Федеральное государственное автономное образовательное учреждение
высшего образования
«Южный Федеральный Университет»

На правах рукописи

Веденев Кирилл Владимирович

Исследование кодов в групповых алгебрах неабелевых групп и анализ стойкости некоторых кодовых криптосистем

РЕЗЮМЕ ДИССЕРТАЦИИ
на соискание учёной степени кандидата наук
по прикладной математике

Научные руководители:
кандидат технических наук
Косолапов Юрий Владимирович,
кандидат физико-математических наук
Деундяк Владимир Михайлович

Ростов-на-Дону – 2024

1 Актуальность темы диссертации и степень её разработанности

Диссертация посвящена исследованию ряда вопросов теории кодирования и её криптографических приложений. Теория кодирования – это междисциплинарная область, объединяющая в себе методы математики, информатики и инженерии для обеспечения надёжной и безошибочной передачи информации по зашумлённым каналам связи. По мере своего развития теория кодирования нашла многочисленные приложения, выходящие за рамки непосредственного исправления ошибок при передаче данных. Значительная часть этих приложений включает в себя, например, схемы шифрования с открытым ключом, алгоритмы цифровой подписи, схемы разделения секрета, протоколы защищённых многосторонних вычислений, методы сокрытия информации (стеганографии), методы защиты от несанкционированного копирования, а также методы обеспечения теоретико-информационной конфиденциальности с помощью кодового зашумления и т. д.

Каждое обозначенное приложение предъявляет свои специфические требования к используемым кодам. Так, при исправлении ошибок в каналах связи основное внимание сосредоточено на минимизации вносимой избыточности и разработке эффективных алгоритмов кодирования и декодирования. В свою очередь, при построении и анализе криптографических примитивов на основе кодов акцент делается на стойкости к известным атакам. Таким образом, конструирование помехоустойчивых кодов, удовлетворяющих разнообразным требованиям, и анализ их применимости в различных сценариях является одной из главных задач теории кодирования.

Теория кодирования тесно связана с линейной и общей алгеброй. Например, почти все коды, используемые на практике в настоящий момент, являются линейными кодами, то есть векторными подпространствами пространств $\mathbb{F}_q^n$, где $\mathbb{F}_q$ обозначает конечное поле мощности q. Переход от неструктурированных кодов к линейным существенно упрощает процесс кодирования, который в этом случае может быть выполнен путём умножения вектора сообщения на порождающую матрицу кода. Более того, данный переход также упрощает нахождение минимального расстояния, поскольку для линейных кодов оно совпадает с минимальным весом. В 1957 году Ю. Пранж ввёл подкласс линейных кодов, называемых *циклическими кодами* [117], которые характеризуются тем свойством, что для любого кодового слова $\mathbf{c} = (c_1, c_2, \dots, c_n)$ из кода C его циклический сдвиг $\mathbf{c}' = (c_n, c_1, \dots, c_{n-1})$ также является кодовым словом в C. Это дополнительное свойство позволяет осуществлять применение мощных алгебраических методов для исследования таких кодов. Как следствие, это позволяет получать оценки параметров, такие как границы Боуза-Чоудхури-Хоквингема (БЧХ) [32], и разрабатывать эффективные алгоритмы декодирования (см., например, [6; 11; 41; 64; 115]).

Естественным обобщением циклических кодов являются *групповые коды* (или же *G-коды*), представляющие собой идеалы конечных групповых алгебр $\mathbb{F}_q G$, где G – конечная группа. В частности, циклические коды длины n можно рассматривать как идеалы групповой алгебры $\mathbb{F}_q C_n$, где C_n – циклическая группа порядка n. Понятие групповых кодов было независимо предложено С. Д. Берманом в работах [17; 18] и Ф. Дж. Мак-Вильямс в работах [95; 96]. Так, С. Д. Берман обнаружил, что двоичные коды Рида-Маллера, ещё один эффективный класс линейных кодов, могут рассматриваться как идеалы элементарных абелевых 2-групп [17], также он проанализировал алгебраическую структуру кодов в полупростых абелевых групповых алгебрах [18]. В свою очередь, в работах [95; 96] Ф. Дж. Мак-Вильямс распространила некоторые теоремы о циклических кодах на коды над абелевыми группами.

Групповые коды являются ярким примером того, как богатая внутренняя алгебраическая структура позволяет применять алгебраические методы для изучения свойств кодов, а также

строить коды, обладающие многими положительными свойствами циклических кодов. В настоящее время установлено, что многие хорошо известные эффективные коды являются групповыми, в том числе обобщённые коды Рида-Маллера и расширенные коды Рида-Соломона [79; 88]. Кроме того, групповая структура оказывается полезной при декодировании, о чём, например, свидетельствуют комбинаторные методы декодирования для групповых кодов, предложенные в работе [44], декодеры для двоичных кодов Рида-Маллера, использующие групповую структуру [88], перестановочные декодеры для кодов над полупростыми абелевыми групповыми алгебрами [40], а также алгоритмы декодирования на основе ансамблей автоморфизмов, предложенные для кодов Рида-Маллера и для кодов с низкой плотностью проверок на чётность (LDPC-кодов) с групповой структурой [12; 13; 69].

В своей основополагающей работе [95] Ф. Дж. Мак-Вильямс в качестве перспективного направления исследований обозначила «поиск класса групп, не являющихся циклическими, которые порождали бы коды с желаемыми характеристиками». В связи с этим и потенциальными приложениями групповых кодов (в том числе в криптографии), одной из проблем, рассматриваемых в диссертации, является **проблема построения и изучения кодов в неабелевых групповых алгебрах**, в частности, в групповых алгебрах диэдральных и метациклических групп.

Ниже приведён краткий обзор известных результатов, в котором работы сгруппированы по различным аспектам исследования групповых кодов.

- *Структура абелевых кодов.* Алгебраическая структура кодов над абелевыми группами активно изучалась в работах [5; 17; 18; 89; 95; 96; 119; 121]. В работе [82] Й. Йенсен обнаружил, что коды над абелевыми группами могут рассматриваться как обобщённые каскадные коды (см. [27; 152]), что позволяет получать нижние оценки минимального расстояния таких кодов, используя их каскадную структуру. Другая нижняя оценка минимального расстояния, полученная П. Камионом в работе [36] (см. также [20; 122]), основана на обобщённом дискретного преобразования Фурье и обобщает границу БЧХ для циклических кодов. В работе [19] Бернал и др. обобщили границу Камиона и предложили метод, позволяющий распространить любую оценку минимального расстояния на основе определяющих множеств для циклических кодов на случай абелевых кодов. Отметим также, что для некоторых классов абелевых кодов в работах [23; 125] была показана применимость локаторного декодирования с использованием алгоритма Берлекампа-Месси-Сакаты.

- *Примеры кодов над абелевыми группами.* К известным примерам хороших кодов над абелевыми группами относятся циклические коды, обобщённые квадратично-вычетные коды [94], обобщённые коды Рида-Маллера [88], коды Коши [21; 67], гиперболические коды [84], произведения циклических кодов [22] и коды Бермана [18]. Отметим, что недавно было доказано, что коды Рида-Маллера и коды Бермана достигают шенноновской ёмкости для двоичного канала связи со стираниями (binary erasure channel – BEC) [106; 120]. В 2022 и 2023 году было также показано, что шенноновской ёмкости для BEC [105] достигает более широкий класс абелевых кодов, а коды Рида-Маллера, в свою очередь, достигают шенноновской ёмкости не только для BEC, но и для любого двоичного канала связи без памяти [4].

- *Мажоритарное декодирование групповых кодов.* В работе [151] К.-Х. Циммерман показал, что, используя методы теории модулярных представлений, можно строить групповые коды, допускающие L-шаговое мажоритарное декодирование (см. [99]). Исследования

по мажоритарному декодированию групповых кодов были продолжены В. Деундяком и др. в статьях [56; 58]. В работах [53; 91] К. Тжай и др. предложили подход к построению одношаговых мажоритарно декодируемых циклических кодов с использованием идемпотентов групповой алгебры $\mathbb{F}_q C$. Важно отметить, что предложенные циклические коды демонстрируют отличные характеристики в качестве LDPC-кодов.

- *Связь между абелевыми и неабелевыми кодами.* В работе [124] Р. Сабин и С. Ломонако обнаружили, что все центральные коды (т.е. двусторонние идеалы) в групповых алгебрах полупрямых произведений циклических групп комбинаторно эквивалентны абелевым кодам (т.е. идеалам в абелевых групповых алгебрах), причём минимальные расстояния этих кодов оказываются довольно небольшими. В [124] было также показано существование односторонних идеалов в тех же групповых алгебрах, образующих коды с лучшими параметрами, чем у известных абелевых кодов, причём некоторые из полученных кодов не уступали по своим параметрам наилучшим из известных линейных кодов.

  В работе [21] Бернал и др. получили критерий, позволяющий определить, является ли заданный линейный код групповым, исходя из свойств подгрупп группы перестановочных автоморфизмов кода. В той же работе ими также был получен следующий результат, обобщающий результат Сабин и Ломонако: если группа G содержит две абелевы подгруппы A и B такие, что $G = \{ab \mid a \in A, b \in B\}$, то все центральные коды в $\mathbb{F}_q G$ комбинаторно эквивалентны абелевым кодам. Кроме того, в [21] было неконструктивно доказано существование односторонних групповых кодов, не эквивалентных никаким абелевым кодам. В 2013 году, в работе [73] Пильядо и др. доказали, что все центральные групповые коды длины меньше 24 являются комбинаторно эквивалентными абелевым кодам, и что существуют центральные неабелевы коды длины 24. Дальнейшие уточняющие результаты, касающиеся существования центральных неабелевых кодов, были получены в работах [72; 107; 110; 149].

- *Коды в неабелевых групповых алгебрах.* В работе [123] Р. Сабин предложила использовать представления полупростых групповых алгебр для изучения минимальных групповых кодов. В частности, полупростота групповой алгебры означает, что она может быть разложена в прямую сумму минимальных двусторонних идеалов (центральных кодов), каждое слагаемое которой изоморфно некоторому неприводимому представлению группы G над полем $\mathbb{F}_q$ (в свою очередь, каждое такое представление изоморфно некоторой полной матричной алгебре). В работе [124] Р. Сабин и С. Ломонако, используя неприводимые представления, построили примеры кодов в полупростых групповых алгебрах некоторых расщепимых метациклических групп $G_{n,m,r} = \langle x, y \mid x^n = y^m = e, xy = y^r x \rangle$, где $r^m \equiv 1 \pmod{n}$. Для этого, в частности, ими был описан алгоритм нахождения неприводимых представлений таких групп в случае, когда поле $\mathbb{F}_q$ содержит все корни n-й степени из единицы.

  В работе [68] Дутра и др. рассмотрели центральные коды в полупростых групповых алгебрах диэдральных групп $\mathbb{F}_q D_{2n}$, где $D_{2n} = G_{n,2,-1} = \langle x, y \mid x^n = y^2 = e, xy = y^{-1}x \rangle$, задаваемые идемпотентами, построенными по подгруппам, и вычислили их размерность и минимальные кодовые расстояния. Однако стоит отметить, что в силу упомянутого выше результата Бернала и др. [21] все эти коды комбинаторно эквивалентны абелевым кодам. В работе [10] С. Ассуэна и С. Майлс рассмотрели и описали все примитивные центральные идемпотенты в полупростых групповых алгебрах $\mathbb{F}_q G$ неабелевых расще-

пимых метациклических групп над конечным полем в случае, когда порядок группы G равен $p^m l^n$, где p и l — различные простые числа. Затем в своих недавних работах [8; 9] С. Ассуэна и С. Майлс предложили конструкцию нецентральных кодов для тех же классов групп на основе идемпотентов, и получили ряд примеров кодов, параметры которых совпадают с параметрами наилучших известных линейных кодов. Отметим, что конструкции групповых кодов, основанные на идемпотентах, также исследовались в работах [70; 76—78; 116; 128].

В работе [34] О. Броше и А. дель-Рио предложили вычислительный метод, основанный на рассмотрении некоторых пар подгрупп, для построения разложения Веддербёрна и нахождения примитивных центральных идемпотентов полупростых групповых алгебр конечных групп G, у которых существует нормальная абелева группа, факторгруппа по которой является сверхразрешимой. Основываясь на этой работе, в [111] Г. Олтеану и В. Гельдер предложили алгоритмы построения минимальных левых групповых кодов над метациклическими группами вида $C_{q^m} \leftthreetimes C_{p^n}$, где C_{p^n} действует точно на C_{q^m}, p и q — различные простые числа, а характеристика поля $\mathbb{F}_s$ не делит pq. Кроме того, в [111] были представлены конструкции некоторых наилучших известных линейных кодов в виде групповых кодов. В работе [14] Бакши и др. предложили алгоритм вычисления набора примитивных центральных идемпотентов, группы автоморфизмов и вида разложения Веддербёрна для полупростых групповых алгебр конечных метаабелевых групп с помощью пар Шоды. Стоит отметить, что в [14] для разложения Веддербёрна получено только описание вида, а не явный изоморфизм.

В 2015 году, Ф.Мартинес [35] получил явное разложение Веддербёрна с соответствующим изоморфизмом для полупростых групповых алгебр диэдральных групп $\mathbb{F}_q D_{2n}$. В 2020 году Гао и др. [71] обобщили этот результат, получив явное разложение Веддербёрна для групповых алгебр $\mathbb{F}_q G_{n,2,r}$, $r^m \equiv 1 \pmod{n}$, где группа $G_{n,m,r}$ определена выше. Кроме того, в [71] в этих групповых алгебрах были описаны некоторые коды, обладающие комплементарными двойственными кодами, (linear complimentary dual – LCD), а также центральные самодвойственные коды.

В 2016 году Као и др. [37] исследовали каскадную структуру диэдральных кодов, используя исключительно теорию конечных полей и теорию циклических и косоциклических кодов. С помощью аналогичных методов, Као и др. [112] доказали существование каскадной структуры у кодов над классом метациклических групп вида $G_{n,3,r}$. В 2022 году Као и др. [38] уточнили результаты работы [37] и получили описание диэдральных LCD-кодов и самодвойственных кодов в терминах их каскадной структуры.

В 2021 году М. Борелло и А. Джеймос [28] получили нижнюю оценку минимального расстояния диэдральных кодов, похожую на границу БЧХ, рассматривая диэдральные коды как подкоды подподполевых образов некоторых циклических кодов, заданных над расширением поля. Стоит отметить, что похожая техника была использована К. Лэлли в работе [87] для получения оценки минимального расстояния квазициклических кодов.

- *Асимптотические характеристики.* В 2006 году Баззи и Миттер [15] доказали, что двоичные диэдральные коды являются асимптотически хорошими. А именно, было показано, что для бесконечного набора длин случайный идеал в двоичной диэдральной групповой алгебре с высокой вероятностью является асимптотически хорошим кодом. В 2007 году Мартинес-Перес и Виллемс [98] улучшили этот результат. В 2020 году Борелло и др. [29] доказали, в предположении справедливости обобщённой гипотезы

Римана, что метациклические коды являются асимптотически хорошими. Также в 2020 году Борелло и Виллемс [30] рассмотрели метациклические групповые алгебры вида $\mathbb{F}_p\langle\alpha,\beta \mid \alpha^p = \beta^q = e, \alpha\beta = \beta^m\alpha\rangle$, где p – фиксированное простое число, q – простое число такое, что $p \mid (q-1)$, $m \not\equiv 1 \pmod{q}$, $m^p \equiv 1 \pmod{q}$, и доказали, что коды в этих алгебрах также являются асимптотически хорошими, причём этот результат не зависит от какие-либо дополнительных предположений.

- *Приложения.* Многие хорошо известные коды, включая циклические коды, коды Рида-Соломона и коды Рида-Маллера, являются групповыми и, следовательно, имеют множество практических применений для защиты информации от ошибок и стираний. В работах [56; 57] В. М. Деундяк и Ю. В. Косолапов исследовали возможность применения некоторых мажоритарно декодируемых групповых кодов в криптографии и высказали предположение, что *использование неабелевых групповых кодов в кодовых криптосистемах может повысить их стойкость к атакам, направленным на восстановление секретного ключа*. В 2023 году Борелло и др. [63] исследовали диэдральные квантовые коды и построили пример коротких диэдральных квантовых кодов, обладающих лучшими параметрами по сравнению с другими известных квантовыми кодами.

Таким образом, представленный обзор работ свидетельствует об актуальности и активном научном интересе к исследованию групповых кодов, а также подчёркивает их теоретическую и практическую значимость.

В последние годы применение теории кодирования в криптографии для создания асимметричных схем шифрования и цифровых подписей привлекает всё больше внимания исследователей и приобретает всё большую практическую значимость. Это обусловлено, главным образом, тем, что задачи факторизации целых чисел и дискретного логарифмирования, лежащие в основе традиционных криптосистем, таких как RSA и криптосистемы на эллиптических кривых, могут быть решены за полиномиальное время на квантовых компьютерах с помощью алгоритма Шора [131]. Это ставит под угрозу их безопасность в условиях появления больших квантовых компьютеров. В отличие от них, криптография на основе кодов опирается на сложность декодирования случайных линейных кодов, которая считается трудноразрешимой даже для квантовых компьютеров [24]. Появившись в 1978 году, кодовая криптография является старейшей и наиболее изученной альтернативой традиционным криптосистемам, основанным на теории чисел и эллиптических кривых.

В 1978 году, практически одновременно с публикацией криптосистемы RSA, Роберт Мак-Элис в своей основополагающей работе [101] предложил первую схему шифрования с открытым ключом, основанную на помехоустойчивых кодах. В качестве открытого ключа эта криптосистема предполагает использование матриц вида $\tilde{G} = SGP$, где G - порождающая матрица двоичного кода Гоппы, исправляющего t ошибок, S – случайная обратимая $(k \times k)$-матрица, а P – случайная $(n \times n)$-матрица перестановки. Шифрование сообщения $m \in \mathbb{F}_2^k$ выполняется по формуле $y = m\tilde{G} + \varepsilon$, где ε - случайная ошибка с весом Хэмминга t. При наличии матриц S и P восстановление исходного сообщения m у легального пользователя не вызывает затруднений, так как он может воспользоваться эффективным декодером кода Гоппы. В свою очередь, атакующая сторона вынуждена решать задачу декодирования случайного линейного кода или же задачу восстановления секретного ключа. Примечательно, что оптимизированная современная версия криптосистемы Мак-Элиса на основе кодов Гоппы [45] по-прежнему считается надежной и была выбрана в качестве финалиста 3-го раунда конкурса NIST по стандартизации постквантовых криптосистем [135]. Несмотря на множество достоинств, криптосистема Мак-Элиса обладает существенным недостатком – большим размером

открытых ключей, что во многих случаях ограничивает её практическую применимость.

Для устранения этого недостатка было предпринято множество попыток заменить коды Гоппы в протоколе Мак-Элиса более эффективными кодами, такими как обобщённые коды Рида-Соломона, коды Рида-Маллера, алгебро-геометрические коды, LDPC-коды, каскадные коды и некоторые групповые коды [26; 57; 59; 81; 83; 103; 108; 132]. Кроме того, для повышения криптостойкости предлагалиль различные улучшения самого механизма сокрытия секретного кода (см., например, [2; 3; 16; 55; 85; 97; 127; 137; 148]). Однако многие из этих модификаций и предложений оказались уязвимы к струкрутным атакам на ключ (см., например, [31; 43; 46; 47; 49; 50; 60—62; 65; 102; 113; 114; 133; 150]).

Вышесказанное, в сочетании с тем, что криптография на основе кодов является одним из ведущих кандидатов на роль квантово-стойких криптографических примитивов, подчеркивают важность и актуальность **проблемы анализа стойкости кодовых криптосистем**, рассматриваемой в данной диссертационной работе. При этом представляется, что для оценки стойкости кодовых криптосистем, должны последовательно выполняться следующие шаги:

1. *Оценка применимости известных атак к рассматриваемой криптосистеме*. Любая новая криптосистема должна быть устойчива к уже известным атакам.

2. *Оценка возможности сведения стойкости новых криптосистем к стойкости известных криптосистем*.

3. *Анализ применимости и разработка новых методов криптоанализа*.

Приведём далее обзор работ, затрагивающие различные аспекты анализа стойкости кодовых криптосистем.

При атаке на кодовые криптосистемы можно действовать двумя способами: осуществлять *атаки на сообщения* или же *структурные атаки на ключ*. Атаки на сообщения предполагают, что криптоаналитику известны открытый ключ и зашифрованное сообщение, при этом цель таких атак – восстановить открытый текст, не используя никаких специальных свойств или структурных особенностей применяемых кодов. Применительно к кодовым криптосистемам это означает, что криптоаналитик, как правило, должен выполнить декодирование случайно выглядещего линейного кода от t ошибок. Наиболее эффективными алгоритмами решения этой задачи в настоящее время являются алгоритмы декодирования по информационным совокупностям (information set decoding – ISD) [25; 33; 54; 66; 92; 93; 100; 136], представляющие собой усовершенствования алгоритма Пранжа [118], а также алгоритмы статистического декодирования [134]. Несмотря на продвинутость этих методов, их сложность остаётся экспоненциальной. Таким образом, возможность практически реализуемых атак на сообщения можно предотвратить, выбрав параметры криптосистемы таким образом, чтобы сложность наилучшей из известных атак на сообщения соответствовала требуемому уровню стойкости.

Наиболее опасными атаками являются структурные атаки на ключ, которые, если они существуют, невозможно предотвратить выбором параметров криптосистемы. Цель атак на ключ – восстановить секретный ключ (полностью или частично) по открытому ключу, используя специальные свойства применяемых кодов и уязвимости в механизмах их сокрытия. Действительно, многие используемые на практике коды обладают ярко выраженной алгебраической структурой (так, например, коды Рида-Соломона (RS) и коды Рида-Маллера (RM) являются кодами на основе вычисления значений многочленов) или же комбинаторной структурой (такой как, например, каскадное строение или мажоритарная декодируемость). Если механизм сокрытия недостаточно надёжен, эти структуры могут быть использованы для атаки на секретный ключ. В результате структурные атаки на ключ обычно используют:

- *Алгебраические свойства кодов* (например, свойства произведений Шура-Адамара [31; 43; 47; 50; 61; 62; 65; 113; 150] и группы автоморфизмов [114; 129; 133]).
- *Комбинаторные свойства кодов* (например, каскадную структуру [46; 130] или распределение слов малого веса [51]).
- *Линейно-алгебраические свойства механизмов сокрытия кодов* (см., например, [39; 52; 90]).

Основное внимание в криптографической части диссертации уделяется структурным атакам на ключ, поскольку в них можно эффективно использовать алгебраические и комбинаторные свойства кодов. Следует отметить, что известные структурные атаки на ключ по степени восстановления секретного ключа (в порядке убывания) можно классифицировать следующим образом:

- *Атаки с полным восстановлением ключа*. В результате таких атак криптоаналитик полностью раскрывает секретный ключ и получает возможность эффективно дешифровывать любые сообщения (см., например, [31; 43; 46; 47; 49; 50; 60—62; 65; 102; 113; 114; 133; 150]).
- *Атаки с частичным востановлением ключа.* Такие атаки позволяют криптоаналитик восстановить секретный ключ лишь частично, что, тем не менее, потенциально может быть использовано для снижения сложности атак на сообщения (см., например, [46; 86]).
- *Атаки-различители.* В этом случае криптоаналитик способен отличить открытый код от случайного кода с теми же параметрами (см., например, [1; 65; 104; 148]). Существование различителей не означает автоматически существования атак с частичным или полным восстановлением ключа; тем не менее, многие криптосистемы были взломаны путём усиления атак-различителей. Таким образом, даже такая минимальная степень восстановления секретного ключа является крайне нежелательной.

Обычно структурные атаки на ключ проводятся только по открытому ключю. Тем не менее, для построения структурных атак возможно также использование дополнительной информации, такой как утечки по сторонним каналам (side-channel attacks) и накопленые ошибки расшифрования. Следовательно, структурные атаки на ключ можно классифицировать на: 1) *атаки без подсказок* и 2) *атаки с подсказками*. Важным подклассом атак с подсказками являются *реакционные атаки*, которые используют ошибки расшифрования (см., например, атаки на криптосистему HQC и криптосистемы на основе QC-MDPC кодов [74; 75; 109; 147]).

Подводя итог, следует отметить, что кодовая криптография является чрезвычайно динамичной областью исследований, в которой активно разрабатываются новые криптографические примитивы и атаки. Принимая во внимание теоретическую и практическую значимость кодовой криптографии, существующие и перспективные кодовые криптосистемы должны тщательно анализироваться на предмет возможных уязвимостей.

2 Цели и задачи

В связи с обозначенными проблемами в диссертации поставлены следующие **цели**:

1) исследование диэдральных и метациклических групповых кодов, в том числе их криптографических свойств;

2) анализ стойкости недавно предложенных асимметричных схем шифрования на основе кодов.

Для достижения обозначенных целей были поставлены следующие **задачи**:

1) для диэдральных кодов исследовать их алгебраическую структуру и свойства, включая оценки параметров и алгоритмы декодирования;

2) исследовать алгебраическую структуру метациклических групповых алгебр и метациклических кодов, а также получить оценки параметров для метациклических кодов;

3) исследовать применимость диэдральных и метациклических кодов в кодовых криптосистемах;

4) исследовать стойкость асимметричных криптосистем на основе квази-групповых и квази-воспроизводимых кодов с умеренной плотностью проверок на четность (MDPC-кодов) к реакционным атакам;

5) теоретически оценить вероятность ошибочного декодирования регулярных небинарных MDPC кодов для последующего выбора параметров семантически стойких QC-MDPC криптосистем;

6) проанализировать стойкость недавно предложенных кодовых криптосистем, основанных на подполевых образах кодов.

3 Основные результаты, выносимые на защиту

На защиту выносятся следующие результаты, полученные в диссертации:

1. Алгебраическое описание диэдральных кодов (в том числе, двойственных кодов и кодов, индуцированных циклическими кодами); верхние и нижние границы минимального расстояния диэдральных кодов; алгоритм декодирования диэдральных кодов; алгебраическое описание строения квадратов Шура-Адамара диэдральных кодов.

2. Разложение типа Веддербёрна групповых алгебр расщепимых метациклических групп, алгебраическое описание метациклических кодов с использованием этого разложения; представление метациклических кодов в виде обобщенных каскадных кодов; оценки минимального кодового расстояния для метациклических кодов; возможность использования каскадной структуры для построения структурных атак с частичным восстановлением ключа на криптосистемы типа Мак-Элиса, основанные на метациклических кодах.

3. Теорема об эквивалентности квази-воспроизводимых кодов на основе перестановок и квази-групповых кодов; реакционная атака на криптосистемы, основанные на квази-групповых MDPC кодах.

4. Теоретические оценки вероятности ошибочного декодирования для регулярных небинарных MDPC кодов; параметры семантически стойких криптосистем на основе этих кодов.

5. Две структурные атаки с полным восстановлением ключа на криптосистему Иванова-Крука-Зяблова [80], оценка сложности атак на сообщения для криптосистемы Иванова-Крука-Зяблова.

4 Научная новизна и личный вклад автора.

Все результаты, выносимые на защиту, являются новыми и получены автором самостоятельно. Вклад научных руководителей состоит в постановке задач и обсуждении полученных результатов.

5 Методы исследования

Исследование групповых кодов и их свойств в диссертации проводится с использованием методов линейной алгебры и классической теории кодирования, а также теории колец и теории представлений групп (в частности, используется теория разложений Веддербёрна групповых алгебр и алгебр скрещенных произведений). При анализе стойкости кодовых криптосистем применяются алгебраические методы (такие как произведения Шура-Адамара и алгебраическое описание кодов), комбинаторика, теория вероятностей и компьютерные эксперименты.

6 Практическая значимость

Практическая значимость полученных в диссертации результатов о диэдральных и метациклических кодах в части оценки их параметров и разработки алгоритмов декодирования заключается в возможности внедрения этих кодов в схемы связи для борьбы с помехами. В свою очередь, результаты диссертации в части строения квадратов Шура-Адамара диэдральных кодов могут найти применение при построении линейных схем разделения секрета и протоколов защищенных многосторонних вычислений на их основе. Результаты построения атак на криптосистему Иванова-Крука-Зяблова и криптосистему на основе квази-групповых MDPC кодов расширяют спектр известных криптоаналитических подходов и могут быть полезны при разработке стандартов постквантовых криптографических примитивов. Теоретические оценки вероятности ошибочного декодирования для регулярных небинарных MDPC кодов непосредственно позволяют строить семантически стойкие постквантовые криптосистемы на основе этих кодов, а также могут использоваться при выборе кодов для высоконадёжных систем связи.

7 Степень достоверности

Достоверность результатов диссертации обоснована строгими математическими доказательствами, а в ряде случаев подтверждена компьютерными экспериментами. Кроме того, основные результаты опубликованы в рецензируемых журналах и представлены на известных конференциях в области алгебры, теории кодирования и кодовой криптографии.

8 Публикации

Результаты диссертации опубликованы в следующих работах: [138; 140—146]. Работы [138; 139; 141—144; 146] опубликованы в изданиях, индексируемых в Scopus и WoS, работы [139; 145] опубликованы в изданиях, рекомендованных ВАК для публикации результатов диссертационных исследований.

9 Апробация результатов

Основные результаты диссертации докладывались на следующих российских и международных конференциях:

- XVII Международная конференция «Алгебра, теория чисел, дискретная геометрия» *(г. Тула, Россия, 2019)*;
- XVIII Международная конференция «Алгебра, теория чисел, дискретная геометрия» *(г. Тула, Россия, 2020)*;
- XVII International Symposium Problems of Redundancy in Information and Control Systems REDUNDANCY 2021
  (г. Москва, Россия, 2021);
- International Workshop on Code-Based Cryptography CBCrypto 2022
  (г. Тронхейм, Норвегия, 2022);
- 8th Huawei Optical Workshop *(г. Казань, Россия, 2022)*;
- International Workshop on Code-Based Cryptography CBCrypto 2023
  (г. Лион, Франция, 2023);
- 9th Huawei Optical Workshop *(г. Санкт-Петербург, Россия, 2023)*;
- XVIII International Symposium Problems of Redundancy in Information and Control Systems REDUNDANCY 2023
  (г. Москва, Россия, 2023).

10 Содержание работы и общие выводы исследования

Введение содержит постановку проблем, рассматриваемых в диссертации, обоснование их актуальности, обзор работ по теме исследования, формулировку целей и основных задач диссертационного исследования. Также во введении сформулированы основные положения и результаты, выносимые на защиту, и представлена структура работы.

Глава 1 посвящена построению систематической теории диэдральных кодов. В частности, с использованием разложения Веддербёрна алгебры $\mathbb{F}_q D_{2n}$, описанного Ф. Мартинесом в работе [35], в главе получено полное алгебраическое описание D_{2n}-кодов, включая описание их порождающих идемпотентов и базисов. Кроме того, получено явное описание двойственных кодов и критерий самодвойственности для диэдральных кодов. В главе также изучены диэдральные коды, индуцированные циклическими кодами, и установлена связь между теориями диэдральных и циклических кодов. В частности, получены верхняя и нижняя оценки на минимальное расстояние D_{2n}-кодов и разработан алгоритм декодирования на основе теории индуцированных кодов. В главе также приводятся некоторые иллюстративные примеры диэдральных кодов. В связи с криптографическими приложениями произведений и квадратов Шура-Адамара линейных кодов (см. [42]), в главе 1 исследованы произведения и квадраты Шура-Адамара для диэдральных кодов. В частности, показано, что квадраты Шура-Адамара диэдральных кодов обладают сильной алгебраической структурой. Эти результаты указывают на то, что диэдральные коды нежелательно использовать в кодовых криптосистемах типа

Мак-Элиса ввиду потенциальных уязвимостей. Тем не менее, диэдральные коды могут найти применение в других областях, что было показано, например, в работе М. Борелло и др. [29], где на основе некоторых результатов этой главы были построены эффективные квантовые коды малой длины.

Результаты первой главы, касающиеся строения и свойств диэдральных кодов (в том числе, двойственных и индуцированных кодов) были опубликованы в серии работ [138; 139; 145; 146] в 2018–2020 гг. Результаты, касающиеся произведений и квадратов Шура-Адамара диэдральных кодов, опубликованы в работе [143] в 2021 г.

Глава 2 продолжает исследование кодов в неабелевых групповых алгебрах. Расщепимые метациклические группы $G_{n,m,r}$, задаваемые следующими копредставлениями

$$G_{n,m,r} = \langle a, b \mid a^n = b^m = e, ba = a^r b \rangle,$$

где $r^m \equiv 1 \pmod{n}$, являются естественным обобщением диэдральных групп. В этой связи естественным образом возникает задача обобщения результатов предыдущей главы на этот более широкий класс групп. Как было продемонстрировано в первой главе, разложение Веддербёрна групповых алгебр в прямую сумму матричных алгебр является очень мощным и удобным инструментом для исследования групповых кодов. Однако задача явного построения такого разложения является нетривиальной. В частности, для рассматриваемого класса групп явное разложение было найдено лишь при серьёзных ограничениях на параметры n, m, r, q.

Основные результаты этой главы заключаются в следующем. Во-первых, получено явное разложение типа Веддербёрна для групповых алгебр расщепимых метациклических групп $\mathbb{F}_q G_{n,m,r}$ с единственным ограничением $\gcd(q, n) = 1$. Во-вторых, на основе этого разложения построена систематическая теория метациклических кодов. В частности, описана алгебраическая структура метациклических кодов. На основе полученной структуры показана возможность представления метациклических кодов в виде обобщенных каскадных кодов, внутренними кодами которых являются циклические коды, а внешними – косые квазициклические коды. С использованием этой обобщенной каскадной структуры показана возможность построения структурных атак с частичным восстановлением ключа на криптосистемы, основанные на *некоторых* метациклических кодах. Кроме того, исследован класс индуцированных кодов и получены оценки основных параметров метациклических кодов. Часть результатов этой главы опубликована в работе [140], полная версия главы принята к представлению на CBCrypto 2024.

Глава 3. Криптосистемы на основе квазициклических кодов с умеренной плотностью проверок на четность (QC–MDPC-кодов) считаются одними из самых перспективных постквантовых криптосистем благодаря малому размеру открытого ключа и отличному сочетанию характеристик. Однако из-за вероятностного декодирования MDPC-кодов существует ненулевая вероятность ошибочного декодирования. В 2016 году К. Гуо, Т. Йоханссон и П. Станковский [75] показали, что ошибки декодирования могут быть использованы для построения эффективных атак на ключ. В 2021 году, для предостращения таких атаки П. Сантини, Э. Персичетти и М. Балди [126] предложили обобщение квази-циклических кодов, названное квази-воспроизводимыми (quasi-reproducible – QR) кодами, а также предложили основанные на таких кодах QR–MDPC-криптосистемы. В данной главе доказано, что предложенные QR-MDPC-криптосистемы, допускающие короткие ключи и в силу этого использующие квази-воспроизводимые коды на основе перестановок с однострочным символом, на самом деле

эквивалентны криптосистемам на основе квази-групповых MDPC кодоы. В свою очередь, для таких криптосистем в главе продемонстрирована возможность построения реакционной атаки на ключ, обобщающей атаку Гуо-Йоханссона-Станковского, предложенную ранее для квази-циклических кодов. Следует также отметить, что другие классы криптосистем на основе двоичных квази-воспроизводимых MDPC-кодов, вероятно, имеют большие размеры открытых ключей по сравнению с QC-MDPC-криптосистемами, для которых вероятность ошибочного декодирования оценена теоретически (см., например, [7]). Результаты главы 3 опубликованы в работе [141].

Глава 4 посвящена построению теоретических оценок вероятности ошибочного декодирования (decoding failure rate – DFR) небинарных MDPC-кодов, расширяя результаты предыдущих исследований для бинарных случая. Теоретические оценки DFR особенно важны для криптографических приложений MDPC-кодов. В частности, как упоминалось выше, использование ошибок декодирования позволяет восстановить секретный ключ MDPC-криптосистемы. Это означает, что для достижения желаемого уровня стойкости в модели защищённости от адаптивных атак по подобранным шифртекстам (IND-CCA2), вероятность ошибочного декодирования должна быть строго ограничена сверху пренебрежимо малыми величинами (порядка 2^{-128}).

В этой главе для небинарных MDPC кодов исследуется их гарантированная корректирующая способность при декодировании одношаговым мажоритарным декодером (OSML), а также проводится вероятностный анализ одноитерационного параллельного symbol-flipping (SF) декодера. Кроме того оценивается вероятность ошибочного декодирования в следующем сценарии совместного использования этих декодеров: SF декодер применяется для снижения веса ошибки до уровня, при котором OSML декодер может успешно исправить все оставшиеся ошибки. В результате с использованием некоторых минималистычных предположений, получена верхняя оценка на DFR. Точность и обоснованность результирующей теоретической модели проверяется с помощью численного моделирования. В качестве приложения полученных результатов, в главе предлагаются возможные параметры семантически стойких небинарных QC-MDPC криптосистем для различных уровней стойкости по классификации NIST, наряду с их теоретически оцененной DFR.

Следует отметить, что результирующие размеры ключей в небинарном случае оказываются несколько больше по сравнению с бинарным. Однако вычислительные преимущества современных алгоритмов ISD обычно плохо масштабируются с увеличением размера поля, поэтому остается возможным, что небинарные коды в конечном итоге могут сравняться или превзойти бинарные MDPC-коды для криптографических приложений. Результаты этой главы опубликованы в работе [144].

Глава 5. В 2021 году Ф. Иванов, Е. Крук и В. Зяблов [80] предложили новую криптосистему, основанную на подполевых образах обобщенных кодов Рида-Соломона (Generalized Reed-Solomon codes– GRS codes) над расширениями полей. В предложенном ими подходе подполевые образы GRS-кодов маскируются специальным преобразованием таким образом, что полученные публичные коды оказываются не эквивалентными подполевым образам GRS-кодов, но при этом сохраняется возможность исправлять пакетные ошибки. В этой главе показано, что криптосистема Иванова-Крука-Зяблова не является стойкой, так как её секретный ключ может быть восстановлен за полиномиальное время. Так, в данной главе предложены две атаки с полным восстановлением ключа: первая атака основана на модифицированных квадратах Шура-Адамара, предложенных в работе [48], а вторая использует

только линейную алгебру и возможность отличать матрицы некоторого специального вида от случайных матриц.

Следует отметить, что вторая атака, основанная на методах линейной алгебры, может быть обобщена для восстановления секретной матрицы Q протокола Иванова-Крука-Зяблова и для других классов кодов, отличных от GRS кодов. Таким образом, используемое в этой криптосистеме маскирующее преобразование является нестойким. Кроме того, в главе уточнена оценка сложности атак на сообщения для криптосистем с пакетными ошибками, в силу чего представляется, что использование маскирующих преобразований, допускающих декодирование пакетных ошибок, не позволяет уменьшить размер ключей по сравнению с классическими подходами. Результаты данной главы опубликованы в работе [142].

Заключение диссертации содержит краткое изложение основных результатов диссертации и некоторые заключительные замечания. В частности полученные результаты позволяют следать следующие выводы.

В диссертации впервые проведено исследование применимости неабелевых групповых кодов в кодовых криптосистемах. Результаты диссертации показывают, что неабелева структура (по крайней мере, для рассмотренных классов групп) не приводит к существенному повышению стойкости кодовых криптосистем к структурным атакам. Также в диссертации выявлены уязвимости некоторых продвинутых механизмов маскировки в протоколах шифрования типа Мак-Элиса.

В частности, для диэдральных кодов была выявлена *сильная алгебраическая* структура самих кодов и их квадратов, которая является потенциальной уязвимостью. Так, наличие этой структуры позволяет строить *атаки-различители* на основе размерности квадратов Шура-Адамара для диэдральных кодов с малой скоростью. Для метациклических кодов их алгебраическая структура влечёт существование *сильной комбинаторной* структуры (представление в виде обобщённых каскадных кодов), что позволяет применить известную *атаку с частичным восстановлением ключа* Пучингера и др. [46] к широкому классу метациклических кодов. Реакционная атака на квазивоспроизводимые MDPC-коды иллюстрирует идею *редуцируемости* стойкости к известным криптосистемам (на основе QG- и QC-MDPC-кодов). Атаки с полным восстановлением ключа на основе модифицированных квадратов на криптосистему Иванова-Крука-Зяблова также могут рассматриваться как пример редуцируемости стойкости к криптосистеме, рассмотренной в [48]. Наконец, вторая атака из Главы 5, основанная на методах линейной алгебры и различителях матриц, иллюстрирует построение *новых криптоаналитических методов*.

Дальнейшие исследования, связанные с обозначенными во введении проблемами, могут заключаться в изучении других классов неабелевых групповых алгебр и соответствующих кодов, а также в поиске эффективных подклассов кодов для различных приложений (в том числе для исправление ошибок в зашумленных каналах связи, а также для криптографии). Также актуальным направлением является разработка новых кодовых криптосистем и алгоритмов цифровых подписей на основе кодов, наряду с совершенствованием криптоаналитических методов их анализа.

Список литературы

1. A Distinguisher for High-Rate McEliece Cryptosystems / J.-C. Faugere [и др.] // IEEE Transactions on Information Theory. — 2013. — Т. 59, № 10. — С. 6830—6844. — ISSN 1557-9654. — DOI: 10.1109/tit.2013.2272036.
2. A new code-based public-key cryptosystem resistant to quantum computer attacks / E. Egorova [и др.] // Journal of Physics: Conference Series. — 2019. — Т. 1163. — С. 012061. — ISSN 1742-6596. — DOI: 10.1088/1742-6596/1163/1/012061.
3. A variant of the McEliece cryptosystem with increased public key security / M. Baldi [и др.] // WCC 2011-Workshop on coding and cryptography. — 2011. — С. 173—182.
4. *Abbe E.*, *Sandon C.* A proof that Reed-Muller codes achieve Shannon capacity on symmetric channels // 2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS). — IEEE, 2023. — DOI: 10.1109/focs57990.2023.00020.
5. Abelian Codes in Principal Ideal Group Algebras / S. Jitman [и др.] // IEEE Transactions on Information Theory. — 2013. — Т. 59, № 5. — С. 3046—3058. — ISSN 1557-9654. — DOI: 10.1109/tit.2012.2236383.
6. Algebraic decoding of cyclic codes: a polynomial ideal point of view / X. Chen [и др.] // Contemporary Mathematics. — 1994. — Т. 168. — С. 15—15.
7. Analysis of the error correction capability of LDPC and MDPC codes under parallel bit-flipping decoding and application to cryptography / P. Santini [и др.] // IEEE Transactions on Communications. — 2020. — Т. 68, № 8. — С. 4648—4660.
8. *Assuena S.* Good codes from metacyclic groups II // Journal of Algebra and Its Applications. — 2020. — Т. 21, № 02. — ISSN 1793-6829. — DOI: 10.1142/s0219498822500402.
9. *Assuena S.*, *Milies C. P.* Good codes from metacyclic groups // Contemp. Math. — 2019. — Т. 727. — С. 39—49.
10. *Assuena S.*, *Milies C. P.* Group algebras of metacyclic groups over finite fields // São Paulo Journal of Mathematical Sciences. — 2016. — Т. 11, № 1. — С. 46—52. — ISSN 2316-9028. — DOI: 10.1007/s40863-016-0043-7.
11. *Augot D.*, *Betti E.*, *Orsini E.* An introduction to linear and cyclic codes // Gröbner Bases, Coding, and Cryptography. — 2009. — С. 47—68.
12. Automorphism ensemble decoding of quasi-cyclic LDPC codes by breaking graph symmetries / M. Geiselhart [и др.] // IEEE Communications Letters. — 2022. — Т. 26, № 8. — С. 1705—1709.
13. Automorphism ensemble decoding of Reed-Muller codes / M. Geiselhart [и др.] // IEEE Transactions on Communications. — 2021. — Т. 69, № 10. — С. 6424—6438.
14. *Bakshi G. K.*, *Gupta S.*, *Passi I. B. S.* The Algebraic Structure of Finite Metabelian Group Algebras // Communications in Algebra. — 2015. — Т. 43, № 6. — С. 2240—2257. — ISSN 1532-4125. — DOI: 10.1080/00927872.2014.888566.
15. *Bazzi L.*, *Mitter S.* Some randomized code constructions from group actions // IEEE Transactions on Information Theory. — 2006. — Т. 52, № 7. — С. 3210—3219. — ISSN 0018-9448. — DOI: 10.1109/tit.2006.876244.
16. *Berger T. P.*, *Loidreau P.* How to mask the structure of codes for a cryptographic use // Designs, Codes and Cryptography. — 2005. — Т. 35. — С. 63—79.

17. *Berman S. D.* On the theory of group codes // Cybernetics. — 1969. — Т. 3, № 1. — С. 25—31. — ISSN 1573-8337. — DOI: 10.1007/bf01072842.

18. *Berman S. D.* Semisimple cyclic and Abelian codes. II // Cybernetics. — 1970. — Т. 3, № 3. — С. 17—23. — ISSN 1573-8337. — DOI: 10.1007/bf01119999.

19. *Bernal J. J.*, *Guerreiro M.*, *Simon J. J.* From ds-Bounds for Cyclic Codes to True Minimum Distance for Abelian Codes // IEEE Transactions on Information Theory. — 2019. — Т. 65, № 3. — С. 1752—1763. — ISSN 1557-9654. — DOI: 10.1109/tit.2018.2868446.

20. *Bernal J. J.*, *Bueno-Carreno D. H.*, *Simon J. J.* Computing the Camion's multivariate BCH bound // 2013 IEEE Information Theory Workshop (ITW). — IEEE, 2013. — DOI: 10.1109/itw.2013.6691285.

21. *Bernal J. J.*, *Rio A. del*, *Simon J. J.* An intrinsical description of group codes // Designs, Codes and Cryptography. — 2009. — Т. 51, № 3. — С. 289—300. — ISSN 1573-7586. — DOI: 10.1007/s10623-008-9261-z.

22. *Bernal J. J.*, *Bueno-Carreño D. H.*, *Simón J. J.* Constructions of Abelian Codes Multiplying Dimension of Cyclic Codes // Mathematics in Computer Science. — 2019. — Т. 14, № 2. — С. 415—421. — ISSN 1661-8289. — DOI: 10.1007/s11786-019-00416-5.

23. *Bernal-Buitrago J. J.*, *Simon-Pinero J. J.* A New Approach to the Berlekamp-Massey-Sakata Algorithm: Improving Locator Decoding // IEEE Transactions on Information Theory. — 2021. — Т. 67, № 1. — С. 268—281. — ISSN 1557-9654. — DOI: 10.1109/tit.2020.3027751.

24. *Bernstein D. J.*, *Lange T.* Post-quantum cryptography // Nature. — 2017. — Т. 549, № 7671. — С. 188—194.

25. *Bernstein D. J.*, *Lange T.*, *Peters C.* Smaller Decoding Exponents: Ball-Collision Decoding // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 2011. — С. 743—760. — ISBN 9783642227929. — DOI: 10.1007/978-3-642-22792-9_42.

26. *Bernstein D. J.*, *Lange T.*, *Peters C.* Wild McEliece // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 2011. — С. 143—158. — ISBN 9783642195747. — DOI: 10.1007/978-3-642-19574-7_10.

27. *Blokh È. L.*, *Zyablov V. V.* Coding of generalized concatenated codes // Problemy Peredachi Informatsii. — 1974. — Т. 10, № 3. — С. 45—50.

28. *Borello M.*, *Jamous A.* Dihedral codes with prescribed minimum distance // Arithmetic of Finite Fields: 8th International Workshop, WAIFI 2020, Rennes, France, July 6–8, 2020, Revised Selected and Invited Papers 8. — Springer. 2021. — С. 147—159.

29. *Borello M.*, *Moree P.*, *Solé P.* Asymptotic performance of metacyclic codes // Discrete Mathematics. — 2020. — Т. 343, № 7. — С. 111885. — ISSN 0012-365X. — DOI: 10.1016/j.disc.2020.111885.

30. *Borello M.*, *Willems W.* Group codes over fields are asymptotically good // Finite Fields and Their Applications. — 2020. — Т. 68. — С. 101738. — ISSN 1071-5797. — DOI: 10.1016/j.ffa.2020.101738.

31. *Borodin M. A.*, *Chizhov I. V.* Effective attack on the McEliece cryptosystem based on Reed-Muller codes // Discrete Mathematics and Applications. — 2014. — Т. 24, № 5. — ISSN 0924-9265. — DOI: 10.1515/dma-2014-0024.

32. *Bose R. C.*, *Ray-Chaudhuri D. K.* On a class of error correcting binary group codes // Information and control. — 1960. — Т. 3, № 1. — С. 68—79.

33. *Both L.*, *May A.* Optimizing BJMM with nearest neighbors: full decoding in 22/21n and McEliece security // WCC workshop on coding and cryptography. T. 214. — 2017.

34. *Broche O.*, *Del Río Á.* Wedderburn decomposition of finite group algebras // Finite Fields and Their Applications. — 2007. — T. 13, № 1. — C. 71—79. — ISSN 1071-5797. — DOI: 10.1016/j.ffa.2005.08.002.

35. *Brochero Martinez F.* Structure of finite dihedral group algebra // Finite Fields and Their Applications. — 2015. — T. 35. — C. 204—214. — ISSN 1071-5797. — DOI: 10.1016/j.ffa.2015.05.002.

36. *Camion P.* Abelian Codes. — University of Wisconsin, Mathematics Research Center, 1971. — (Army. Mathematics Research Center, Madison, Wis. MRC technical summary report).

37. *Cao Y.*, *Cao Y.*, *Fu F.-W.* Concatenated structure of left dihedral codes // Finite Fields and Their Applications. — 2016. — T. 38. — C. 93—115. — ISSN 1071-5797. — DOI: 10.1016/j.ffa.2016.01.001.

38. *Cao Y.*, *Cao Y.*, *Ma F.* Construction and enumeration of left dihedral codes satisfying certain duality properties // Discrete Mathematics. — 2022. — T. 345, № 11. — C. 113059. — ISSN 0012-365X. — DOI: 10.1016/j.disc.2022.113059.

39. *Cayrel P.-L.*, *Otmani A.*, *Vergnaud D.* On Kabatianskii-Krouk-Smeets Signatures // Lecture Notes in Computer Science. — Springer Berlin Heidelberg. — C. 237—251. — ISBN 9783540730743. — DOI: 10.1007/978-3-540-73074-3_18.

40. *Chabanne H.* Permutation decoding of abelian codes // IEEE Transactions on Information Theory. — 1992. — T. 38, № 6. — C. 1826—1829. — ISSN 0018-9448. — DOI: 10.1109/18.165460.

41. *Charpin P.*, *Pless V.*, *Huffman W.* Open problems on cyclic codes // Handbook of coding theory. — 1998. — T. 1, № 11. — C. 965.

42. *Chizhov I. V.* A Hadamard Product of Linear Codes: Algebraic Properties and Algorithms for Calculating It // Moscow University Computational Mathematics and Cybernetics. — 2023. — Дек. — T. 47, № 4. — C. 239—250. — ISSN 1934-8428. — DOI: 10.3103/s0278641923040179.

43. *Chizhov I.*, *Borodin M.* Hadamard products classification of subcodes of Reed-Muller codes codimension 1 // Discrete Math. Appl. — 2020. — T. 32, № 1. — C. 115—134.

44. *Clark G. C.*, *Cain J. B.* Simple Nonalgebraic Decoding Techniques for Group Codes // Error-Correction Coding for Digital Communications. — Boston, MA : Springer US, 1981. — C. 97—140. — ISBN 978-1-4899-2174-1. — DOI: 10.1007/978-1-4899-2174-1_3.

45. Classic McEliece: conservative code-based cryptography / D. J. Bernstein [и др.] // NIST submissions. — 2017. — T. 1, № 1. — C. 1—25.

46. Code-Based Cryptosystems Using Generalized Concatenated Codes / S. Puchinger [и др.] // Springer Proceedings in Mathematics & Statistics. — Springer International Publishing, 2017. — C. 397—423. — ISBN 9783319569321. — DOI: 10.1007/978-3-319-56932-1_26.

47. *Couvreur A.*, *Lequesne M.* On the security of subspace subcodes of Reed-Solomon codes for public key encryption // IEEE Transactions on Information Theory. — 2021. — T. 68, № 1. — C. 632—648.

48. *Couvreur A.*, *Lequesne M.* On the Security of Subspace Subcodes of Reed–Solomon Codes for Public Key Encryption // IEEE Transactions on Information Theory. — 2022. — Янв. — T. 68, вып. 1. — C. 632—648. — ISSN 0018-9448. — DOI: 10.1109/TIT.2021.3120440.

49. *Couvreur A.*, *Lequesne M.*, *Tillich J.-P.* Recovering Short Secret Keys of RLCE in Polynomial Time // Post-Quantum Cryptography / под ред. J. Ding, R. Steinwandt. — Cham : Springer International Publishing, 2019. — С. 133—152.

50. *Couvreur A.*, *Marquez-Corbella I.*, *Pellikaan R.* Cryptanalysis of McEliece Cryptosystem Based on Algebraic Geometry Codes and Their Subcodes // IEEE Transactions on Information Theory. — 2017. — Т. 63, № 8. — С. 5404—5418. — ISSN 1557-9654. — DOI: 10.1109/tit.2017.2712636.

51. Cryptanalysis of LEDAcrypt / D. Apon [и др.] // Lecture Notes in Computer Science. — Springer International Publishing, 2020. — С. 389—418. — ISBN 9783030568771. — DOI: 10.1007/978-3-030-56877-1_14.

52. Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko Cryptosystems / Y. Lee [и др.] // IEEE Communications Letters. — 2020. — Т. 24, № 12. — С. 2678—2681. — ISSN 2373-7891. — DOI: 10.1109/lcomm.2020.3019054.

53. Cyclotomic idempotent-based binary cyclic codes / C. Tjhai [и др.] // Electronics Letters. — 2005. — Т. 41, № 6. — С. 341. — ISSN 0013-5194. — DOI: 10.1049/el:20057266.

54. Decoding Random Binary Linear Codes in 2 n/20: How 1+1=0 Improves Information Set Decoding / A. Becker [и др.] // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 2012. — С. 520—536. — ISBN 9783642290114. — DOI: 10.1007/978-3-642-29011-4_31.

55. Designing a Public Key Cryptosystem Based on Quasi-cyclic Subspace Subcodes of Reed-Solomon Codes / T. P. Berger [и др.] // Communications in Computer and Information Science. — Springer International Publishing, 2019. — С. 97—113. — ISBN 9783030362379. — DOI: 10.1007/978-3-030-36237-9_6.

56. *Deundyak V. M.*, *Kosolapov Y. V.* Algorithms for Majority Decoding of Group Codes // Modeling and Analysis of Information Systems. — 2015. — Т. 22, № 4. — С. 464. — ISSN 1818-1015. — DOI: 10.18255/1818-1015-2015-4-464-482.

57. *Deundyak V. M.*, *Kosolapov Y. V.* Cryptosystem Based on Induced Group Codes // Modeling and Analysis of Information Systems. — 2016. — Т. 23, № 2. — С. 137—152. — ISSN 1818-1015. — DOI: 10.18255/1818-1015-2016-2-137-152. — (in Russian).

58. *Deundyak V. M.*, *Lelyuk E. A.* A Graph-Theoretical Method for Decoding Some Group MLD-Codes // Journal of Applied and Industrial Mathematics. — 2020. — Т. 14, № 2. — С. 265—280. — ISSN 1990-4797. — DOI: 10.1134/s1990478920020064.

59. *Deundyak V.*, *Kosolapov Y.* On the Berger-Loidreau Cryptosystem on the Tensor Product of Codes // Journal of Computational and Engineering Mathematics. — 2018. — Т. 5, № 2. — С. 16—33. — ISSN 2313-8106. — DOI: 10.14529/jcem180202.

60. *Deundyak V.*, *Kosolapov Y.* The Use of the Direct Sum Decomposition Algorithm for Analyzing the Strength of Some Mceliece Type Cryptosystems // Bulletin of the South Ural State University. Series “Mathematical Modelling, Programming and Computer Software”. — 2019. — Т. 12, № 3. — С. 89—101. — ISSN 2071-0216. — DOI: 10.14529/mmp190308.

61. *Deundyak V. M.*, *Kosolapov Y. V.*, *Maystrenko I. A.* On the Decipherment of Sidel’nikov-Type Cryptosystems // Lecture Notes in Computer Science. — Springer International Publishing, 2020. — С. 20—40. — ISBN 9783030540746. — DOI: 10.1007/978-3-030-54074-6_2.

62. *Deundyak V. M.*, *Kosolapov Y. V.* On some properties of the Schur—Hadamard product for linear codes and their applications // Prikladnaya Diskretnaya Matematika. — 2020. — № 4. — С. 72—86.

63. Dihedral Quantum Codes / M. Borello [и др.]. — 2023. — arXiv: 2310.15092 [quant-ph].

64. *Ding C.*, *Li C.* BCH cyclic codes // Discrete Mathematics. — 2024. — Т. 347, № 5. — С. 113918.

65. Distinguisher-based attacks on public-key cryptosystems using Reed–Solomon codes / A. Couvreur [и др.] // Designs, Codes and Cryptography. — 2014. — Т. 73, № 2. — С. 641—666. — ISSN 1573-7586. — DOI: 10.1007/s10623-014-9967-z.

66. *Dumer I.* On syndrome decoding of linear codes // Proc. Ninth All-Union Symp. Redundancy in Information Systems. Nauka. Т. 2. — 1986. — С. 157—159.

67. *Dür A.* The automorphism groups of Reed-Solomon codes // Journal of Combinatorial Theory, Series A. — 1987. — Т. 44, № 1. — С. 69—82. — ISSN 0097-3165. — DOI: 10.1016/0097-3165(87)90060-4.

68. *Dutra F. S.*, *Ferraz R. A.*, *Milies C. P.* Semisimple group codes and dihedral codes // Algebra and Discrete Mathematics. — 2009. — № 3. — С. 28—48.

69. Enhancing Iterative Decoding of Cyclic LDPC Codes Using Their Automorphism Groups / C. Chen [и др.] // IEEE Transactions on Communications. — 2013. — Т. 61, № 6. — С. 2128—2137. — ISSN 0090-6778. — DOI: 10.1109/tcomm.2013.032713.120050.

70. *Ferraz R. A.*, *Milies C. P.* Essential idempotents in group algebras and coding theory // Indian Journal of Pure and Applied Mathematics. — 2021. — Т. 52, № 3. — С. 747—760. — ISSN 0975-7465. — DOI: 10.1007/s13226-021-00187-5.

71. *Gao Y.*, *Yue Q.*, *Wu Y.* LCD codes and self-orthogonal codes in generalized dihedral group algebras // Designs, Codes and Cryptography. — 2020. — Т. 88, № 11. — С. 2275—2287. — ISSN 1573-7586. — DOI: 10.1007/s10623-020-00778-z.

72. Group codes of dimension 2 and 3 are abelian / C. García Pillado [и др.] // Finite Fields and Their Applications. — 2019. — Т. 55. — С. 167—176. — ISSN 1071-5797. — DOI: 10.1016/j.ffa.2018.09.009.

73. GROUP CODES OVER NON-ABELIAN GROUPS / C. G. PILLADO [и др.] // Journal of Algebra and Its Applications. — 2013. — Т. 12, № 07. — С. 1350037. — ISSN 1793-6829. — DOI: 10.1142/s0219498813500370.

74. *Guo Q.*, *Johansson T.* A New Decryption Failure Attack Against HQC // Lecture Notes in Computer Science. — Springer International Publishing, 2020. — С. 353—382. — ISBN 9783030648374. — DOI: 10.1007/978-3-030-64837-4_12.

75. *Guo Q.*, *Johansson T.*, *Stankovski Wagner P.* A Key Recovery Reaction Attack on QC-MDPC // IEEE Transactions on Information Theory. — 2019. — Т. 65, № 3. — С. 1845—1861. — ISSN 1557-9654. — DOI: 10.1109/tit.2018.2877458.

76. *Gupta S.*, *Rani P.* Codes from Dihedral 2-Groups // Mathematical Notes. — 2022. — Т. 112, № 5/6. — С. 885—897. — ISSN 1573-8876. — DOI: 10.1134/s0001434622110232.

77. *Gupta S.*, *Rani P.* Central and non central codes of dihedral 2-groups // Algebra and Discrete Mathematics. — 2022. — Т. 33, № 1. — С. 87—98. — ISSN 2415-721X. — DOI: 10.12958/adm1569.

78. *Gupta S.*, *Rani P.* Codes defined over dihedral groups of order $2p^r$ // Rendiconti del Circolo Matematico di Palermo Series 2. — 2022. — Т. 72, № 4. — С. 2349—2361. — ISSN 1973-4409. — DOI: 10.1007/s12215-022-00805-z.

79. Ideal representation of Reed–Solomon and Reed–Muller codes / E. Couselo [и др.] // Algebra and Logic. — 2012. — Т. 51, № 3. — С. 195—212. — ISSN 1573-8302. — DOI: 10.1007/s10469-012-9183-8.

80. *Ivanov F.*, *Krouk E.*, *Zyablov V.* New code-based cryptosystem based on binary image of generalized Reed-Solomon code // 2021 XVII International Symposium" Problems of Redundancy in Information and Control Systems"(REDUNDANCY). — IEEE. 2021. — С. 66—69.

81. *Janwa H.*, *Moreno O.* // Designs, Codes and Cryptography. — 1996. — Т. 8, № 3. — С. 293—307. — ISSN 0925-1022. — DOI: 10.1023/a:1027351723034.

82. *Jensen J.* The concatenated structure of cyclic and Abelian codes // IEEE Transactions on Information Theory. — 1985. — Т. 31, № 6. — С. 788—793. — ISSN 0018-9448. — DOI: 10.1109/tit.1985.1057109.

83. *Kabatiansky G.*, *Tavernier C.* A new code-based cryptosystem via pseudorepetition of codes // Proceedings of ACCT XVI. — 2018. — С. 189—191.

84. *Kelarev A.*, *Solé P.* Error-correcting codes as ideals in group rings // Contemporary Mathematics. — 2001. — Т. 273. — С. 11—18.

85. *Khathuria K.*, *Rosenthal J.*, *Weger V.* Encryption scheme based on expanded Reed-Solomon codes // Advances in Mathematics of Communications. — 2021. — Т. 15, № 2. — С. 207—218. — ISSN 1930-5338. — DOI: 10.3934/amc.2020053.

86. *Kosolapov Y. V.*, *Lelyuk E. A.* On the structural security of a McEliece-type cryptosystem based on the sum of tensor products of binary Reed-Muller codes // Prikladnaya Diskretnaya Matematika. — 2022. — № 57. — С. 22—39. — ISSN 2311-2263. — DOI: 10.17223/20710410/57/2.

87. *Lally K.* Quasicyclic Codes of Index l over $\mathbb{F}_q$ Viewed as $\mathbb{F}_q$-Submodules of $(\mathbb{F}_q[x]/\langle x^m - 1\rangle)^l$ // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 15th International Symposium, AAECC-15, Toulouse, France, May 12–16, 2003 Proceedings 15. — Springer. 2003. — С. 244—253.

88. *Landrock P.*, *Manz O.* Classical codes as ideals in group algebras // Designs, Codes and Cryptography. — 1992. — Т. 2, № 3. — С. 273—285. — ISSN 1573-7586. — DOI: 10.1007/bf00141972.

89. *Langevin P.* Weights of Abelian Codes // Designs, Codes and Cryptography. — 1998. — Т. 14, № 3. — С. 239—245. — ISSN 0925-1022. — DOI: 10.1023/a:1008252803758.

90. *Lau T. S. C.*, *Tan C. H.* Polynomial-time plaintext recovery attacks on the IKKR code-based cryptosystems // Advances in Mathematics of Communications. — 2023. — Т. 17, № 2. — С. 353—366. — ISSN 1930-5338. — DOI: 10.3934/amc.2020132.

91. LDPC Codes / M. Tomlinson [и др.] // Signals and Communication Technology. — Springer International Publishing, 2017. — С. 315—354. — ISBN 9783319511030. — DOI: 10.1007/978-3-319-51103-0_12.

92. *Lee P. J.*, *Brickell E. F.* An observation on the security of McEliece's public-key cryptosystem // Workshop on the Theory and Application of of Cryptographic Techniques. — Springer. 1988. — С. 275—280.

93. *Leon J. S.* A probabilistic algorithm for computing minimum weights of large error-correcting codes // IEEE Transactions on Information Theory. — 1988. — Т. 34, № 5. — С. 1354—1359.

94. *Lint J. van*, *MacWilliams F.* Generalized quadratic residue codes // IEEE Transactions on Information Theory. — 1978. — Т. 24, № 6. — С. 730—737. — ISSN 0018-9448. — DOI: 10.1109/tit.1978.1055965.

95. *MacWilliams F. J.* Binary Codes Which Are Ideals in the Group Algebra of an Abelian Group // Bell System Technical Journal. — 1970. — Т. 49, № 6. — С. 987—1011. — ISSN 0005-8580. — DOI: 10.1002/j.1538-7305.1970.tb01812.x.

96. *MacWilliams F. J.* Codes and ideals in group algebras // Combinatorial mathematics and its applications. — 1969. — Т. 317. — С. 317—328.

97. *Marquez-Corbella I.*, *Tillich J.-P.* Using Reed-Solomon codes in the (U | U + V) construction and an application to cryptography // 2016 IEEE International Symposium on Information Theory (ISIT). — IEEE, 2016. — DOI: 10.1109/isit.2016.7541435.

98. *Martínez-Perez C.*, *Willems W.* Self-Dual Doubly Even 2-Quasi-Cyclic Transitive Codes Are Asymptotically Good // IEEE Transactions on Information Theory. — 2007. — Т. 53. — С. 4302—4308.

99. *Massey J. L.* Advances in threshold decoding // Advances in Communication Systems. Т. 3. — Elsevier, 1968. — С. 91—115.

100. *May A.*, *Meurer A.*, *Thomae E.* Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$ // Advances in Cryptology – ASIACRYPT 2011. — Springer Berlin Heidelberg, 2011. — С. 107—124. — ISBN 9783642253850. — DOI: 10.1007/978-3-642-25385-0_6.

101. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // Coding Thv. — 1978. — Т. 4244. — С. 114—116.

102. *Minder L.*, *Shokrollahi A.* Cryptanalysis of the Sidelnikov Cryptosystem // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 2007. — С. 347—360. — ISBN 9783540725404. — DOI: 10.1007/978-3-540-72540-4_20.

103. *Monico C.*, *Rosenthal J.*, *Shokrollahi A.* Using low density parity check codes in the McEliece cryptosystem // 2000 IEEE International Symposium on Information Theory (Cat. No.00CH37060). — IEEE. — (ISIT-00). — DOI: 10.1109/isit.2000.866513.

104. *Mora R.*, *Tillich J.-P.* On the dimension and structure of the square of the dual of a Goppa code // Designs, Codes and Cryptography. — 2022. — Т. 91, № 4. — С. 1351—1372. — ISSN 1573-7586. — DOI: 10.1007/s10623-022-01153-w.

105. *Natarajan L. P.*, *Krishnan P.* A Family of Capacity-Achieving Abelian Codes for the Binary Erasure Channel // 2022 National Conference on Communications (NCC). — IEEE, 2022. — DOI: 10.1109/ncc55593.2022.9806780.

106. *Natarajan L. P.*, *Krishnan P.* Berman Codes: A Generalization of Reed-Muller Codes that Achieve BEC Capacity // 2022 IEEE International Symposium on Information Theory (ISIT). — IEEE, 2022. — DOI: 10.1109/isit50566.2022.9834598.

107. New Examples of Non-Abelian Group Codes / C. G. Pillado [и др.] // CIM Series in Mathematical Sciences. — Springer International Publishing, 2015. — С. 203—208. — ISBN 9783319172965. — DOI: 10.1007/978-3-319-17296-5_21.

108. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory // Prob. Contr. Inform. Theory. — 1986. — Т. 15, № 2. — С. 157—166.

109. *Nilsson A.*, *Johansson T.*, *Stankovski Wagner P.* Error Amplification in Code-based Cryptography // IACR Transactions on Cryptographic Hardware and Embedded Systems. — 2018. — С. 238—258. — ISSN 2569-2925. — DOI: 10.46586/tches.v2019.i1.238-258.

110. Non-Abelian Group Codes over an Arbitrary Finite Field / C. García Pillado [и др.] // Journal of Mathematical Sciences. — 2017. — Т. 223, № 5. — С. 504—507. — ISSN 1573-8795. — DOI: 10.1007/s10958-017-3363-y.

111. *Olteanu G.*, *Van Gelder I.* Construction of minimal non-abelian left group codes // Designs, Codes and Cryptography. — 2014. — Т. 75, № 3. — С. 359—373. — ISSN 1573-7586. — DOI: 10.1007/s10623-014-9922-z.

112. On a Class of Left Metacyclic Codes / Y. Cao [и др.] // IEEE Transactions on Information Theory. — 2016. — Т. 62, № 12. — С. 6786—6799. — ISSN 1557-9654. — DOI: 10.1109/tit.2016.2613115.

113. *Otmani A.*, *Kalachi H. T.* Square Code Attack on a Modified Sidelnikov Cryptosystem // Codes, Cryptology, and Information Security. — Springer International Publishing, 2015. — С. 173—183. — ISBN 9783319186818. — DOI: 10.1007/978-3-319-18681-8_14.

114. *Otmani A.*, *Tillich J.-P.*, *Dallot L.* Cryptanalysis of Two McEliece Cryptosystems Based on Quasi-Cyclic Codes // Mathematics in Computer Science. — 2010. — Т. 3, № 2. — С. 129—140. — ISSN 1661-8289. — DOI: 10.1007/s11786-009-0015-8.

115. *Peterson W. W.*, *Brown D. T.* Cyclic codes for error detection // Proceedings of the IRE. — 1961. — Т. 49, № 1. — С. 228—235.

116. *Polcino Milies C.*, *Melo F. D. de.* On Cyclic and Abelian Codes // IEEE Transactions on Information Theory. — 2013. — Т. 59, № 11. — С. 7314—7319. — ISSN 1557-9654. — DOI: 10.1109/tit.2013.2275111.

117. *Prange E.* Cyclic error-correcting codes in two symbols // TN-57-013, Technical notes issued by Air Force Cambridge Research Labs. — 1957.

118. *Prange E.* The use of information sets in decoding cyclic codes // IRE Transactions on Information Theory. — 1962. — Т. 8, № 5. — С. 5—9.

119. *Rajan B.*, *Siddiqi M.* Transform domain characterization of abelian codes // IEEE Transactions on Information Theory. — 1992. — Т. 38, № 6. — С. 1817—1821. — ISSN 0018-9448. — DOI: 10.1109/18.165458.

120. Reed-Muller codes achieve capacity on erasure channels / S. Kudekar [и др.] // Proceedings of the forty-eighth annual ACM symposium on Theory of Computing. — ACM, 2016. — (STOC '16). — DOI: 10.1145/2897518.2897584.

121. *Sabin R. E.* On determining all codes in semi-simple group rings // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 1993. — С. 279—290. — ISBN 9783540476306. — DOI: 10.1007/3-540-56686-4_50.

122. *Sabin R. E.* On minimum distance bounds for abelian codes // Applicable Algebra in Engineering, Communication and Computing. — 1992. — Т. 3, № 3. — С. 183—197. — ISSN 1432-0622. — DOI: 10.1007/bf01268659.

123. *Sabin R. E.* On row-cyclic codes with algebraic structure // Designs, Codes and Cryptography. — 1994. — Т. 4, № 2. — С. 145—155. — ISSN 1573-7586. — DOI: 10.1007/bf01578868.

124. *Sabin R. E.*, *Lomonaco S. J.* Metacyclic error-correcting codes // Applicable Algebra in Engineering, Communication and Computing. — 1995. — Т. 6, № 3. — С. 191—210. — ISSN 1432-0622. — DOI: 10.1007/bf01195337.

125. *Sakata S.* Decoding binary 2-D cyclic codes by the 2-D Berlekamp-Massey algorithm // IEEE Transactions on Information Theory. — 1991. — Т. 37, № 4. — С. 1200—1203. — ISSN 0018-9448. — DOI: 10.1109/18.86974.

126. *Santini P.*, *Persichetti E.*, *Baldi M.* Reproducible families of codes and cryptographic applications // Journal of Mathematical Cryptology. — 2021. — Т. 16, № 1. — С. 20—48.

127. Security of generalised Reed-Solomon code-based cryptosystems / M. Baldi [и др.] // IET Information Security. — 2019. — Т. 13, № 4. — С. 404—410.

128. *Sehrawat S.*, *Pruthi M.* Codes over non-abelian groups // Journal of Information and Optimization Sciences. — 2019. — Т. 40, № 3. — С. 789—804. — ISSN 2169-0103. — DOI: 10.1080/02522667.2018.1563956.

129. *Sendrier N.* Finding the permutation between equivalent linear codes: the support splitting algorithm // IEEE Transactions on Information Theory. — 2000. — Т. 46, № 4. — С. 1193—1203. — ISSN 0018-9448. — DOI: 10.1109/18.850662.

130. *Sendrier N.* On the Concatenated Structure of a Linear Code // Applicable Algebra in Engineering, Communication and Computing. — 1998. — Т. 9, № 3. — С. 221—242. — ISSN 1432-0622. — DOI: 10.1007/s002000050104.

131. *Shor P.* Algorithms for quantum computation: discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. — IEEE Comput. Soc. Press. — (SFCS-94). — DOI: 10.1109/sfcs.1994.365700.

132. *Sidelnikov V. M.* A public-key cryptosystem based on binary Reed-Muller codes // Discrete Mathematics and Applications. — 1994. — Т. 4, № 3. — ISSN 1569-3929. — DOI: 10.1515/dma.1994.4.3.191.

133. *Sidelnikov V. M.*, *Shestakov S. O.* On an encoding system constructed on the basis of generalized Reed–Solomon codes // Diskretnaya Matematika. — 1992. — Т. 4, № 3. — С. 57—63.

134. Statistical Decoding 2.0: Reducing Decoding to LPN / K. Carrier [и др.] // Lecture Notes in Computer Science. — Springer Nature Switzerland, 2022. — С. 477—507. — ISBN 9783031229725. — DOI: 10.1007/978-3-031-22972-5_17.

135. Status report on the third round of the NIST post-quantum cryptography standardization process / G. Alagic [и др.] // US Department of Commerce, NIST. — 2022.

136. *Stern J.* A method for finding codewords of small weight // Lecture Notes in Computer Science. — Springer-Verlag. — С. 106—113. — ISBN 3540516433. — DOI: 10.1007/bfb0019850.

137. Variations of the McEliece cryptosystem / J. Bolkema [и др.] // Algebraic Geometry for Coding Theory and Cryptography: IPAM, Los Angeles, CA, February 2016. — Springer. 2017. — С. 129—150.

138. *Vedenev K. V.*, *Deundyak V. M.* Codes in a Dihedral Group Algebra // Automatic Control and Computer Sciences. — 2019. — Т. 53, № 7. — С. 745—754. — ISSN 1558-108X. — DOI: 10.3103/s0146411619070198.

139. *Vedenev K. V.*, *Deundyak V. M.* Relationship between Codes and Idempotents in a Dihedral Group Algebra // Mathematical Notes. — 2020. — Т. 107, № 1/2. — С. 201—216. — ISSN 1573-8876. — DOI: 10.1134/s0001434620010204.

140. *Vedenev K.* The Structure of Some Split Metacyclic Group Algebras // «Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории» Материалы XVIII Международной конференции, посвященной 100-летию со дня рождения профессоров Б. М. Бредихина, В. И. Нечаева и С. Б. Стечкина. — 2020. — С. 120—123.

141. *Vedenev K.*, *Kosolapov Y.* A Reaction Attack against Cryptosystems Based on Quasi–Group MDPC Codes // 2023 XVIII International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY). — 2023. — С. 70—75. — DOI: 10.1109/Redundancy59964.2023.10330086.

142. *Vedenev K.*, *Kosolapov Y.* Cryptanalysis of Ivanov–Krouk–Zyablov Cryptosystem // Lecture Notes in Computer Science. — Springer Nature Switzerland, 2023. — С. 137—153. — ISBN 9783031296895. — DOI: 10.1007/978-3-031-29689-5_8.

143. *Vedenev K.*, *Kosolapov Y.* On Squares of Dihedral Codes // 2021 XVII International Symposium" Problems of Redundancy in Information and Control Systems"(REDUNDANCY). — IEEE. 2021. — С. 55—60.

144. *Vedenev K.*, *Kosolapov Y.* Theoretical analysis of decoding failure rate of non-binary QC-MDPC codes // Code-Based Cryptography - 11th International Workshop CBCrypto 2023. Т. 14311 / под ред. A. Esser, P. Santini. — Springer Nature Switzerland, 2023. — (Lecture Notes in Computer Science). — (to appear, eprint: https://eprint.iacr.org/2023/1224).

145. *Vedenev K. V.*, *Deundyak V. M.* Codes in Dihedral Group Algebra // Modeling and Analysis of Information Systems. — 2018. — Т. 25, № 2. — С. 232—245. — ISSN 1818-1015. — DOI: 10.18255/1818-1015-2018-2-232-245.

146. *Vedenev K. V.*, *Deundyak V. M.* Some properties of dihedral group codes. — 2020. — arXiv: 2005.08283 [math.RA].

147. *Wang T.*, *Wang A.*, *Wang X.* Exploring Decryption Failures of BIKE: New Class of Weak Keys and Key Recovery Attacks // Lecture Notes in Computer Science. — Springer Nature Switzerland, 2023. — С. 70—100. — ISBN 9783031385483. — DOI: 10.1007/978-3-031-38548-3_3.

148. *Wang Y.* Quantum resistant random linear code based public key encryption scheme RLCE // 2016 IEEE International Symposium on Information Theory (ISIT). — IEEE, 2016. — DOI: 10.1109/isit.2016.7541753.

149. When are all group codes of a noncommutative group Abelian (a computational approach)? / C. G. Pillado [и др.] // Journal of Mathematical Sciences. — 2012. — Т. 186, № 4. — С. 578—585. — ISSN 1573-8795. — DOI: 10.1007/s10958-012-1006-x.

150. *Wieschebrink C.* Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes // Lecture Notes in Computer Science. — Springer Berlin Heidelberg, 2010. — С. 61—72. — ISBN 9783642129292. — DOI: 10.1007/978-3-642-12929-2_5.

151. *Zimmermann K.-H.* Beiträge zur algebraischen Codierungstheorie mittels modularer Darstellungstheorie. — Lehrstuhl II für Mathematik, Universität Bayreuth, 1994.

152. *Zyablov V.*, *Shavgulidze S.*, *Bossert M.* An Introduction to Generalized Concatenated Codes // European Transactions on Telecommunications. — 1999. — Т. 10, № 6. — С. 609—622. — ISSN 1541-8251. — DOI: 10.1002/ett.4460100606.