Отзыв

научного консультанта на диссертационную работу

Алғазы Күнболат Тілеуханұлы

на тему «Разработка и исследование алгоритмов шифрования на базе различных подходов», представленную на соискание ученой степени доктора философии (PhD) по специальности – «6D100200 - Системы информационной безопасности»

Диссертационная работа Алғазы К.Т. посвящена разработке и исследованию симметричного блочного алгоритма шифрования. Представленная к защите диссертация выполнена на актуальную тему, связанную с обеспечением информационную безопасности. В Республике Казахстан в 2017 г. принята Концепция «Киберщит Казахстана». В ней указывается на необходимость проведения отечественных разработок в области криптографической защиты информации и постепенную замену зарубежных средств защиты информации на отечественные. Основная цель таких программ, предлагаемых государством – создание современного информационного общества с использованием возможностей современной науки и технологий. А в информационном обществе обеспечение информационной безопасности одна из самых актуальных проблем. Известно, что в развитых странах существуют собственные алгоритмы защиты информации, соответствующие государственному стандарту криптографической защиты информации, что в свою очередь формирует надежное государство.

В процессе работы над диссертационной работой Алғазы К.Т. проанализировал современные алгоритмы защиты информации, работы зарубежных и отечественных ученых. В результате проведенных исследований был разработан новый алгоритм шифрования, а также предложена вторая версия этого алгоритма с использованием ключей на основе непозиционных полимиальных систем счисления (НПСС).

В диссертационной работе приведены результаты подробного исследования разработанного алгоритма. Исследование криптографической стойкости алгоритма начинается с криптоанализа каждого преобразования. Затем, в зависимости от полученных результатов, анализируется алгоритм в целом. Исследование надежности алгоритма проводилось с использованием статистического анализа зашифрованных текстов, полученных с помощью алгоритма шифрования, и проверки лавинного эффекта алгоритма. Также проводились статистические исследования последовательности ключей, полученных с использованием алгоритма генерации раундовых ключей. Один из наиболее распространенных современных методов – это атаки, основанные на линейном и дифференциальном криптоанализе. Были проведены исследования стойкости разработанного алгоритма к этим атакам. Также приведены результаты атаки методом бумеранга и алгебраических атак, таких как XL и XSL. Известно, что стойкость многих алгоритмов к дифференциальному и линейному криптоанализу обеспечивают S-блоки.

Это, в свою очередь, привело к обширным исследованиям свойств S-блоков. Также были изучены S-блоки, используемые в алгоритме. Была получена система уравнений, необходимая для алгебраических атак на S-блок.

Кроме того, было проведено отдельное исследование алгоритма шифрования на основе НПСС. В работе показано, что использование в шифровании непозиционных систем счисления увеличивает криптографическую стойкость алгоритма. Применение таких методов криптоанализа, как дифференциальный, линейный и другие, не является эффективным.

Исследовательская работа выполнялись в рамках проекта программно-целевого финансирования КН МОН РК «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» - BR05236757 (2018-2020 гг.)

Результаты диссертационного исследования имеют научное и практическое значение, использование которых обеспечивает решение проблемы информационной безопасности, важной для развития цифрового потенциала страны. Основные результаты диссертационной работы опубликованы в научных журналах, индексируемых базой Scopus, Thomson Reuters и в изданиях, рекомендованных Комитетом по контролю в сфере образовании и науки МОН РК. Также, доложены на международных и отечественных конференциях и семинарах.

За годы обучения соискатель продемонстрировал способность самостоятельно проводить теоретические и экспериментальные исследования, а также решать научные задачи. Его отличает профессионализм и ответственность в выполнении исследовательской работы.

Диссертационная работа Алғазы К.Т. на тему «Разработка и исследование алгоритмов шифрования на базе различных подходов» удовлетворяет всем требованиям Комитетом по контролю в сфере образовании и науки МОН РК и считаю, что автор исследования заслуживает степень доктора философии (PhD) по специальности «6D100200 - Системы информационной безопасности».

Научный консультант
д.т.н., профессор Р.Г. Бияшев

КАДР БӨЛІМІ