МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М. В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Хабибулин Марат Ильдарович

Ресурс параллелизма в реконструкции поверхности мтодом движущихся наименьших квадратов

КУРСОВАЯ РАБОТА

Научный руководитель:
доцент, к.ф.-м.н.
Никольский Илья Михайлович

Москва, 2022

Оглавление

Введение

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 Р. Дж. Мак-Элисом [**MCEliece**]. Данная криптосистема основывается на $\mathbb{NP}$-трудной проблеме в теории кодирования. Основная идея её построения состоит в маскировке некоторого кода, имеющего эффективные алгоритмы декодирования, под код, не обладающий видимой алгебраической и комбинаторной структурой, такие коды принято называть кодами общего положения. Эта криптосистема обладает одним важным преимуществом — высокой скоростью зашифрования и расшифрования. Однако, у неё имеется серьёзный недостаток — относительно низкая скорость передачи (R). Обычно у кодовых криптосистем $R < 1$, тогда как у криптосистемы RSA скорость в точности равна 1.

В этой работе рассматривается обобщение криптосистемы Мак-Элиса, предложенное в 1994 коду В.М. Сидельниковым [**Sidelnikov1**]. В этой работе модификация, предложенная В. М. Сидельниковым, называется криптосистемой

Мак-Элиса–Сидельникова. Криптосистема Мак-Элиса–Сидельникова строится на основе u-кратного использования кодов Рида–Маллера $RM(r, m)$. Она имеет высокую криптографическую стойкость, скорость передачи близкую к 1 и сравнительно невысокую сложность шифрования секретных сообщений и расшифрования криптограмм этих сообщений.

В работе исследуются вопросы, связанные с пространством эквивалентных секретных ключей, то есть секретных ключей, порождающих одинаковые открытые ключи, новой криптосистемы. Опишем краткое содержание разделов работы.

В § 1 даётся определение криптосистемы Мак-Элиса, описываются её секретный и открытый ключи. Приводятся алгоритмы зашифрования и расшифрования.

В § 2 изучается ключевое пространство криптосистемы Мак-Элиса. Устанавливается связь классов эквивалентностей секретных ключей с группой автоморфизмов линейного кода, лежащего в основе этой криптосистемы.

В § 3 описывается криптосистема Мак-Элиса–Сидельникова: секретный и открытый ключи, алгоритмы зашифрования и расшифрования.

§ 4 посвящён ключевому пространству новой криптосистемы. В нём

вводятся множества, необходимые для описания классов эквивалентности секретных ключей. Получаются нижние и верхние оценки на мощности введённых множеств и на число открытых ключей криптосистемы Мак-Элиса–Сидельникова.

В § 5 изучается криптосистема Мак-Элиса–Сидельникова в случае двух блоков ($u = 2$).

В настоящей работе получаются нижние оценки на мощность множества открытых ключей криптосистемы Мак-Элиса–Сидельникова(теорема **??**) при использовании произвольного числа блоков u. Для кодов Рида–Маллера с u-кратным повторением строится множество, которое, в некотором смысле, является аналогом группы автоморфизмов обычного кода Рида–Маллера, и устанавливается связь этого множества с классами эквивалентности секретных ключей.

Для случая двух блоков ($u = 2$) полностью описывается указанное множество при использовании кодов Рида–Маллера $RM(r, m)$ $(r \leqslant 2, r < m)$ и матриц определённого вида (теоремы **??**, **??**). Тем самым при $u = 2, r \geqslant 2, r < m$ описываются все классы эквивалентности секретных ключей с представителями особого вида и вычисляются их мощности. Для некоторых классов эквивалентности секретных ключей приводятся нижние оценки на их мощность(теоремы **??** и **??**).