АННОТАЦИЯ

диссертационной работы Сақан Қайрат Сақанұлы на тему: «Разработка алгоритмов хеширования на основе итеративных блочных шифров и исследование их криптостойкости», представленной на соискание степени доктора философии (PhD) по образовательной программе «8D06301 – Системы информационной безопасности»

Актуальность темы исследования. В эпоху стремительного развития современных электронных устройств, средств связи и интернет-технологий для обеспечения безопасности информации в основном используются криптографические методы – системы шифрования и хеширования.

Хеш-функции широко используются в электронных системах, начиная от защиты паролей и ключей, проверки целостности и аутентификации и заканчивая технологией блокчейн, а также в области постквантовой криптографии. Так как квантовый компьютер обеспечивает всего лишь квадратичное ускорение в решении задачи нахождения прообраза для хеш-функции, криптографические алгоритмы на основе хеш-функций могут с успехом использоваться и в постквантовой криптографии.

На сегодняшний день с помощью новых конструкций и способов проектирования разрабатывается множество новых систем и моделей защиты данных. Однако расширение возможностей информационных технологий и стремительное развитие вычислительных мощностей приводит к появлению новых специализированных атак и модифицированных вариантов существующих атак. В связи с этим возникает необходимость постоянно разрабатывать и обновлять системы защиты информации, в том числе существующие модели и системы хеширования, то есть разрабатываемые хеш-функции должны проходить строгие проверки по свойствам безопасности.

Основным преимуществом хеш-функций, построенных на основе блочного шифра, является использование хорошо изученных криптографических примитивов и конструкций. Также в блочном шифре можно регулировать требуемый уровень безопасности и производительности хеш-функций за счет внесения изменений в такие параметры как длина блока и ключа и число раундов. Использование криптостойкого блочного шифра в алгоритме хеширования позволяет затруднить применение методов линейного и дифференциального криптоанализа для поиска коллизий, а также первого и второго прообраза. Углубленный анализ компонентов блочного шифра, используемых при разработке хеш-функций, а также роль хеш-функций в современных технологиях требуют непрерывного и целенаправленного научного исследования.

Основным направлением диссертационной работы является разработка нового алгоритма хеширования на основе блочного шифра, обеспечивающего высокий уровень безопасности и вычислительной производительности.

С учетом того, что сейчас для защиты информации в электронных системах Республики Казахстан в основном используются международные стандарты, криптографические средства и программное обеспечение иностранного производства, создание отечественных систем хеширования данных является безусловно актуальным и необходимым вопросом.

Цель диссертационной работы. Разработка безопасного и высокопроизводительного алгоритма хеширования на основе блочного шифра, адаптированного к программно-аппаратной реализации и параллельным вычислениям, а также исследование его свойств безопасности и эффективности.

Задачи исследования, реализующие цель диссертационного исследования:

– проведение обзора и анализа современных хеш-функций, методов исследования коллизий в хеш-функциях, изучение видов атак и методов криптоанализа;

– разработка нового алгоритма блочного шифрования, используемого в качестве сжимающей функцией;

– разработка нового алгоритма хеширования на основе блочного шифра;

– исследование свойств безопасности разработанного алгоритма хеширования с применением наборов статистических тестов, критерием лавинного эффекта, методов криптоанализа и «близких коллизий»;

– программная и программно-аппаратная реализация разработанного алгоритма хеширования и оценка его эффективности.

Объект исследования: системы шифрования и криптографические хеш-функции.

Предмет исследования:

– разработанный алгоритм блочного шифрования с особой архитектурой таблиц замены, использующий S-блоки малой размерности;

– разработанный алгоритм хеширования на основе блочного шифра, использующегося в качестве функции сжатия.

Методы исследования: теория булевых функций, линейная алгебра, теория вероятности и математическая статистика, методы криптографического анализа и типы атак для исследования хеш-функций, лавинный эффект.

Научная новизна исследования:

– разработан новый симметричный алгоритм блочного шифрования для применения в алгоритме хеширования;

– разработан новый алгоритм хеширования на основе блочного шифра, адаптированный для параллельных вычислений и программно-аппаратной реализации;

– предложена новая схема сопряженного применения четырех 4-битных S-блоков относительно индексов элемента матрицы, применение которой позволяет повысить безопасность алгоритма и более эффективно использовать память микросхемы в аппаратной реализации;

– предложена новая схема применения нелинейного преобразования в функции сжатия, которая позволяет уменьшить число раундов;

– предложена возможность выбора k частей блока хеширования относительно размера исходного хешируемого сообщения, что в свою очередь, повышает производительность вычислений (k=3,…, 8, k – количество частей).

Теоретическая и практическая значимость работы. Теоретическая и практическая ценность полученных результатов в ходе проведенных научных исследований повышает возможность использования криптографических средств защиты информации в электронных устройствах, специальных системах передачи и хранения данных, что в дальнейшем открывает новые возможности для развития отечественных информационных систем.

Разработанный алгоритм хеширования HBC-256 был включен как отдельный раздел в монографии «Разработка и исследование алгоритмов хеширования произвольной длины» издательства «Guppyprint» г. Алматы (ISBN 978-601-08-2549-9, с. 95).

Результаты исследовательской работы опубликованы в международных научных журналах, индексируемых в базе данных SCOPUS и Web of Science, а также в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МНВО РК (Приложение А в диссертации).

Результаты исследований данного алгоритма хеширования, полученные зарубежными учеными, были включены в сборник работ летней школы-конференции «Криптография и информационная безопасность», организованной Новосибирским государственным университетом и «Криптографическим центром» (г. Новосибирск) по теме «Исследование криптографических свойств новых функций хеширования HBC и HAS01».

Национальным институтом интеллектуальной собственности МЮ РК выдано 1 авторское свидетельство на научное произведение и 3 авторских свидетельства на программное обеспечение алгоритма хеширования HBC-256 (Приложение Ә в диссертации).

Главный вывод защиты. На основе блочного шифра разработан новый алгоритм хеширования, адаптированный к программно-аппаратной реализации и параллельным вычислениям. Безопасность и эффективность разработанного алгоритма хеширования обоснована с применением наборов статистических тестов, критерия лавинного эффекта, метода «близких коллизий», а также методов дифференциального, линейного и алгебраического криптоанализа. В условиях новейших технологических мощностей разработанный алгоритм хеширования позволяет повысить его криптографическую стойкость и эффективность применения.

Уровень достоверности и результаты апробации. Достоверность проведенных исследований и полученных результатов диссертации показана в третьем разделе диссертации.

Результаты исследования представлены на следующих научно-практических конференциях, а также на научных семинарах отечественных и

зарубежных научно-исследовательских институтов и высших учебных заведений (Приложение Б в диссертации):

– V, VI и VII международные научно-практические конференции «Информатика и прикладная математика» (Алматы, 2020-2022 гг.);

– международная научно-практическая конференция «Актуальные проблемы информационной безопасности в Казахстане» (АПБИК-2021, Алматы, 11 июня 2021г.);

– международная научная конференция в области информационных технологий, посвященной 75-летию профессора У.А. Тукеева (Алматы, 8 октября 2021г.);

– IV международная научно-техническая конференция «Минские научные чтения-2021. Передовые технологии и материалы будущего» (Минск, Беларусь, 9-10 декабря 2021г.);

– международная конференция «Computer Data Analysis and Modeling: Stochastics & data Science» (CDAM-2022, Минск, Беларусь, 6-9 сентября 2022г.);

– научный семинар факультета «Кибербезопасности, компьютерной и программной инженерии» Национального авиационного университета Украины (Киев, Украина, 3.12.2021 г.);

– научный семинар «Научно-исследовательского института прикладных проблем математики и информатики» при Белорусском государственном университета (Минск, Беларусь, 6 сентября 2022 г.);

– научный семинар факультета Electrical Engineering and Computer Science Department of Khalifa University (Абу-Даби, ОАЭ, 12 декабря 2022г.);

– научные семинары «Института информационных и вычислительных технологии» и факультета информационных технологий КазНУ им. Аль-Фараби (2020-2023гг., Алматы).

Связь темы диссертации с планами научно-исследовательских работ. Диссертационная работа выполнена в соответствии с планом докторской диссертации, утвержденном Институтом информационных и вычислительных технологий КН МНВО РК и с планом научно-исследовательских работ проекта ПЦФ OR11465439 «Разработка и исследование алгоритмов хеширования произвольной длины для цифровых подписей и оценка их стойкости». Результаты проведенных исследований по данной диссертационной работе включены в отчеты данного проекта ПЦФ за 2021-2022 годы и получен акт внедрения (Приложение В в диссертации).

Публикация результатов. В ходе проведения научного исследования по теме диссертации опубликовано 24 научных работ. Из них 7 статей опубликованы в журналах, индексированных в базах Scopus и Web of Science, 1 монография, 7 статей – в изданиях, рекомендованных Комитетом по контролю в сфере образования и науки МНВО РК, 10 статей в сборниках международных и отечественных научно-практических конференций и других научных журналах.

Объем и структура работы. Диссертационная работа состоит из введения, четырех разделов, заключения, списка источников и приложений.

Объем диссертации – 103 страницы, в том числе 30 рисунков, 28 таблиц, 99 источников и 6 приложений.

Во введении представлено обоснование актуальности темы диссертации. Были сформулированы цель, объект и предмет исследовательской работы, также приведены сведения о научной новизне, практической значимости, публикациях и апробаций результатов работы.

В первом разделе представлены сведения об основных понятиях, терминах и разновидностях хеш-функций. Описаны требования, предъявляемые к хеш-функциям и выделены их основные свойства. В конце раздела перечисляются критерии оценки качества хеш-функций и классификации атак на них.

Во втором разделе описан алгоритм хеширования HBC-256, разработанный на основе блочного шифра и удовлетворяющий всем требованиям, предъявляемые к хеш-функциям. В качестве блочного шифра рассматривается новый алгоритм шифрования CF, спроектированный по SP-сети. В разделе подробно описаны криптографические примитивы и преобразования, используемые при разработке алгоритма шифрования CF. С целью повышения вычислительной эффективности представлена новая схема, минимизирующая количество раундов. Для экономии памяти микросхемы используются четыре 4-битные таблицы замены S-блока и показан принцип их эффективного использования.

В третьем разделе представлены результаты проведенной работы по оценке безопасности разработанного алгоритма хеширования HBC-256. Приведена оценка сложности атак на данный алгоритм, а также по наборам статистических тестов NIST и Д. Кнута оценивается уровень статистической безопасности алгоритма. Рассмотрен лавинный и строгий лавинный эффекты, описывающие связь между исходным сообщением и хеш-значением. Также оцениваются возможности нахождения коллизий методами «близких коллизий», дифференциального, линейного и алгебраического криптоанализа.

В четвертом разделе приведены сведения о программной и программно-аппаратной реализации разработанного алгоритма хеширования. Приведены основные характеристики алгоритма HBC-256 по типам реализации, оценена их вычислительная производительность, а также представлены данные сравнительного анализа относительно других алгоритмов хеширования.

В заключении отражены результаты исследовательской работы и дается их краткая оценка.