Отзыв научного консультанта на диссертационную работу
Сақан Қайрат Сақанұлы
«Разработка алгоритмов хеширования на основе итеративных блочных шифров и исследование их криптостойкости», представленную на соискание ученой степени доктора философии (PhD) по образовательной программе – «8D06301 – Системы информационной безопасности»

В современном информационном мире одной из ключевых задач является обеспечение безопасности и достоверности информации. Множество информационных систем, включая IoT устройства, используют различные криптографические преобразования для обеспечения информационной безопасности при хранении и передаче данных. Одним из базовых криптографических преобразований, используемых в различных задачах обеспечения безопасности, являются хеш-функции. Современные хеш-функции используются для осуществления различных процедур защиты информации, таких как аутентификация пользователей, контроль целостности данных, электронная подпись, формирование транзакций криптовалют, поиск вредоносного программного обеспечения, оптимизация алгоритмов биометрической идентификации. Как известно, построение хеш-функций на основе блочных шифров – самый популярный и устоявшийся подход, в которым функция сжатия представляется блочным шифром, где на его вход подаются блок сообщения и хеш-значение предыдущей итерации. Безопасность таких хеш-функцией основывается стойкостью используемого шифра.

В процессе реализации плана диссертационной работы соискателем проведен анализ трудов зарубежных и отечественных ученых, занимающихся по данному направлению, а также изучены современные алгоритмы хеширования для различных целей, в том числе облегченные алгоритмы хеширования и алгоритмы хеширования для технологии блокчейн.

В результате проведенных научно-исследовательских работ соискателем разработан новый алгоритм хеширования HBC-256 на основе предложенного им итеративного блочного шифра CF. Для построения хеш-функции использована конструкция Меркля-Дамгарда с модификацией Wide-pipe, а для обеспечения необратимости, т. е. невозможности восстановления исходного сообщения из хеш-значения, схема Девиса-Мэйера. При проектировании алгоритма CF с целью повышения безопасности была использована новая схема применения нелинейного узла, которая позволила существенно снизить число раундов шифрования. Предложенная схема хеширования алгоритма HBC-256 разработана для параллельного вычисления, что позволяет существенно повысить его производительность.

В работе большое внимание уделено проведению анализа безопасности разработанного алгоритма хеширования HBC-256 с применением методов криптографического анализа, а также наборов статистических тестов NIST и Д. Кнута. Кроме того, проведена оценка степени лавинного и строго лавинного

эффектов, а также получена практическая оценка поиска «близких коллизиий» в хеш-значениях.

Все результаты исследования по безопасности алгоритма HBC-256 оценены положительно, основные требования, предъявляемые к хеш-функциям, выполняются и алгоритм обладает всеми свойствами надежно спроектированных хеш-функций.

Осуществлены программная и аппаратная реализации предложенного алгоритма хеширования HBC-256. Программная реализация предназначена для получения хеш-значений данных произвольной длины и проверки целостности файлов на основе сравнения хеш-значений. Разработан также макетный образец программно-аппаратного комплекса, реализующий алгоритм хеширования HBC-256.

Данная работа проводилась в рамках выполнения проекта программно-целевого финансирования OR11465439 «Разработка и исследование алгоритмов хеширования произвольной длины для цифровых подписей и оценка их стойкости». Полученные результаты включены в отчёты указанного проекта ПЦФ в 2021-2022 гг. Полученные соискателем научные результаты регулярно представлялись на научных семинарах Лаборатории информационной безопасности Института информационных и вычислительных технологий КН МНВО. Результаты диссертационной работы соискателя также обсуждались на научных семинарах зарубежных научных организаций: в Белорусском государственном университете (г. Минск, Беларусь), Национальном авиационном университете (г. Киев, Украина), Университете Халифа (г. Абу Даби, ОАЭ), на которых были получены объективные оценки и конкретные рекомендации, которые были учтены в дальнейшей при выполнении его работы.

Особо отмечаю его ответственное отношение к выполнению научно-исследовательской работы и профессионализм. За период обучения в докторантуре соискатель самостоятельно выполнил поставленные ему задачи и полностью решил их за время обучения.

Соискателем за период обучения в докторантуре опубликовано 24 научные работы, в том числе 7 статей опубликованы в журналах, индексируемых в базе данных Scopus и Web of Science, из них 4 – по теме исследования.

На основании вышеизложенного считаю, что диссертационная работа Сакана К. С. «Разработка алгоритмов хеширования на основе итеративных блочных шифров и исследование их криптостойкости» является завершенной научной работой, результаты которой имеют научное и практическое значение и соответствует предъявляемым требованиям к диссертациям по образовательной программе «8D06301 – Системы информационной безопасности», а соискатель Сакан К.С. заслуживает допуска к защите диссертации на соискание ученой степени доктора философии (PhD).

Отечественный научный консультант д.т.н. Нысанбаева С.Е.