Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО
ITMO University

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ / OBJECTIVES FOR A GRADUATION THESIS

Обучающийся / Student Игнатьева Ксения Евгеньевна
Группа/Group N3451
Факультет/институт/кластер/ Faculty/Institute/Cluster факультет безопасности информационных технологий
Квалификация/ Degree level Бакалавр
Направление подготовки/ Subject area 10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы/Major Технологии защиты информации 2017
Специализация/ Specialization
Тема ВКР/ Thesis topic Разработка алгоритма обеспечения защищенного взаимодействия на основе криптосистемы McEliece с использованием кодов с малой плотностью проверок на четность
Руководитель ВКР/ Thesis supervisor Таранов Сергей Владимирович, кандидат технических наук, Университет ИТМО, факультет безопасности информационных технологий, доцент (квалификационная категория "ординарный доцент")

Срок сдачи студентом законченной работы до / Deadline for submission of complete thesis 31.05.2021

Техническое задание и исходные данные к работе/ Requirements and premise for the thesis
Цель: снижение размера ключа криптосистемы McEliece за счёт компактного способа представления порождающей матрицы LDPC-кода. Техническое задание: 1. Провести анализ существующих классов криптосистемы McEliece. 2. Выявить преимущества и недостатки рассмотренных систем, в частности криптосистемы McEliece, использующей LDPC-коды. 3. Проанализировать существующие классы LDPC-кодов на применимость к криптосистеме McEliece, выделить недостатки этой системы. 4. Разработать алгоритм, основанный на криптосистеме McEliece с использованием LDPC-кодов, решающий проблему длины ключа. 5. Разработать систему показателей эффективности для исследуемых методов защиты. 6. Провести оценку эффективности разработанного алгоритма и сравнить с аналогами. Исходные данные к работе: 1. Классы криптосистемы McEliece: - с использованием кодов Гоппы; - с использованием кодов Рида-Соломона; - с использованием кодов Рида-Маллера; - являющиеся комбинацией оригинальной криптосистемы McEliece и McEliece с использованием LDPC-кодов; - с использованием LDPC-кодов. 2. Методы защиты информации в криптосистемах на основе помехоустойчивого кодирования: - коды Гоппы; - коды Риды-Соломона; - коды Рида-Маллера; - LDPC и QC-LDPC коды. 3. Методы кодирования и декодирования LDPC кодов, способы построения проверочных матриц, информация о различных классах LDPC кодов.

Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов)/ Content of the thesis (list of key issues)

1. Анализ существующих классов криптосистемы McEliece.
2. Описание разработанного алгоритма, решающего проблему длины ключа в системе McEliece, использующую LDPC-коды.
3. Описание разработанной системы показателей и критериев оценки эффективности для исследуемых методов защиты.
4. Оценка эффективности разработанного алгоритма и сравнение с аналогами.

Перечень графического материала (с указанием обязательного материала) / List of graphic materials (with a list of required material)

1. Блок-схема разработанного алгоритма обеспечения защищенного взаимодействия.
2. Таблица преимуществ и уязвимостей классов криптосистемы McEliece.
3. Сравнительная таблица результатов оценки эффективности разработанного алгоритма и аналогов.

Исходные материалы и пособия / Source materials and publications

1. Biswas B., Sendrier N. Lecture Notes in Computer Science//McEliece Cryptosystem Implementation: Theory and Practice, 2008, С. 47-62.
2. Berger T.P., Cayrel P.-L., Gaborit P., Otmani A. Reducing Key Length of the McEliece Cryptosystem, 2014, С. 77-97.
3. Красавин А.А. Труды МФТИ//Использование модифицированной (U|U+V)-конструкции в криптосистеме McEliece, 2018, Т. 10, N 2, С. 109-113.
4. Branco P., Mateus P., Salema C., Souto A. Information Sciences//Using Low-Density Parity-Check codes to improve the McEliece cryptosystem, 2020, N 510, С. 243-255.
5. Baldi M. LDPC codes in the McEliece cryptosystem: attacks and countermeasures. – Ancona, Italy: Polytechnic University of Marche, 2009. – 15 с.

Дата выдачи задания/ Objectives issued on 16.03.2021

СОГЛАСОВАНО / AGREED:

Руководитель ВКР/ Thesis supervisor

Документ подписан
Таранов Сергей Владимирович
16.03.2021

(эл. подпись)

Таранов Сергей Владимирович

Задание принял к исполнению/ Objectives assumed by

(эл. подпись)

Руководитель ОП/ Head of educational program

(эл. подпись)