МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М.В. ЛОМОНОСОВА

На правах рукописи

Чижов Иван Владимирович

Пространство ключей криптосистемы Мак-Элиса–Сидельникова

05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2010

Работа выполнена на кафедре математической кибернетики факультета Вычислительной математики и кибернетики Московского государственного университета имени М.В. Ломоносова.

Научный руководитель:	кандидат физико-математических наук, доцент Карпунин Григорий Анатольевич.
Официальные оппоненты:	доктор физико-математических наук, доцент Куракин Владимир Леонидович; кандидат физико-математических наук, доцент Черепнёв Михаил Алексеевич.
Ведущая организация:	Томский государственный университет.

Защита диссертации состоится «16» июня 2010 года в 16 часов 45 минут на заседании диссертационного совета Д 501.002.16 при Московском государственном университете имени М.В. Ломоносова по адресу: 119991, Российская Федерация, Москва, ГСП-1, Ленинские горы, д.1, Московский государственный университет имени М.В. Ломоносова, механико-математический факультет, аудитория 14-08.

С диссертацией можно ознакомиться в библиотеке механико-математического факультета МГУ (Главное здание, 14 этаж).

Автореферат разослан 14 мая 2010 года.

Ученый секретарь
диссертационного совета,
доктор физико-математических наук, доцент  Корнев А. А.

Общая характеристика работы

Актуальность работы определяется потребностью в исследовании альтернативных традиционным криптосистем с открытым ключом. Бурное развитие теории чисел за последние 5 лет позволило значительно снизить стойкость RSA — широко распространённой на практике криптосистемы с открытым ключом. Это диктует необходимость в исследовании других криптосистем с открытым ключом с целью поиска альтернатив криптосистеме RSA. Одной из таких альтернатив являются кодовые криптосистемы, то есть криптосистемы, основанные на задачах из теории кодов, исправляющих ошибки. В основе кодовых криптосистем лежит идея использования быстро декодируемых кодов, исправляющих ошибки, в качестве основного элемента шифрующего преобразования. В настоящее время широкую известность получили две кодовые криптосистемы — криптосистема Мак–Элиса и криптосистема Нидеррайтера, оригинальные версии которых используют коды Гоппы и расширенные коды Рида–Соломона, соответственно. В.М. Сидельников и С.О. Шестаков показали несостоятельность идеи использования для построения кодовых криптосистем расширенных кодов Рида–Соломона, так как в этом случае такие криптосистемы не будут стойкими.

Кодовые криптосистемы имеют особенность, которая отличает их от многих других криптосистем. В кодовых криптосистемах одному и тому же открытому ключу могут соответствовать несколько секретных ключей, и поэтому секретные ключи могут быть разбиты на классы эквивалентности. При этом вопрос строения этих классов эквивалентности для кодовых криптосистем оказывается важным. Так атака В.М. Сидельникова и С.О. Шестакова использует строение ключевого пространства кодовой криптосистемы для вскрытия криптосистемы Мак-Элиса на основе обобщённых кодов Рида–Соломона. Следовательно, в некоторых случаях структура пространства ключей кодовой криптосистемы может помочь в её криптоанализе.

Атака В.М. Сидельникова и С.О. Шестакова показала невозможность использовать расширенные коды Рида–Соломона для построения кодовых криптосистем, поэтому в 1994 году В.М. Сидельников предложил использовать для построения кодовых криптосистем коды Рида–Маллера, которые позволяют увеличить как скорость расшифрования криптограммы, так и скорость передачи криптосистемы. Кроме того, В.М. Сидельников предложил усиленный вариант криптосистем

Мак-Элиса, в конструкции которой используется не одна копия кода, а некоторое число u копий кода, число u становится параметром криптосистемы. Такая криптосистема в диссертации получила название криптосистемы Мак-Элиса–Сидельникова. До недавнего времени ключевое пространство усиленного варианта кодовых криптосистем на основе кодов Рида–Маллера оставалось полностью не изученным. Диссертация посвящена исследованию структуры множества ключей криптосистемы Мак-Элиса–Сидельникова и разработке методов использования структуры этого множества в криптоанализе криптосистемы Мак-Элиса–Сидельникова, что, с учётом представленных выше соображений, свидетельствует об её актуальности и практической значимости.

Цель диссертационной работы заключается:

- в получении оценок на число открытых ключей криптосистемы Мак-Элиса–Сидельникова;
- в исследовании структуры множества отрытых ключей криптосистемы Мак-Элиса–Сидельникова;
- в разработке методов, позволяющих использовать сведения о структуре открытых ключей криптосистемы Мак-Элиса–Сидельникова для криптоанализа такого вида криптосистем.

Научная новизна.

- Получена нижняя оценка на мощность множества открытых ключей криптосистемы Мак-Элиса–Сидельникова, которая позволила заключить, что число ключей криптосистемы достаточно велико, чтобы противостоять атаке на криптосистему полным перебором по всему множеству открытых ключей.
- Установлена связь классов эквивалентности секретных ключей со специально введенным множеством перестановок. Это множество перестановок является в некотором смысле обобщением группы автоморфизмов кодов.
- В случае использования произвольного числа копий кода Рида-Маллера описывается ряд классов эквивалентности секретных ключей.

- Задача изучения некоторых классов эквивалентности секретных ключей сведена к изучению перестановочной эквивалентности особого вида подпространств кода Рида-Маллера и описаны все перестановки, которые переводят подпространство особого вида в некоторое другое подпространство кода Рида–Маллера. С использованием описания перестановок были получены описания ряда классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова.

- Доказана полиномиальная эквивалентность некоторых задач, связанных со стойкостью криптосистемы Мак-Элиса—Сидельникова, и задачи взлома оригинальной криптосистемы Мак-Элиса на основе подкодов кода Рида-Маллера, размерность которых на единицу меньше размерности кода, а также была доказана возможность восстановления части секретного ключа криптосистемы Мак-Элиса–Сидельникова, используя знание структуры класса эквивалентности, в который попадает секретный ключ.

Практическая значимость. Работа носит теоретический характер. Вместе с тем, полученные при её выполнении результаты могут найти применение: в синтезе и криптоанализе кодовых криптосистем; при изучении перестановочной эквивалентности подпространств кодов; при изучении свойств кодов, исправляющих ошибки, полученных из других кодов операцией комбинирования; в учебном процессе.

На защиту выносятся следующие основные результаты и положения:

- нижняя оценка мощности множества открытых ключей криптосистемы Мак-Элиса–Сидельникова;

- описание ряда классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова для произвольного числа блоков кода Рида–Маллера;

- описание классов эквивалентности с представителями особого вида в случае криптосистемы с двумя блоками;

- метод восстановления части секретного ключа криптосистемы Мак-Элиса–Сидельникова, использующий знание структуры класса эквивалентности, в который попадает секретный ключ;

- доказательство полиномиальной эквивалентности задачи взлома оригинальной криптосистемы Мак-Элиса, построенной на основе подкодов кода Рида–Маллера, размерность которых на единицу меньше размерности кода, и задачи взлома криптосистемы Мак-Элиса–Сидельникова с ограничениями на ключевое пространство.

Апробация работы
Результаты работы докладывались:

- на семинаре «Дискретная математика и математическая кибернетика» кафедры математической кибернетики факультета Вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова;

- на VII общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009), 2009 год

- на VI общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008), 2008 года;

- на V общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2007), 2007 год;

- на VII международной конференции «Дискретные модели в теории управляющих систем», 2006 год;

- на VIII Сибирской научной школе-семинаре с международным участием «Компьютерная безопасность и криптография — SIBECRYPT'09», 2009 год.

Публикации. Основное содержание диссертации опубликовано в 7 работах, список которых приведён в конце автореферата [1]—[7]. Работ, написанных в соавторстве, нет.

Личный вклад автора заключается в проведённом им исследовании пространства ключей криптосистемы Мак-Элиса–Сидельникова, в получении описаний структуры классов эквивалентности секретных ключей криптосистемы, а также в исследовании возможности применения знаний структуры этих классов в криптоанализе криптосистемы Мак-Элиса–Сидельникова.

Структура и объем диссертации Диссертационная работа, общим объёмом 170 страниц, состоит из введения, четырёх глав и заключения. Список литературы включает 34 наименования.

Содержание работы

Во Введении обоснована актуальность диссертационной работы, сформулирована цель и аргументирована научная новизна исследований, показана практическая значимость полученных результатов, представлены выносимые на защиту научные положения.

В первой главе приводятся основные сведения из теории кодов, исправляющих ошибки и вводятся необходимые в дальнейшем изложении термины и определения. Даётся краткое введение в криптографию и криптосистемы с открытым ключом. Приводится описание криптосистемы Мак-Элиса.

Криптосистема Мак-Элиса — одна из старейших криптосистем с открытым ключом. Она была предложена в 1978 Р. Дж. Мак-Элисом[1]. Стойкость рассматриваемой криптосистемы основывается на $\mathbb{NP}$-трудной задаче в теории кодирования. Основная идея её построения состоит в маскировке некоторого линейного кода, имеющего эффективные алгоритмы декодирования, под код, не обладающий видимой алгебраической и комбинаторной структурой. Такие коды принято называть кодами общего положения. Предполагается, что декодирование кода общего положения является трудной задачей[2]. Не зная структуры кода, невозможно построить эффективный алгоритм декодирования такого кода. Именно эта идея и заложена в конструкции криптосистемы, предложенной Р. Дж. Мак-Элисом.

Криптосистема Мак-Элиса, как и все другие известные кодовые криптосистемы обладают одним важным преимуществом — высокой скоростью зашифрования и расшифрования. Однако, в подобных криптосистемах имеется недостаток — относительно низкая скорость передачи (R). Обычно у кодовых криптосистем $R < 1$, тогда как почти у всех криптосистем, используемых на практике, скорость равна 1. С развитием вычислительной техники и с увеличением производительно-

[1] McEliece R. J. A public-key cryptosystem based on algebraic coding theory // DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol. 1978. Vol. January. Pp. 114–116.

[2] Barg A. Complexity Issues in Coding Theory // Handbook of Coding Theory Volume II / Ed. by V. S. Pless, W. C. Huffman. Amsterdam: Elsevier, 1998. Pp. 649–755.

сти вычислительных систем низкая скорость передачи кодовых систем может перестать быть существенным недостатком, сдерживающим использование этих криптосистем на практике.

В 1986 году Нидеррайтер [3] предложил модификацию криптосистемы Мак-Элиса, которая получила название криптосистемы Нидеррайтера. Криптосистема Мак-Элиса и криптосистема Нидеррайтера, построенные на основе одних и тех же кодов, например, кодов Гоппы, с точки зрения стойкости являются эквивалентными[4]. В той же работе [3] автор предлагает использовать для построения как новой криптосистемы, так и криптосистемы Мак-Элиса обобщённые коды Рида–Соломона. В 1992 году В.М. Сидельников и С.О. Шестаков показали, что использование обобщённых кодов Рида–Соломона для построения криптосистем Мак-Элиса и Нидеррайтера делает эти криптосистемы нестойкими[5]. При этом атака В.М. Сидельникова и С.О. Шестакова использует для взлома знание свойств структуры классов эквивалентности секретных ключей.

В.М. Сидельников [6] в 1994 году рассмотрел возможность использования кодов Рида–Маллера для построения криптосистемы Мак-Элиса. Он провёл криптографический анализ такой криптосистемы. Результаты показали, что криптосистема Мак-Элиса на основе кодов Рида–Маллера не обеспечивает достаточной стойкости. Кроме того в 2007 году Л. Миндер в работе[7] усилил атаку В.М. Сидельникова, однако она остаётся до сих пор неполиномиальной. В той же работе [6] рассматривается некоторое усиление криптосистемы Мак-Элиса на основе кодов Рида–Маллера — криптосистема Мак-Элиса–Сидельникова.

В диссертации исследуются вопросы, связанные со структурой классов эквивалентности секретных ключей, то есть секретных ключей, порождающих одинаковые открытые ключи, новой криптосистемы.

В первой главе описывается криптосистема Мак-Элиса–Сидельникова. Эта криптосистема строится на основе u-кратного использования кодов Рида–Маллера $RM(r, m)$. Всюду далее через $k = \sum_{i=0}^{r} \binom{m}{i}$ бу-

[3] Niederreiter H. Knapsack-type crytosystems and algebraic coding theory // Prob. Contr. Inform. Theory. 1986. Vol. 15(2). Pp. 157–166.

[4] Li Y. X., Deng R. H., Wang X. M. The equivalence of McEliece's and Niederreiter's public-key cryptosystems // IEEE Transactions on Information Theory. 1994. Vol. 40. Pp. 271–273.

[5] Сидельников В. М., Шестаков С. О. О безопасности системы шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискретная математика. 1992. Т. 4(3). С. 57-63.

[6] Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида-Маллера // Дискретная математика. 1994. Т. 6(2). С. 3-20.

[7] Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov cryptosystem // Advances in Cryptology- EUROCRYPT 2007, Lecture Notes in Computer Science. 2007. Vol. 4515. Pp. 347–360.

дет обозначаться размерность кода Рида–Маллера $RM(r,m)$, а через $n = 2^m$ — его длина.

Секретным ключом криптосистемы является кортеж

$$(\boldsymbol{H}_1, \boldsymbol{H}_2, \ldots, \boldsymbol{H}_u, \Gamma). \tag{1}$$

Здесь $\boldsymbol{H}_1, \boldsymbol{H}_2, \ldots, \boldsymbol{H}_u$ — невырожденные матрицы размера $k \times k$ над полем $GF(2)$, которые выбираются случайно и равновероятно из множества всех двоичных невырожденных матриц размера $k \times k$. Матрица Γ имеет размеры $u \cdot n \times u \cdot n$ и является перестановочной, то есть в каждой её строчке и в каждом столбце стоит ровно одна единица, поэтому можно считать, что Γ — это перестановка на множестве из un элементов.

Открытым ключом криптосистемы Мак-Элиса–Сидельникова является матрица

$$\boldsymbol{G}' = (\boldsymbol{H}_1\boldsymbol{R} \| \boldsymbol{H}_2\boldsymbol{R} \| \ldots \| \boldsymbol{H}_u\boldsymbol{R}) \cdot \Gamma, \tag{2}$$

где символом $\|$ обозначена конкатенация матриц по столбцам, а $\boldsymbol{R}$ — стандартная форма порождающей матрицы кода $RM(r,m)$. Под стандартной формой порождающей матрицы понимается $(k \times n)$-матрица вида

$$R = \begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ G_r \end{pmatrix},$$

где

$$G_0 = (1, 1 \ldots, 1),$$

$$G_1 = \begin{pmatrix} \Omega_{y_m} \\ \vdots \\ \Omega_{y_2} \\ \Omega_{y_1} \end{pmatrix}, G_2 = \begin{pmatrix} \Omega_{y_{m-1}y_m} \\ \vdots \\ \Omega_{y_1y_3} \\ \Omega_{y_1y_2} \end{pmatrix}, G_r = \begin{pmatrix} \Omega_{y_{m-r+1}y_{m-r+2}\ldots y_m} \\ \vdots \\ \Omega_{y_1y_2\ldots y_{r-1}y_{r+1}} \\ \Omega_{y_1y_2\ldots y_{r-1}y_r} \end{pmatrix},$$

здесь Ω_f — вектор значений булевой функции $f(y_1, \ldots, y_m)$. Отметим, что в дальнейшем мы не будем делать различий между булевыми функциями и их векторами значений.

Даётся следующее определение эквивалентности секретных ключей в криптосистеме Мак-Элиса–Сидельникова. Два секретных ключа

$$(\boldsymbol{H}_1, \boldsymbol{H}_2, \ldots, \boldsymbol{H}_u, \Gamma) \text{ и } (\boldsymbol{H}'_1, \boldsymbol{H}'_2, \ldots, \boldsymbol{H}'_u, \Gamma')$$

называются *эквивалентными*, если соответствующие им открытые ключи совпадают, то есть выполняется соотношение

$$(\boldsymbol{H}_1\boldsymbol{R}\|\boldsymbol{H}_2\boldsymbol{R}\|\ldots\|\boldsymbol{H}_u\boldsymbol{R})\cdot\Gamma=(\boldsymbol{H}'_1\boldsymbol{R}\|\boldsymbol{H}'_2\boldsymbol{R}\|\ldots\|\boldsymbol{H}'_u\boldsymbol{R})\cdot\Gamma'. \qquad (3)$$

Введённое отношение является отношением эквивалентности. Тем самым, всё множество секретных ключей разбивается на классы эквивалентности и число классов эквивалентности совпадает с числом открытых ключей. Класс эквивалентности с представителем $(\boldsymbol{H}_1,\ldots,\boldsymbol{H}_u,\Gamma)$ будем обозначать так: $[(\boldsymbol{H}_1,\ldots,\boldsymbol{H}_u,\Gamma)]$.

Во второй главе изучается ключевое пространство криптосистемы Мак-Элиса–Сидельникова. Устанавливается связь классов эквивалентности секретных ключей со специально введенным множеством перестановок $\mathcal{G}$.

Рассмотрим множество $\mathcal{G}(\boldsymbol{H}_1,\boldsymbol{H}_2,\ldots,\boldsymbol{H}_u)$, состоящее из перестановок $\Gamma\in S_{un}$, для которых существуют невырожденные двоичные матрицы $\boldsymbol{H}'_1,\boldsymbol{H}'_2,\ldots,\boldsymbol{H}'_u$ такие, что

$$(\boldsymbol{H}_1\boldsymbol{R}\|\boldsymbol{H}_2\boldsymbol{R}\|\ldots\|\boldsymbol{H}_u\boldsymbol{R})\Gamma=(\boldsymbol{H}'_1\boldsymbol{R}\|\boldsymbol{H}'_2\boldsymbol{R}\|\ldots\|\boldsymbol{H}'_u\boldsymbol{R}). \qquad (4)$$

Во второй главе доказано следующее утверждение.

Теорема. 2.1. *Существует взаимно однозначное соответствие между классом эквивалентности* $[(\boldsymbol{H}_1,\boldsymbol{H}_2,\ldots,\boldsymbol{H}_u,\Gamma)]$ *секретных ключей и множеством* $\mathcal{G}(\boldsymbol{H}_1,\boldsymbol{H}_2,\ldots,\boldsymbol{H}_u)$.

При этом класс эквивалентности $[(\boldsymbol{H}_1,\boldsymbol{H}_2,\ldots,\boldsymbol{H}_u,\Gamma)]$ *состоит из ключей вида*

$$(\boldsymbol{H}'_1,\boldsymbol{H}'_2,\ldots,\boldsymbol{H}'_u,\Gamma_g^{-1}\cdot\Gamma), \qquad (5)$$

где Γ_g *принадлежит множеству* $\mathcal{G}(\boldsymbol{H}_1,\boldsymbol{H}_2,\ldots,\boldsymbol{H}_u)$ *и*

$$(\boldsymbol{H}_1\boldsymbol{R}\|\boldsymbol{H}_2\boldsymbol{R}\|\ldots\|\boldsymbol{H}_u\boldsymbol{R})\Gamma_g=(\boldsymbol{H}'_1\boldsymbol{R}\|\boldsymbol{H}'_2\boldsymbol{R}\|\ldots\|\boldsymbol{H}'_u\boldsymbol{R}). \qquad (6)$$

Тем самым вопрос изучения структуры классов эквивалентности секретных ключей сводится к изучению структуры множества перестановок $\mathcal{G}$.

Далее во второй главе описывается ряд классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова в случае использования произвольного числа блоков кода Рида–Маллера.

Для этого с помощью автоморфизмов кода Рида–Маллера вводится понятие группы расширенных автоморфизмов. Напомним, что

автоморфизмом некоторого кода $\mathcal{C}$ называется множество перестановок координат кодовых слов, которые переводят код $\mathcal{C}$ в себя. Известно, что совокупность всех автоморфизмов кода относительно операции умножения перестановок является группой. Рассмотрим некоторую перестановку $\sigma \in S_n$. Построим, используя её, i «длинных» перестановок $\sigma[i] \in S_{un}$ следующим образом. Положим $\sigma[i](j) = j$ для любого $j \notin I = \{(i-1)\cdot n + 1, (i-1)\cdot n + 2, \ldots, i \cdot n\}$, а $\sigma[i](j) = (i-1)n + \sigma(j - (i-1)n)$, для всех $j \in I$. Другими словами, перестановка $\sigma[i]$ в i-том блоке действует как перестановка σ, а во всех остальных блоках — как единичная перестановка. Тогда *группой расширенных автоморфизмов* $\mathcal{A}_u(RM(r,m))$ кода Рида–Маллера $RM(r,m)$ назовём множество всех возможных произведений описанных перестановок $\sigma[i]$ для всех возможных $1 \leqslant i \leqslant u$ и всех возможных перестановок σ из группы автоморфизмов кода $RM(r,m)$.

В диссертации доказана следующая теорема.

Теорема. 2.2. *Пусть невырожденные матрицы $\boldsymbol{D}_1, \boldsymbol{D}_2, \ldots, \boldsymbol{D}_u$ задают автоморфизмы $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_u$ кода $RM(r,m)$ соответственно, то есть для $1 \leqslant i \leqslant u$ выполнены равенства $\boldsymbol{D}_i\boldsymbol{R} = \boldsymbol{R}\boldsymbol{\sigma}_i$. Обозначим через $\boldsymbol{\sigma}_1[1]$,$\boldsymbol{\sigma}_2[2]$,...,$\boldsymbol{\sigma}_u[u]$ перестановки из $\mathcal{A}_u(RM(r,m))$, соответствующие перестановкам $\boldsymbol{\sigma}_1, \ldots, \boldsymbol{\sigma}_u$. И пусть $\boldsymbol{H}$ — любая невырожденная матрица.*

Тогда

$$\mathcal{G}(\boldsymbol{H}\boldsymbol{D}_1, \ldots, \boldsymbol{H}\boldsymbol{D}_u) = \boldsymbol{\sigma}_1^{-1}[1] \cdot \boldsymbol{\sigma}_2^{-1}[2] \ldots \boldsymbol{\sigma}_u^{-1}[u] \cdot \mathcal{G}(\boldsymbol{E}, \ldots, \boldsymbol{E}). \quad (7)$$

Эта теорема дает описание множества $\mathcal{G}(\boldsymbol{H}\boldsymbol{D}_1, \ldots, \boldsymbol{H}\boldsymbol{D}_u)$. С помощью неё в диссертации доказана теорема, дающая описание ряда классов эквивалентности.

Теорема. 2.4. *Пусть невырожденные матрицы $\boldsymbol{D}_1, \boldsymbol{D}_2, \ldots, \boldsymbol{D}_u$ задают автоморфизмы $\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \ldots, \boldsymbol{\sigma}_u$ кода $RM(r,m)$ соответственно. Обозначим через $\boldsymbol{\sigma}_1[1]$,$\boldsymbol{\sigma}_2[2]$,...,$\boldsymbol{\sigma}_u[u]$ перестановки из $\mathcal{A}_u(RM(r,m))$, соответствующие перестановкам $\boldsymbol{\sigma}_1, \ldots, \boldsymbol{\sigma}_u$. И пусть $\boldsymbol{H}$ — любая невырожденная матрица.*

Тогда класс эквивалентности $[(\boldsymbol{H}\boldsymbol{D}_1, \boldsymbol{H}\boldsymbol{D}_2 \ldots, \boldsymbol{H}\boldsymbol{D}_u, \Gamma)]$ состоит из кортежей вида

$$(\boldsymbol{H}\boldsymbol{A}_1, \boldsymbol{H}\boldsymbol{A}_2, \ldots, \boldsymbol{H}\boldsymbol{A}_u, \boldsymbol{\gamma}_1^{-1}[1] \cdot \boldsymbol{\gamma}_2^{-1}[2] \ldots \boldsymbol{\gamma}_u^{-1}[u]\Gamma' \cdot \cdot\boldsymbol{\sigma}_1[1] \cdot \boldsymbol{\sigma}_2[2] \ldots \boldsymbol{\sigma}_u[u]\Gamma), \quad (8)$$

где $\boldsymbol{A}_1, \boldsymbol{A}_2, \ldots, \boldsymbol{A}_u$ *задают автоморфизмы* $\boldsymbol{\gamma}_1, \boldsymbol{\gamma}_2, \ldots, \gamma_u$ *кода Рида–Маллера* $RM(r,m)$, $\boldsymbol{\gamma}_1[1], \boldsymbol{\gamma}_2[2], \ldots, \boldsymbol{\gamma}_u[u]$ *— соответствующие этим автоморфизмам расширенные автоморфизмы, а перестановка* $\Gamma' \in S_{un}$ *сохраняет матрицу* $(\boldsymbol{R}\|\boldsymbol{R}\|\ldots\|\boldsymbol{R})$, *то есть*

$$(\boldsymbol{R}\|\boldsymbol{R}\|\ldots\|\boldsymbol{R})\Gamma' = (\boldsymbol{R}\|\boldsymbol{R}\|\ldots\|\boldsymbol{R}). \tag{9}$$

Следует отметить, что эта структурная теорема позволяет, в частности, вычислить мощность каждого класса эквивалентности.

Во второй главе также получена нижняя оценка на мощность множества $\mathcal{E}$ открытых ключей криптосистемы Мак-Элиса–Сидельникова (верхняя оценка получена Г.А. Карпуниным [8] .

Теорема. 2.6. *Справедливы неравенства для числа* $|\mathcal{E}|$ *открытых ключей криптосистемы Мак-Элиса–Сидельникова*

$$\frac{(u\cdot n)!h_k}{(u!)^n|Aut(RM(r,m))|} \leqslant |\mathcal{E}| < \frac{(u\cdot n)!(h_k)^u}{u!|Aut(RM(r,m))|^u}, \tag{10}$$

здесь n *— длина кода Рида–Маллера* $RM(r,m)$, *используемого для построения криптосистемы,* u *— число блоков криптосистемы,*

$$h_k = (2^k-1)(2^k-2)(2^k-2^2)\ldots(2^k-2^{k-1}) \ -$$

число обратимых $(k\times k)$*-матриц над полем* $GF(2)$, *и* $Aut(RM(r,m))$ *— группа автоморфизмов кода Рида–Маллера* $RM(r,m)$.

Оценка на число открытых ключей опубликована в работе [1].

Нижняя оценка позволяет определить насколько богато множество открытых ключей криптосистемы Мак-Элиса–Сидельникова при каждых конкретных значениях параметров u, r, m. Если обнаружится, что число открытых ключей невелико, то криптосистема заведомо окажется не стойкой. Так для предложенных В.М. Сидельниковым [6] значений $u = 4$, $r = 3$, $m = 10$ из нижней оценки (10) следует, что число открытых ключей будет не меньше, чем

$$10^{20897} < |\mathcal{E}|. \tag{11}$$

Тем самым число ключей в криптосистеме Мак-Элиса–Сидельникова достаточно велико, чтобы противостоять атаке полным перебором ключей.

[8] Карпунин Г. А. О ключевом пространстве криптосистемы Мак-Элиса на основе двоичных кодов Рида-Маллера // Дискретная математика. 2004. Т. 16(2). С. 79-84.

Результаты второй главы опубликованы в работах [1] и [2].

В третьей главе даётся описание классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова с представителем особого вида в случае использования только двух копий кода Рида–Маллера для построения криптосистемы.

Вначале вводится в рассмотрение следующий тип матриц. Пусть $I = \{i_1, i_2, \ldots, i_p\}$ — множество натуральных чисел таких, что выполнена цепочка неравенств $1 \leqslant i_1 \leqslant i_2 \leqslant \ldots \leqslant i_p \leqslant k$. Пусть также $\widetilde{A} = \{\widetilde{\alpha}^{i_1}, \widetilde{\alpha}^{i_2}, \ldots, \widetilde{\alpha}^{i_p}\}$ — множество двоичных наборов длины k. Рассмотрим матрицу $\boldsymbol{T}^I_{\widetilde{A}}$ вида

$$\boldsymbol{T}^I_{\widetilde{A}} = \begin{pmatrix} & & & & i_1 & & i_2 & & i_p & & \\ & & & & \downarrow & & \downarrow & & \downarrow & & \\ & 1 & 0 & \ldots & 0 & \ldots & 0 & \ldots & 0 & \ldots & 0 \\ & 0 & 1 & \ldots & 0 & \ldots & 0 & \ldots & 0 & \ldots & 0 \\ & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ i_1 \to & \alpha_1^{i_1} & \alpha_2^{i_1} & \ldots & \alpha_{i_1}^{i_1} & \ldots & \alpha_{i_2}^{i_1} & \ldots & \alpha_{i_p}^{i_1} & \ldots & \alpha_k^{i_1} \\ & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ i_2 \to & \alpha_1^{i_2} & \alpha_2^{i_2} & \ldots & \alpha_{i_1}^{i_2} & \ldots & \alpha_{i_2}^{i_2} & \ldots & \alpha_{i_p}^{i_2} & \ldots & \alpha_k^{i_2} \\ & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ i_p \to & \alpha_1^{i_p} & \alpha_2^{i_p} & \ldots & \alpha_{i_1}^{i_p} & \ldots & \alpha_{i_2}^{i_p} & \ldots & \alpha_{i_p}^{i_p} & \ldots & \alpha_k^{i_p} \\ & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots & \ldots & \vdots \\ & 0 & 0 & \ldots & 0 & \ldots & 0 & \ldots & 0 & \ldots & 1 \end{pmatrix}, \quad (12)$$

здесь $\widetilde{\alpha}^{i_j} = (\alpha_1^{i_j}, \alpha_2^{i_j}, \ldots, \alpha_k^{i_j})$ для $1 \leqslant j \leqslant p$. При этом для того, чтобы такая матрица была невырождена необходимо наложить на элементы множества $\widetilde{A}$ дополнительное условие, а именно нужно потребовать невырожденность матрицы

$$\begin{pmatrix} \alpha_{i_1}^{i_1} & \alpha_{i_2}^{i_1} & \ldots & \alpha_{i_p}^{i_1} \\ \alpha_{i_1}^{i_2} & \alpha_{i_2}^{i_2} & \ldots & \alpha_{i_p}^{i_2} \\ \alpha_{i_1}^{i_p} & \alpha_{i_2}^{i_p} & \ldots & \alpha_{i_p}^{i_p} \end{pmatrix}. \quad (13)$$

В случае когда $I = \{i\}$, $\widetilde{A} = \{\widetilde{\alpha}\}$ матрицу $\boldsymbol{T}^I_{\widetilde{A}}$ будем обозначать как $\boldsymbol{T}^i_{\widetilde{\alpha}}$.

Далее рассматривается два случая.

Первый случай — $u = 2$ и $I = \{i\}$.

Рассматривается код Рида–Маллера $RM(r, m)$ с $r > 1$, так как полное описание множества $\mathcal{G}(\boldsymbol{E}, \boldsymbol{H})$ для кода $RM(1, m)$ и всех матриц $\boldsymbol{H}$ было найдено Г.А. Карпуниным [8] .

Оказывается, что в этом случае задача описания классов эквивалентности сводится к задаче изучения перестановочной эквивалентности $(k-1)$-мерных подпространств кода $RM(r, m)$. Особый интерес представляют подпространства

$$\Pi_{\boldsymbol{w}} = \{\boldsymbol{v} \in RM(r, m) | (\boldsymbol{w}, \boldsymbol{v}) = 0\},$$

где $\boldsymbol{w}$ — моном вида $\overline{x}_1\overline{x}_2 \dots \overline{x}_{m-t}$ при $t > 0$.

Для таких подпространств в диссертации доказана теорема.

Теорема. 3.3. *Пусть* $2r \leqslant m$, $0 < t \leqslant r$, *и* $\boldsymbol{w} = \overline{x}_1\overline{x}_2 \dots \overline{x}_{m-t}$. *Тогда, если* $\Gamma(\Pi_{\boldsymbol{w}})$ — *множество перестановок, переводящих код* $\Pi_{\boldsymbol{w}}$ *в подкод кода* $RM(r, m)$, *то*

$$\Gamma(\Pi_{\boldsymbol{w}}) = I(\Pi_{\boldsymbol{w}}) \times \mathrm{Aut}(RM(r, m)). \tag{14}$$

Здесь $I(\Pi_{\boldsymbol{w}})$ — *множество перестановок* γ *таких, что* $\boldsymbol{x}^\gamma = \boldsymbol{x}$ *для любого* $\boldsymbol{x}$ *из подпространства* $\Pi_{\boldsymbol{w}}$.

Используя эту теорему, в диссертации получено описание множества классов эквивалентности в первом случае.

Теорема. 3.5. *Пусть* $RM(r, m)$ — *код Рида–Маллера такой, что* $2r \leqslant m$ *и* $r > 1$, i — *натуральное число, большее нуля;* $\boldsymbol{H}$ — *любая невырожденная двоичная матрица;* $\widetilde{\boldsymbol{\alpha}}$ — *произвольный двоичный вектор длины* k, *у которого в координате с номером* i *стоит единица. Тогда класс эквивалентности* $[(\boldsymbol{H}, \boldsymbol{H}\boldsymbol{T}^i_{\widetilde{\boldsymbol{\alpha}}}, \Gamma)]$ *состоит из кортежей вида*

$$(\boldsymbol{H}\boldsymbol{T}^i_{\widetilde{\boldsymbol{\beta}}}\boldsymbol{D}_1, \boldsymbol{H}\boldsymbol{T}^i_{\widetilde{\boldsymbol{\gamma}}}\boldsymbol{D}_2, {\boldsymbol{\sigma}_{\boldsymbol{L}}}^{-1}[1]\boldsymbol{\sigma}_R^{-1}[2]\Gamma'^{-1}\Gamma). \tag{15}$$

Здесь $\boldsymbol{\sigma}_L, \boldsymbol{\sigma}_R$ — *автоморфизмы кода Рида–Маллера* $RM(r, m)$, *соответствующие матрицам* $\boldsymbol{D_1}$ *и* $\boldsymbol{D_2}$, *а для перестановки* Γ' *выполняются два условия*

1) *Если* $\boldsymbol{R}'$ — $(k-1) \times n$-*матрица, получающаяся удалением строки с номером* i *из матрицы* $\boldsymbol{R}$, *то*

$$(\boldsymbol{R}'\|\boldsymbol{R}')\Gamma' = (\boldsymbol{R}'\|\boldsymbol{R}'); \tag{16}$$

2) Если $\overrightarrow{\boldsymbol{r_i}}$ *— строка матрицы* $\boldsymbol{R}$ *с номером* i*, то*

$$(\overrightarrow{\boldsymbol{r_i}}\|\widetilde{\boldsymbol{\alpha}}\boldsymbol{R})\Gamma' = (\widetilde{\boldsymbol{\beta}}\boldsymbol{R}\|\widetilde{\boldsymbol{\gamma}}\boldsymbol{R}) \in RM(r,m) \times RM(r,m). \qquad (17)$$

Приведённая структурная теорема 3.5 даёт не только описание классов, но с её помощью может быть вычислена мощность каждого класса эквивалентности.

Второй случай — $u = 2$, $|I| > 1$. В этом случае рассматривается матрица $\boldsymbol{T}^I_{\widetilde{A}}$, где $|I| = p > 1$. в другое подпространство того же кода. Описание классов эквивалентности теперь сводится к задаче описания перестановок, которые переводят подпространство Π_V размерности $k-p$ кода Рида–Маллера $RM(r,m)$ в другое подпространство того же кода. При этом, если V — множество из p линейно независимых векторов длины n, то подпространство Π_V определяется следующим образом

$$\Pi_V = \{\boldsymbol{w} \in RM(r,m) | (\boldsymbol{w},\boldsymbol{v}) = 0,\ \forall \boldsymbol{v} \in V\}. \qquad (18)$$

Для целей описания классов эквивалентности секретных ключей в диссертации рассматриваются только подпространства Π_V, которые задаются множеством $V = \check{V}$, где

$$\check{V} = \{x_{i_1^1}x_{i_2^1}\dots x_{i_{t_1}^2}, x_{i_1^2}x_{i_2^2}\dots x_{i_{t_2}^2}, \dots, x_{i_1^p}x_{i_2^p}\dots x_{i_{t_p}^p}\}. \qquad (19)$$

В диссертации доказано утверждение.

Утверждение. 3.11. *Пусть* $\Pi_{\check{V}}$ *— подкод кода* $RM(r,m)$*, задаваемый множеством* $\check{V}$*. Пусть также* $m-1 > 2r > \sharp$*, где* $\sharp$ *— общее число различных переменных, встречающихся в мономах из множества* $\check{V}$*. Рассмотрим перестановку* σ *такую, что* $(\Pi_{\check{V}})^\sigma$ *— подкод* $RM(r,m)$*. Тогда* σ *принадлежит группе автоморфизмов* $Aut(RM(r,m))$ *кода Рида–Маллера* $RM(r,m)$*.*

Используя это утверждение, в диссертации получено описание подмножеств классов эквивалентности $[\boldsymbol{H}, \boldsymbol{H}\boldsymbol{T}^I_{\widetilde{A}}, \Gamma]$.

Теорема. 3.6. *Пусть* $RM(r,m)$ *— код Рида–Маллера такой, что* $2r+1 < m$*. Пусть также* $\boldsymbol{H}$ *— любая невырожденная матрица размера* $k \times k$*. Далее, пусть существует перестановка* Γ_g^{-1} *— перестановка из* $\mathcal{G}(\boldsymbol{E}, \boldsymbol{T}^I_{\widetilde{A}})$*, представимая в виде* $\Gamma'\sigma_L[1]\sigma_R[2]$*, где* Γ' *такая перестановка, что*

$$(\boldsymbol{R}'\|\boldsymbol{R}')\Gamma' = (\boldsymbol{R}'\|\boldsymbol{R}'), \qquad (20)$$

здесь $\boldsymbol{R}'$ *—* $(k-p)\times n$*-матрица, получающаяся удалением* p *строк с номерами из множества* I *из матрицы* $\boldsymbol{R}$*. Тогда класс эквивалентности* $[\boldsymbol{H}, \boldsymbol{HT}^I_{\widetilde{A}}, \Gamma]$ *содержит кортежи вида*

$$(\boldsymbol{HT}^I_{\widetilde{B}}\boldsymbol{D}_1, \boldsymbol{HT}^I_{\widetilde{C}}\boldsymbol{D}_2, {\boldsymbol{\sigma_L}}^{-1}[1]\boldsymbol{\sigma}_R^{-1}[2]\Gamma'^{-1}\Gamma). \tag{21}$$

Здесь $\boldsymbol{\sigma}_L, \boldsymbol{\sigma}_R$ *— автоморфизмы кода Рида–Маллера* $RM(r,m)$*, соответствующие матрицам* $\boldsymbol{D_1}$ *и* $\boldsymbol{D_2}$*,* $\widetilde{B} = \{\widetilde{\beta}^{i_1}, \widetilde{\beta}^{i_2}, \ldots, \widetilde{\beta}^{i_p}\}$*,* $\widetilde{C} = \{\widetilde{\gamma}^{i_1}, \widetilde{\gamma}^{i_2}, \ldots, \widetilde{\gamma}^{i_p}\}$ *— множества двоичных наборов длины* k*, а для перестановки* Γ' *выполняется условие: если* $\overrightarrow{\boldsymbol{r_i}}$ *— строка матрицы* $\boldsymbol{R}$ *с номером* i*, то для любого* $i \in I$ *должно выполняться соотношение*

$$(\overrightarrow{\boldsymbol{r_i}} \| \widetilde{\boldsymbol{\alpha}}^i \boldsymbol{R})\Gamma' = (\widetilde{\boldsymbol{\beta}}^i \boldsymbol{R} \| \widetilde{\boldsymbol{\gamma}}^i \boldsymbol{R}) \in RM(r,m) \times RM(r,m). \tag{22}$$

Приведённая структурная теорема 3.6 даёт не только описание подмножества классов эквивалентности, но с её помощью может быть вычислена мощность этих подмножеств, то есть может быть получена оценка снизу на мощность каждого класса эквивалентности.

Результаты третьей главы опубликованы в работах [2]—[6].

В четвёртой главе рассматривается вопрос, связанный с полиномиальной эквивалентностью оригинальной криптосистемы Мак-Элиса, построенной на основе кодов Рида–Маллера и криптосистемы Мак-Элиса–Сидельникова с ограничениями на ключевое пространство.

Рассматриваются следующие задачи mcRMi и mcSRM.

Задача mcRMi

Вход: Число m большее $2r$ и $1 \leqslant i \leqslant k$, матрица $\boldsymbol{G} = \boldsymbol{H}' \cdot \boldsymbol{R}' \cdot \gamma'$, где $\boldsymbol{H}'$ — невырожденная двоичная $(k-1)\times(k-1)$-матрица, $\boldsymbol{R}'$ — $((k-1)\times n)$-матрица, получающаяся из порождающей матрицы $\boldsymbol{R}$ кода Рида–Маллера $RM(r,m)$ выкидыванием строки с номером i и γ' — перестановочная $(n\times n)$-матрица.

Найти: Невырожденную матрицу $\boldsymbol{M}'$ размера $(k-1)\times(k-1)$ и перестановочную $(n\times n)$-матрицу σ' такие, что $\boldsymbol{M}' \cdot \boldsymbol{G} \cdot \sigma'$ — порождающая матрица кода $\mathcal{R}'$, порождаемого матрицей $\boldsymbol{R}'$, то есть найдётся невырожденная $((k-1)\times(k-1))$-матрица $\boldsymbol{L}'$, что выполнено равенство $\boldsymbol{M}' \cdot \boldsymbol{G} \cdot \sigma' = \boldsymbol{L}' \cdot \boldsymbol{R}'$.

Отметим, что если mcRMi решается эффективно, то криптосистема Мак-Элиса на основе $(k-1)$-мерных подкодах кода Рида–Маллера $RM(r,m)$ эффективно взламывается.

Задача mcSRM

Вход: Число m большее $2r$, матрица $\boldsymbol{G} = (\boldsymbol{H}_1 \cdot \boldsymbol{R} \| \boldsymbol{H}_2 \cdot \boldsymbol{R}) \cdot \Delta$, где $\boldsymbol{H}_1$ и $\boldsymbol{H}_2$ — невырожденные двоичные $(k \times k)$-матрицы, принадлежащие классу эквивалентности $[(\boldsymbol{H}, \boldsymbol{H}\boldsymbol{T}^i_{\widetilde{\alpha}}, \Gamma)]$ для некоторой невырожденной $(k \times k)$-матрицы $\boldsymbol{H}$, некоторой перестановочной $(2n \times 2n)$-матрицы Γ, некоторого числа $1 \leqslant i \leqslant k$ и некоторого вектора $\widetilde{\alpha}$, $\boldsymbol{R}$ — порождающая $(k \times n)$-матрица кода Рида–Маллера $RM(r, m)$ и Δ — перестановочная $(2n \times 2n)$-матрица.
Найти: Невырожденные матрицы $\boldsymbol{H}'_1$ и $\boldsymbol{H}'_2$ размера $(k \times k)$ и перестановочную $(2n \times 2n)$-матрицу Δ' такие, что $\boldsymbol{G} \cdot \Delta' = (\boldsymbol{H}'_1\boldsymbol{R} \| \boldsymbol{H}'_2\boldsymbol{R})$.

Сложность задачи mcSRM определяет сложность восстановления по открытому ключу секретного ключа криптосистемы Мак-Элиса–Сидельникова, при условии, если он попадает в некоторый особый класс эквивалентности.

В диссертации доказана теорема.

Теорема. 4.1. *Пусть существует алгоритм $MTmcRMi$, который решает задачу $mcRMi$ за полиномиальное время. Тогда существует алгоритм $MTmcSRM$, который решает задачу $mcSRM$ за полиномиальное время.*

Теорема 4.1 позволяет заключить, что в криптосистеме Мак-Элиса–Сидельникова имеются классы секретных ключей, выбор которых не увеличивает стойкость новой криптосистемы по сравнению с оригинальной криптосистемой Мак-Элиса.

Этот результат опубликован в работе [7].

В заключении в диссертации рассматривается вопрос о возможности определить часть ключа криптосистемы Мак-Элиса–Сидельникова по перестановке из множества $\mathcal{G}$.

В четвёртой главе доказано следующее утверждение.

Утверждение. 2.11 *Пусть $\widehat{\mathcal{A}}_u(RM(r, m))$ — это множество перестановок вида $\nabla\boldsymbol{\gamma}$, где $\boldsymbol{\gamma}$ — это перестановка из $\mathcal{A}_u(RM(r, m))$, а ∇ — это произвольная перестановка блоков матрицы $(\boldsymbol{H}_1\boldsymbol{R} \| \ldots \| \boldsymbol{H}_u\boldsymbol{R})$. Справедливо равенство*

$$\bigcap_{\boldsymbol{H}_1, \ldots, \boldsymbol{H}_u \in GL(k,2)} \mathcal{G}(\boldsymbol{H}_1, \ldots, \boldsymbol{H}_u) = \widehat{\mathcal{A}}_u(RM(r, m)), \tag{23}$$

В случае $u = 2$ из утверждения 2.11 следует, что наличие во множестве $\mathcal{G}(\boldsymbol{E}, \boldsymbol{H})$ перестановки, не являющейся расширенным автомор-

физмом, особым образом характеризует матрицу $\boldsymbol{H}$, поэтому множество $\mathcal{G}(\boldsymbol{E}, \boldsymbol{H})$ в диссертации получило название G-структуры матрицы $\boldsymbol{H}$.

Для взлома криптосистемы Мак-Элиса–Сидельникова необходимо по матрице $(\boldsymbol{AR} \| \boldsymbol{BR})\Gamma$ восстановить матрицы $\boldsymbol{A}$ и $\boldsymbol{B}$ и перестановку Γ. Предположим, что злоумышленнику оказывается известной перестановка из множества $\mathcal{G}(\boldsymbol{A}, \boldsymbol{B})$. Как он может использовать это знание для восстановления ключа? Если обозначить через $\boldsymbol{H}$ произведение матриц $\boldsymbol{A}^{-1}\boldsymbol{B}$, то, как доказывается в разделе 2.1, $\mathcal{G}(\boldsymbol{A}, \boldsymbol{B}) = \mathcal{G}(\boldsymbol{E}, \boldsymbol{H})$, а значит знание перестановки из множества $\mathcal{G}(\boldsymbol{A}, \boldsymbol{B})$ эквивалентно знанию перестановки из G-структуры матрицы $\boldsymbol{H}$.

Итак, пусть перестановка $\Gamma = \Gamma_{I \leftrightarrow J}\gamma[1]\sigma[2]$ не является расширенным автоморфизмом и принадлежит G-структуре некоторой невырожденной матрицы $\boldsymbol{H}$, здесь $I = \{i_1, i_2, \ldots, i_d\} \subseteq \{1, 2, \ldots, n\} = \mathcal{N}$, $J = \{j_1, j_2, \ldots, j_d\} \subseteq \mathcal{N}$, а $\Gamma_{I \leftrightarrow J}(i_s) = n + j_s$, $\Gamma_{I \leftrightarrow J}(n + j_s) = i_s$ для всех $s = 1, 2, \ldots, d$, и $\Gamma_{I \leftrightarrow J}(i) = i$ для всех $i \neq i_1, \ldots, i_s, n + j_1, \ldots, n + j_s$. Обозначим через $\overline{I}$ дополнение к множеству I, то есть $\overline{I} = \mathcal{N} \setminus I$. Далее, если $\boldsymbol{R}$ — порождающая $(k \times n)$-матрица кода Рида–Маллера $RM(r, m)$, то через R_i будем обозначать столбец с номером i этой матрицы. Кроме того, через p_I обозначим ранг $((n - k) \times |I|)$-матрицы $\boldsymbol{R}_I^{\perp}$, которая является подматрицей матрицы $\boldsymbol{R}^{\perp}$, то есть проверочной матрицы кода $RM(r, m)$, и состоит из столбцов $\boldsymbol{R}^{\perp}$ с номерами из множества I.

В диссертации доказана следующая теорема.

Теорема. 4.1. *Используя перестановку* $\Gamma = \Gamma_{I \leftrightarrow J}\gamma[1]\sigma[2]$, *можно построить* $p_{\overline{I}} + p_{\overline{J}}$ *линейно независимых уравнений относительно* n *неизвестных* $\boldsymbol{H}R_1$, $\boldsymbol{H}R_2$, …, $\boldsymbol{H}R_n$.

Из этой теоремы следует, что знание перестановки из G-структуры, которая не является расширенным автоморфизмом, позволяет получить некоторое число линейных соотношений на матрицу $\boldsymbol{H}$, что позволяет восстановить часть ключа криптосистемы Мак-Элиса–Сидельникова. В силу этого понимание структуры классов эквивалентности секретных ключей криптосистемы Мак-Элиса–Сидельникова может оказаться важным для её взлома. Кроме того, прослеживается связь перестановок из G-структуры с перестановками из группы автоморфизмов кода. При переходе к рассмотрению криптосистемы Мак-Элиса–Сидельникова от криптосистемы Мак-Элиса перестановки из G-структуры являются обобщением понятия автоморфизмов. Такое обобщение оказывается даже более полезным для криптоанализа модифицированной криптосисте-

мы Мак-Элиса, нежели группа автоморфизмов для оригинальной. Причина в том, что перестановки из G-структуры дают систему линейных соотношений на элементы ключа криптосистемы Мак-Элиса–Сидельникова, в то время как автоморфизмы задают линейные соотношения, если они образуют группу со свойством транзитивности. Транзитивные группы автоморфизмов позволяют фиксировать ряд столбцов в матрице — элементе ключа криптосистемы.

Результаты третьей главы опубликованы в работе [7].

В Заключении приводятся основные результаты диссертационной работы.

Благодарности

Автор выражает искреннюю благодарность своему научному руководителю кандидату физико-математических наук, доценту Карпунину Григорию Анатольевичу за постановку задач, постоянное внимание, многочисленные плодотворные обсуждения, помощь в работе и терпение.

Автор выражает глубокую благодарность всей кафедре математической кибернетики факультета ВМК МГУ имени М.В. Ломоносова за содействие в подготовке диссертационной работы и создание творческой атмосферы.

Автор выражает искреннюю признательность Применко Эдуарду Андреевичу за неустанную поддержку и помощь в подготовке диссертации.

Публикации по теме диссертации

1. Чижов И. В. Число открытых ключей криптосистемы Мак-Элиса-Сидельникова // Вестник Московского университета. 2009. Т. 3. С. 40–45.

2. Чижов И. В. Ключевое пространство криптосистемы Мак-Элиса-Сидельникова // Дискретная математика. 2009. Т. 21(3). С. 132–158.

3. Чижов И. В. Об эквивалентных ключах криптосистемы Мак-Элиса-Сидельникова // Труды VII международной конференции «Дискретные модели в теории управляющих систем». 2006. С. 412–419.

4. Чижов И. В. Эквивалентные ключи криптосистемы Мак-Элиса–Сидельникова // Материалы Международного семинара «Дискретная математика и ее приложения», посвященного 75-летию со дня рождения академика О. Б. Лупанова. 2007. С. 461–464.

5. Чижов И. В. Эквивалентные подпространства кодов Рида–Маллера и множество открытых ключей криптосистемы Мак-Элиса–Сидельникова // Материалы VI общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2008). 2009. С. 28–32.

6. Чижов И. В. Эквивалентные подпространства кода Рида-Маллера и пространство ключей криптосистемы Мак-Элиса-Сидельникова // Тезисы докладов VIII Сибирской научной школы-семинара с международным участием «Компьютерная безопасность и криптография - SIBECRYPT'09». 2009. С. 36–38.

7. Чижов И. В. О сложности некоторых задач, связанных со стойкостью криптосистемы Мак-Элиса-Сидельникова // Материалы VII общероссийской научной конференции «Математика и безопасность информационных технологий» (МаБИТ-2009). 2010. С. 35–41.