НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ

Междисциплинарная курсовая работа

Обзор алгоритмов кодовой криптографии

Анджушева Манца
студентка гр. БИБ191

Национальный исследовательский университет
«Высшая школа экономики»

28 мая 2021

Цель работы

Обзор известных асимметричных криптосистем на алгебраических кодах, исследование современного состояния, существующих противоречий и перспектив практического применения на постквантовый период.

Постановка задачи

Криптосистема Мак-Элиса

- Пусть $G - k \times n$ порождающая матрица линейного q-ичного (n, k, d)-кода C, для которого известен эффективный алгоритм декодирования Dec_C t ошибок.
- S — случайная обратимая $k \times k$ матрица
- P – случайная $n \times n$ перестановочная матрица

Постановка задачи

Криптосистема Мак-Элиса

- Пусть $G - k \times n$ порождающая матрица линейного q-ичного (n, k, d)-кода C, для которого известен эффективный алгоритм декодирования Dec_C t ошибок.
- S — случайная обратимая $k \times k$ матрица
- P – случайная $n \times n$ перестановочная матрица
- Секретный ключ: (Dec_C, S, P)

Постановка задачи

Криптосистема Мак-Элиса

- Пусть $G - k \times n$ порождающая матрица линейного q-ичного (n, k, d)-кода C, для которого известен эффективный алгоритм декодирования Dec_C t ошибок.
- S — случайная обратимая $k \times k$ матрица
- P – случайная $n \times n$ перестановочная матрица
- Секретный ключ: (Dec_C, S, P)
- Открытый ключ: $G' = S \times G \times P$, t

Постановка задачи

Плюсы и минусы кодовой криптографии

Преимущество

Масштабируемость и стойкость (на сегодняшний день) к квантовым вычислениям

Проблема

Очень длинные ключи, необходимость которых обуславливается требованиями криптографической стойкости

Задачи

3. искать коды, которые можно описать компактно

Задачи

3. искать коды, которые можно описать компактно

5. изучить алгоритмы декодирования рассмотренных кодов

Задачи

1. углубить знания о криптосистемах с открытым ключом
2. изучить криптосистему Мак-Элиса – первую кодовую криптосистему
3. искать коды, которые можно описать компактно
4. исследовать линейные коды, имеющие полиномиальную сложность декодирования, на возможность построить на их основе асимметричные криптосистемы
5. изучить алгоритмы декодирования рассмотренных кодов
6. описать те алгоритмы кодовой криптографии, которые остаются стойкими на сегодняшний день

Результаты

- **структурирование и подробный анализ ключевых аспектов кодовой криптографии**
- рассмотрены следующие кодовые конструкции:
  1. коды Гоппы
  2. QC LDPC-коды
  3. QC MDPC-коды
- изучены алгоритмы декодирования:
  - для кодов Гоппы — алгоритм Паттерсона, алгоритм Гао
  - для QC LDPC и QC MDPC-кодов — BF, LLR-SPA декодеры
- изучен вопрос практической стойкости рассмотренных криптосистем к атакам

Итоги

	Mc-Eliece (2048, 1696)	QC-LDPC	QC-MDPC
Размер ключей	424 КБайт	6144 байт	9237 бит
Инф. бит	1696	12288	3079
Уровень защиты	80	80	80

- QC-LDPC и QC-MDPC уменьшают размер ключей
- Структурность кода позволяет записать ключ компактно, однако это влечёт за собой неустойчивость криптосистем к структурным атакам
- Криптосистемы QC-LDPC, QC-MDPC и оригинальная система Мак-Элиса пока остаются нераскрытыми
- Выбор параметров этих кодов остаётся проблемой

Спасибо за внимание!