с точностью $\epsilon = 0{,}01$, как $\delta \approx 0{,}4$.

Для фукнции $g^{\lambda_1}_{MD4-40}$ процесс построения G&D-атаки был разбит на два этапа. На первом этапе для поиска «наилучшего» множества угадываемых бит B использовалась MPI-программа PDSAT[15], которая запускалась на пяти вычислительных узлах кластера ИДСТУ СО РАН (180 ядер процессора Intel Xeon E5-2695) на 12 часов. В роли алгоритма A использовался SAT-решатель Rokk с лимитом времени $t = 60$ секунд и объемом выборки $N = 1000$. Обход пространства поиска осуществлялся при помощи алгоритма поиска с запретами (Tabu Search).

В результате было найдено IBS B, состоящее из 20 переменных, с оценкой вероятности $\rho_B = 0{,}126$. На втором этапе данная оценка была пересчитана при помощи вычислительной платформы с процессором Intel Core i7-7700HQ и многопоточного SAT-решателя Painless с лимитом времени $t = 500$ секунд. В данных условиях $\rho_B = 0{,}967$. Итоговая оценка трудоемкости ALO-атаки для

[15]Semenov A., Zaikin O. Algorithm for finding partitionings of hard variants of Boolean satisfiability problem with application to inversion of some cryptographic functions // SpringerPlus. 2016. Vol. 5(1). P. 1–16.

функции f_{MD4-40} составила

$$\approx 2^{20} \cdot 500 \cdot \frac{4}{0{,}967 \cdot 0{,}4} \approx 5\ 421\ 799\ 379 \text{ секунд.}$$

Данная оценка позволяет сделать вывод, что задачу обращения f_{MD4-40} можно решить за 62–63 дня в рамках гипотетического проекта добровольных вычислений, включающем 1000 рабочих станций, оборудованных процессорами Intel Core i7-7700HQ. Такая оценка является реалистичной для современных проектов добровольных вычислений, подобных SAT@home.

В **п. 3.11** приводится ряд новых ослабляющих ограничений, найденных с использованием предложенной техники из п. 3.4, которые дают легко обратимые значения функций f_{MD4-k}, $k \geq 39$. Данные ограничения, задаваемые векторами λ_i из таблицы 1, позволяют строить специальные функции вида $g^{\lambda_i}_{MD4-k} : \{0,1\}^d \to \{0,1\}^{128}$, $d \ll 512$. При этом для некоторых значений параметра k (число шагов алгоритма функции сжатия) задачи поиска прообраза произвольного $\gamma \in Range\ g^{\lambda_i}_{MD4-k}$ решаются за разумное время.

Таблица 1 — Множества новых ослабляющих ограничений, порождающих функции вида $g^{\lambda_i}_{MD4-k}$, для которых задачи обращения решаются в среднем за время меньше t при помощи однопоточного SAT-решателя

	Ослабляющие ограничения	$\lvert X_\lambda \rvert$	$\lvert \hat{X}_\lambda \rvert$	k	t
λ_1	00000000011011101110111010000000000000000	288	128	39	12
λ_2	00000000011011101110111011000000000000000	320	96	43	4,5
λ_3	00000000111011101110111010000000000000000	320	96	44	20
λ_4	00000101111110111011101000000000000000000	320	64	41	5,7
λ_5	00000000111011101110111011000000000000000	448	64	47	914
λ_6	00000000111011101110111011100000000000000	480	32	48	500

В таблице 1 для каждого вектора λ_i приводятся характеристики ослабляющих ограничений, задаваемых данным вектором: $|X_\lambda|$ — количество переменных из множества X^{in}, выведенных по правилу UP, $|\hat{X}_\lambda|$ — размер входа функции $g^{\lambda_i}_{MD4-k}$, k — число шагов базового алгоритма MD4, t — верхняя граница времени решения соответствующей задачи при помощи SAT-решателя Rokk.

Наиболее интересными выглядят ограничения, задаваемые вектором λ_6, после подстановки которых в шаблонную КНФ по правилу UP выводятся 480 переменных из множества X^{in}. При этом остальные 32 переменные — это переменные, кодирующие вход функции $g^{\lambda_6}_{MD4-48}$.

Вычислительные эксперименты показали, что для $k = 48$ задача обращения произвольного $\gamma \in Range\ g^{\lambda_6}_{MD4-48}$ решается в среднем за время меньше 500 секунд при помощи однопоточного SAT-решателя. Несмотря на то, что доля таких «легких выходов» в множестве $\{0,1\}^{128}$ крайне мала, данный подход позволяет за разумное время предъявить соответствующие MD4-прообразы, при

этом количество таких прообразов, исходя из оценки, полученной способом из п. 2.7, близко к 2^{32}.

В **заключении** сформулированы основные результаты научной работы.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

Выполненная работа посвящена разработке новых методов решения задач криптоанализа хеш-функций семейства MD, в основу которых положены алгоритмы и технологии решения проблемы булевой выполнимости (SAT). В рамках проведенного исследования получены следующие результаты:

1. Для задачи поиска коллизий криптографических хеш-функций семейства MD с использованием SAT-подхода выделен новый класс двухблоковых коллизий MD5, а также построены новые дифференциальные пути для задачи поиска одноблоковых коллизий MD4.
2. Разработан и реализован метод автоматического синтеза дополнительных ограничений для задач поиска прообраза неполнораундовых версий хеш-функции MD4.
3. Построена рекордная по трудоемкости атака обращения (preimage attack) на хеш-функцию MD4-39.
4. Построена оценка трудоемкости алгебраической атаки обращения из класса атак «угадывай-и-определяй» (guess-and-determine) на функцию MD4-40.
5. Найдены множества легко обратимых значений хеш-функций MD4-k, $k \geq 39$, в том числе для $k = 48$.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в журналах из перечня ВАК:

1. Богачкова (Грибанова), И.А. Задачи поиска коллизий для криптографических хеш-функций семейства MD как варианты задачи о булевой выполнимости / И.А. Богачкова (Грибанова), О.С. Заикин, С.Е. Кочемазов, И.В. Отпущенников, А.А. Семёнов, О.О. Хамисов // Вычислительные методы и программирование. Новые вычислительные технологии. — 2015. — Т. 16. — С. 61–77. — (doi.org/10.26089/NumMet.v16r107).

2. Gribanova, I.A. Preimage attack on MD4 hash function as a problem of parallel SAT-based cryptanalysis / I.A. Gribanova, O.S. Zaikin, I.V. Otpuschennikov, A.A. Semenov // Вестник Южно-Уральского государственного университета. Сер. Вычислительная математика и информатика. — 2017. — Т. 6. — С. 16–27. — (doi.org/10.14529/cmse170302).

Статьи в изданиях, индексируемых в Web of Science и Scopus:

3. Otpuschennikov, I. Encoding Cryptographic Functions to SAT Using Transalg System / I. Otpuschennikov, A. Semenov, I. Gribanova, O. Zaikin,

S. Kochemazov // Proc. of the 22nd European Conf. on Artificial Intelligence (ECAI 2016). Frontiers in Artificial Intelligence and Applications. — IOS Press, 2016. — Vol. 285. — P. 1594–1595. — (doi.org/10.3233/978-1-61499-672-9-1594).

4. Gribanova, I. The study of inversion problems of cryptographic hash functions from MD family using algorithms for solving boolean satisfiability problem / I. Gribanova, O. Zaikin, S. Kochemazov, I. Otpuschennikov, A. Semenov // Proc. of the Intern. Conf. Mathematical and Information Technologies (MIT-2016). — CEUR-WS, 2017. — Vol. 1839. — P. 98–113.

5. Gribanova, I. Using Automatic Generation of Relaxation Constraints to Improve the Preimage Attack on 39-step MD4 / I. Gribanova, A. Semenov // Proc. of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2018). — IEEE, 2018. — P. 1174–1179. — (doi.org/10.23919/MIPRO.2018.8400213).

Статьи в других изданиях:

6. Богачкова (Грибанова), И.А. Применение алгоритмов решения проблемы булевой выполнимости к криптоанализу хеш-функций семейства MD / И.А. Богачкова (Грибанова), О.С. Заикин, С.Е. Кочемазов, И.В. Отпущенников, А.А. Семёнов // Прикладная дискретная математика. Приложение. — 2015. — № 8. — С. 139–142. — (doi.org/10.17223/2226308X/8/54).

7. Грибанова, И.А. Применение алгоритмов решения проблемы булевой выполнимости к построению разностных путей в задачах поиска коллизий криптографических хеш-функций семейства MD / И.А. Грибанова // Прикладная дискретная математика. Приложение. — 2016. — № 9. — С. 129–132. — (doi.org/10.17223/2226308X/9/51).

8. Gribanova, I. Using parallel SAT algorithms to study the inversion of MD4 hash function / I. Gribanova, O. Zaikin, I. Otpuschennikov, A. Semenov // Материалы конф. «Параллельные вычислительные технологии (ПаВТ) 2017» (г. Казань, 3–7 апреля 2017 г.). — Казань: Казанский (Приволжский) федеральный университет, 2017. — С. 100–109.

9. Грибанова, И.А. Обращение криптографических хеш-функций с использованием несбалансированных приближений раундовых функций / И.А. Грибанова // Прикладная дискретная математика. Приложение. — 2017. — № 10. — С. 157–160. — (doi.org/10.17223/2226308X/10/61).

10. Грибанова, И.А. Новый алгоритм порождения ослабляющих ограничений в задаче обращения хеш-функции MD4-39 / И.А. Грибанова // Прикладная дискретная математика. Приложение. — 2018. — № 11. — С. 139–141. — (doi.org/10.17223/2226308X/11/43).

11. Gribanova, I.A. Parallel Guess-and-determine Preimage Attack with Realistic Complexity Estimation for MD4-40 Cryptographic Hash Function / I.A. Gribanova, A.A. Semenov // Материалы конф. «Параллельные вычислительные технологии (ПаВТ) 2019» (г. Калининград, 2–4 апреля 2019 г.). — Калининград: Балтийский федеральный университет, 2019. — С. 8–18.