МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра комп'ютерної алгебри та дискретної математики

(повна назва кафедри (предметної, циклової комісії))

Дипломна робота

магістра

(освітньо-кваліфікаційний рівень)

на тему «Циклічні коди та їх застосування в криптографії»
«Циклические коды и их применение в криптографии»
«Cyclic codes and their use in cryptography»

Виконав: студент денної форми навчання
напряму підготовки 123– Комп'ютерна інженерія.

(шифр і назва напряму підготовки, спеціальності)

Чан Ван Ань

(прізвище, ім'я, по-батькові)

Керівник: Проф., доктор фіз.-мат. наук, Варбанець П. Д.

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент: доц., к. фіз.-мат. наук, Симонова І.Г.

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент:_____

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рекомендовано до захисту:

Протокол засідання кафедри

№_____ від «___»_____ 2019р.

Завідувач кафедри

_____ Варбанець П. Д.

(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___

протокол № __ від «_»__ ____ 2019 р.

Оцінка _____/_____/_____

(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

_____ _____

(підпис) (прізвище, ініціали)

Одеса - 2019

ЗМІСТ

1. ВВЕДЕНИЕ

При разработке и создании распределенных автоматизированных систем обработки информации и управления (АСОИУ) центральной проблемой на протяжении многих лет является защита информации от случайных ошибок и преднамеренных угроз. Обычно эту проблему разделяют на две: проблему повышения достоверности информации при ее передаче и хранении и проблему информационной безопасности.

Для решения первой используется аппарат теории информации и теории помехоустойчивого кодирования.

Для решения второй проблемы до сих пор не существует единого математического аппарата. Частично проблема информационной безопасности АСОИУ решается криптографическими преобразованиями, частично системами управления доступом, в основе математических моделей которых лежит теория множеств. В основе построения современных криптографических систем лежит теория сложности алгоритмов. Одной из самых перпективных задач этой теории для целей криптографии в настоящее время считает задача декодирования неизвестного (случайного) линейного блокового кода. В настоящее время известно несколько криптографических систем, построенных на базе помехоустойчивых кодов. Лучшими из этих конструкций являются криптосистемы, использующие коды Гоппы.

Коды Гоппы образуют семейство двоичных линейных кодов, задаваемых многочленом Гоппы $G(x)$ степени t с коэффициентами из конечного поля $GF(2^m)$ и подмножеством $L = (a_i, \ldots, a_n)$ этого поля таким, что элементы a^* не являются его корнями $G(x)$. Известны границы на их размерность и минимальное кодовое расстояние, а также быстрые (полиномиальные по времени) алгоритмы декодирования, реализующие конструктивное расстояние кода. Множество неподвижных точек кода относительно действия группы Фробениуса задает код меньшей длины,

который называется $s-$проекционным кодом. Для нового семейства кодов можно получить границы на их размерность и минимальное расстояние, а также перенести на них некоторые результаты, известные для кодов Гоппы, в частности, оценки точности нижней границы на размерность кода для случая, когда степень многочлена Гоппы мала. Кроме того, на основе стандартного алгоритма декодирования кодов Гоппы будет построена полиномиальная декодирующая процедура, позволяющая исправлять ошибки до половины конструктивного расстояния проекционного кода.

Хорошо корректирующая способность кодов Гоппы позволяет использовать их в криптографии. Впервые на возможность строить криптографические системы с помощью линейных кодов обратил внимание Мак Элайес, его идею развил Г. Нидеррайтер. В нашей работе мы показали как, используя перестановочные матрицы и код Гоппы можно шифровать и расшифровывать секретные сообщения с высокой надёжностью относительно взламывания криптосистемы. Нами создан программный продукт, который обеспечивает хорошую скорость шифрования в двоичном алфавите.

ВЫВОДЫ

Изложенные в работе сведение о циклических кодах (и, в частности, о кодах Гоппа) позволяют утверждать, что такие коды обладают хорошей скоростью кодирования, высокой разрешающей способностью, достаточно простой реализуемостью. Теория кодов Гоппа допускает дальнейшие обобщения, в частности , можно исследовать коды Гоппа в алфавите F_p, $p>2$ – простое число. Кроме того, возможно построение кодов Гоппа в алфавите K_q, где K_q – конечное кольцо Галуа характеристики p^v.

Поскольку циклические коды достигают простую схемную реализацию кодирование и вылавливание ошибок (это было показано в моей бакалавровской работе) мы применили новый подход Мак Элайеса и Нидеррайтера к построению криптосистемы, основанной на свойствах кодов Гоппы и сложной процедурой определения перестановочных матриц (высокого порядка) , обеспечивающих криптостойкость криптосистемы.

Мы построили программный продукт, состоящий из 3-х частей: в первой части мы строим проверочную митрицу H кода Гоппы для заданного множества L (как множество элементов конечного поля F_{2^n} с исключенным корнем специального заданного неприводимого многочлена $G(z)$ над F_2). Здесь же дана процедура решения системы линейных однородных уравнений с матрицей H, что и определяет множество кодовых слов кода Гоппы; во

второй части программы дана реализация обнаружния и исправления ошибки в кодовых словах, после прохождения зашумленного канала связи; в третьей части задачи алгоритм определения информационного слова по исправленному кодовому слову.

СПИСОК ЛИТЕРАТУРЫ

[1] Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн Теория кодов, исправляющих ошибки.

[2] Э. Берлекэмп Алгебраическая теория кодирования

[3] Р. Блейхут Теория и практика кодов, контролирующих ошибки

[4] Key One Chung, *Goppa Codes*, December 2004, Department of Mathematics, Iowa State University

[5] Гоппа В. Д. Новый класс линейных корректирующих кодов / / Пробл. передачи информ.1970. Т. 6. № 3. С. 24-30

[6] Patterson N.J. The Algebra Decoding of Goppa Codes//IEEE Trans. Inform Theory. 1975. V.21. № 2. P. 203-207