Федеральное государственное автономное образовательное
учреждение высшего образования «Национальный
исследовательский университет «Высшая школа экономики»

На правах рукописи

Иванов Федор Ильич

Помехоустойчивое кодирование в задачах достоверной и защищенной передачи данных

–

РЕЗЮМЕ

диссертации на соискание ученой степени
доктора наук по прикладной математике

Москва – 2022

Общая характеристика работы

Актуальность работы и постановка проблемы

Активное развитие вычислительной техники и информационных технологий, наблюдаемое в настоящий момент, приводит к все более стремительному усилению требований, предъявляемых к системам передачи информации. Основными требованиями, предъявляемыми к современным телекоммуникационным системам, являются: скорость (объем передаваемых данных на единицу времени), достоверность (вероятность корректного приема и обработки данных) и поддерживаемое число активных абонентов системы. Кроме того, по мере все большей цифровизации современного общества, также крайне актуальными становятся вопросы безопасности, то есть защищенной передачи данных по (в первую очередь) открытым каналам связи. Удовлетворение требований на скорость и достоверность невозможно без использования методов помехоустойчивого кодирования.

В ранних телекоммуникационных системах в качестве помеустойчивых кодов выступали, в первую очередь, алгебраические коды (например, коды БЧХ, Рида-Соломона, Рида-Маллера и др.), которые использовались совместно с их декодерами до половины кодового расстояния (Bounded Distance Decoder). Однако теория кодирования, основанная на алгебраических кодах с их декодированием до половины расстояния, уже не способна удовлетворять покрывать все

сценарии использования современных систем обработки, передачи и хранения информации.

Вместе с тем, активный качественный скачок развития вычислительной техники, наблюдаемый с начала 1990-х, открыл возможность реализации длинных кодов, имплементация которых до этого была затруднительна. Именно новые доступные вычислительные мощности явились причиной активных исследований в области построения длинных кодов, для которых существуют эффективные полиномиальные алгоритмы декодирования, практически реализующие декодирование по максимальному правдоподобию.

В частности, во многих случаях оказались востребованы коды с малой плотностью проверок на четность (МПП-коды), были разработаны такие классы кодов, как турбо-коды, полярные и др. Для этих классов кодов используются методы вероятностного декодирования, теория которых далека от своего завершения. Актуальной становится задача совместного выбора кодов и методов их декодирования. Особенно следует отметить, что при вероятностном декодировании такие метрики, как структура циклов в двудольном графе кода, структура стоп-множеств и др играют не меньшую роль, чем такие классические метрики, как минимальное расстояние и спектр весов. Поэтому актуальной становится задача построения кодовых конструкций, обладающих не только хорошими дистантными и спектральным свойствами, но и обладающими хорошей структурой цик-

лов в графе, подкодов и др.

Как уже было отмечено выше, одним из ключевых требований, предъявляемым к современным телекоммуникационным системам, является достоверность (качество) передаваемых данных. Например, существующие на сегодняшний день, а также перспективные системы, использующие связь по оптоволокну, допускают потерю одного пакета данных из 10^{15}. Это означает, что для выбора кода-кандидата, предлагаемого к использованию в такого рода системах, требуется провести не менее $10^{16} - 10^{18}$ итераций его моделирования, для получения требуемой вероятности ошибки на блок 10^{-15}. Очевидно, что такого рода моделирование ведет с существенным временным и накладным расходам, а в некоторых случаях в принципе не реализуемо. В связи с этим особенно актуальной становится задача построения достаточно точных аналитических оценок, позволяющих оценить эффективность заданного кода без проведения или с минимальным объемом имитационного моделирования.

Решению задачи построения эффективных классов МПП-кодов, а также задачи разработки математического аппарата исследования корректирующих свойств сверточных кодов посвящена первая глава диссертационной работы.

Еще одним существенным требованием является скорость передачи информации, напрямую связанная с временем декодирования. Другими словами, важной для ряда приложений становится задача

минимизации задержки на передачу пакета информации. В первую очередь такими приложениями выступает промышленный интернет вещей, управляющие системы, широкополосная передача видеоконтента, различные приложения дополненной и виртуальной реальности и др. Для удовлетворения данному требованию при заданном уровне достоверности, требуется прибегать к поиску простых алгоритмов кодирования и декодирования кодовых конструкций, не уступающих по эффективности оригинальным. Подходы к решению данной задачи применительно к полярным кодам Арикана рассматривается во второй главе диссертации.

Дополнительное требование, которое с увеличением плотности сетей передачи данных, становится все более значимым, заключается в обеспечении возможности большому числу устройств/абонентов системы вести передачу данных на базовую станцию с заданным уровнем достоверности и задержки. Примером системы, где требование на число активных абонентов является определяющим, может послужить Интернет Вещей (допускается до одного миллиона устройств на квадратный километр). Понятно, что традиционные системы "точка-точка предполагающие одну линию связи между отправителем информации и ее получателем, будут неэффективны в такого рода сценариях. В связи с этим появилась необходимость разрабатывать методы неортогонального некоординированного множественного доступа, допускающую только синхронизацию блоков.

Для анализа эффективности того или иного метода множественного доступа необходимо оценивать его пропускную способность с точки зрения объема информации, которую может передать заданный абонент в сети при заданном ограничении на число других абонентов и другие параметры системы. Решение задачи построения систем множественного доступа приведено в третьей главе.

Наконец, в последнее время все более критическим становится требование обеспечения безопасности передачи данных. Это связано с тем, что цифровые технологии все больше проникают в нашу жизнь, делая многие сферы жизнедеятельности человека, нормальное функционирование организаций и целых отраслей экономики зависимым от нормального функционирования ряда информационных систем и приложений. Следует отметить, что в настоящий момент проблема безопасности не только окончательно не решена, но в целых отраслях, таких, как Интернет Вещей, нет единого понимания того, каким образом следует организовывать защиту. Кроме того, определенную тревогу вызывает также и то, что подавляющее большинство традиционных методов защиты информации, передаваемой по открытым каналам связи, уже не могут считаться надежными, ввиду возможности их взлома с использованием квантового компьютера. В связи с этим становится актуальной разработка таких перспективных методов криптографической защиты данных, которые было бы достаточно легко имплементировать, но которые также бы

не поддавались криптоанализу с использованием квантовых алгоритмов. Разработка постквантовых методов криптографической защиты информации, основанных на системе Мак-Элиса, была проведена в четвертой главе работы.

Существенный вклад в решение проблем построения семейств высокоэффективных кодов, разработки эффективных методов их кодирования, декодирования и исследования их свойств, разработки методов множественного доступа, а также проблемы иссследования и построения кодовых криптосистем, внесли в нашей стране В. Б. Афанасьев, А. М. Барг, Л. А. Бассылыго, Э. Л. Блох, С. В. Беззатеев, И. Е. Бочарова, Э. М. Габидулин, И. И. Думер, К. Ш. Зигангиров, В. А. Зиновьев, В. В. Зяблов, Г. А. Кабатянский, В. Д. Колесник, Е. А. Крук, Б. Д. Кудряшов, Е. Т. Мирончиков, Д. С. Осипов, М. С. Пинскер, Ю. Полянский, П. С. Рыбин, Ю. Л. Сагалович, В. М. Сидельников, В. Р. Сидоренко, Ф. И. Соловьева, П. В. Трифонов, С. В. Федоренко, А. А. Фролов, С. О. Шестаков, Н. А. Шехунова, за рубежом Э. Арикан, М. Балди, Э. Берлекэмп, Р. Блейхут, А. Варди, С. Джонсон, Р. Галлагер, В. Гурусвами, Т. Касами, Р. Кеттер, С. Кудекар, С. Кумар, Р. Мак-Элис, Дж. Месси, Т. Ричардсон, М. Судан, И. Тал, Т. Танака, Р. Урбанке, М. Фоссорье и многие другие.

Цель диссертационной работы

Классическая теория кодирования развивалась в направлении создания новых классов кодов, обладающих хорошими по отноше-

нию к границам параметрами (скоростью, спектром, кодовым расстоянием). Создаваемые алгоритмы декодирования были ориентированы на реализацию корректирующих возможностей этих кодов с возможно меньшей сложностью. Между тем развитие теории и техники использования кодов (связь, системы хранения данных, системы защиты информации) привело к постановке задачи совместного выбора кодов и методов декодирования, ориентированных на на использование в конкретной прикладной задаче.

Целью настоящей диссертационной работы является построение и анализ сигнально-кодовых конструкций и алгоритмов их декодирования для неметрических моделей каналов и сценариев передачи данных.

При этом объектами исследований являются линейные коды, системы множественного доступа и системы защиты информации, основанные на помехоустойчивых линейных кодах, а предметом исследований — методы построения линейных кодов и способы их декодирования, методы построения систем множественного доступа и оценки их пропускных способностей, а также методы построения и анализа систем защиты информации, основанных на помехоустойчивых кодах.

Для достижения указанных целей в работе решаются следующие задачи:

1. Разработка новых конструкций кодов с малой плотностью про-

верок (МПП-кодов), основанных на комбинаторных конструкциях и матрицах перестановок, которые позволяют кодировать и декодировать данные коды с умеренной сложностью, а также оценка экспоненты вероятности ошибки некоторых регулярных конструкций МПП-кодов, при их фиксированной длине.

2. Разработка математического аппарата исследования корректирующих свойств сверточных кодов, который основан на анализе свойств спектра активных расстояний, а также исследование свойств локального исправления стираний сверточными кодами.

3. Постоение высокоэффективных и низкоресурсных схем декодирования полярных кодов, которые основаны на списочных алгоритмах с инвертированием информационных символов и быстром декодировании подкодов полярных кодов.

4. Разработка эффективных методов неортогонального множественного доступа, ориентированных на некоординированную передачу коротких пакетов данных от устройств на базовую станцию, оценка пропускной способности для предложенного метода передачи, а также построение кодовых конструкций для разрешения коллизий, возникающих при указанном выше методе передачи.

5. Разработка методов обеспечения безопасной передачи данных

в системах множественного доступа.

Степень разработанности проблемы и задач диссертационной работы

Анализ степени проработанности проблем, сформулированых выше, должен учитывать требования, которые в настоящий момент предъявляются к системам передачи информации. Соответствие текущего прогресса в исследованиях с практическими требованиями, которые ставятся перед разрабатываемыми системами передачи, обработки и хранения информации, позволит охарактеризовать степень проработанности проблемы.

С каждым годом системы передачи информации все более усложняются, что продиктовано как новыми сценариями, появившимися в последнее время (передача данных между устойствами Интернета Вещей, потоковое видео, виртуальная и дополненная реальности, и т. д.), так и возросшими объемами передаваемого трафика. Но, чем более сложна и универсальна система, тем более высокие требования к ней предъявляются.

Если рассмотреть в качестве примера передачу данных по сотовым сетям связи 5-го поколения (стандарт 5G) [1], то можно выделить 3 основных сценария передачи, для которых актуальны все обозначенные выше проблемы:

- Массовое межмашинное взаимодействие (mMTC) — область применения характеризуется возможностью подключения очень

большого количества простых (зачастую одноплатных) устройств. Ключевым требованием для данного сценария является поддержка большого числа одновременно работающих в сети устройств (до 1 млн. устройств на 1 км. кв. [39]) и простота используемых протоколов передачи информации.

- Передача данных со высокой надежностью и сверхмалой задержкой (URLLC) — ориентирована на предоставление высоконадежного соединения с очень низкой задержкой передачи данных. Ключевым требованием в этом случае служит задержка на передачу данных, она должна не превосходить 1 мс. (в 10 раз меньше, чем в LTE) [8], при этом также требуется достаточно высокая вероятность корректной доставки пакета данных.

- Усовершенствованная мобильная широкополосная связь (eMBB) — ориентирована на поддержку постоянно возрастающей скорости передачи данных и производительности систем [59]. Основным требованием, предъявлемым к данному сценарию, является скорость передачи данных. В частности, она в 50 раз выше, чем в стандарте LTE [63].

Сформулированные выше требования определяют ключевой стек технологий, которые используются при реализации системы передачи данных, используемой для того или иного сценария передачи. И именно в разрезе требований каждого из сценариев следует анали-

зировать возможность применимости той или иной схемы передачи данных, так и степень ее проработанности.

В частности, если говорить про передачу больших объемов данных между небольшим числом абонентов, то можно говорить о схеме передачи ”точка-точка”, где передача данных осуществляется по одной линии от отправителя к получателю. Ключевой задачей, которую требуется решить при передаче информации по схеме ”точка-точка” является обеспечение максимальной скорости передачи (минимизация задержки) при малой вероятности ошибки.

В качестве кодовых конструкций, которые используются в такого рода передаче, выступают полярные коды, коды с малой плотностью проверок на четность (МПП-коды), различные каскадные конструкции как на базе вышеупомянутых кодов, так и на основе алгебраических кодов, сверточных кодов и др.

Коды с малой плотностью проверок были впервые предложены Р. Галлагером в 1960 году в работе [29]. В этой же работе автором была получена нижняя оценка минимального кодового расстояния, а также предложены практически применимые алгоритмы декодирования МПП-кодов: многократный мажоритарный алгоритм и алгоритм "распространения доверия". Ввиду недостаточного уровня развития вычислительной техники, МПП-коды непосредственно после их открытия не нашли широкого применения и были забыты до конца 1990-х.

Активное исследование МПП-кодов возобновилось в конце 1990-х, когда они были ”переоткрыты” Д. Маккеем в статье [42]. С тех пор МПП-коды стали одним из самых популярных направлений для исследований в области помехоустойчивого кодирования.

На сегодняшний день некоторые конструкции МПП-кодов (в частности, квазициклические коды, адаптируемые по скорости передачи [52], [41]) вошли в стандарт 5G в качестве помехоустойчивых кодов канального уровня сценария URLLC (передача данных с высокой достоверностью и малой задержкой) [41], [40], в стандарт 5G EMBB (широкополосная передача) [30], [49]. Среди других практических приложений МПП-кодов следует выделить стандарт IEEE 802.11n/ac (WiFi) [58], стандарт цифрового телевидения DVB S2 [24] и другие. Вместе с тем следует отметить, что используемые в настоящий момент кодовые конструкции получены методом оптимизации некоторого целевого функционала (например, метод эволюции плотностей или метод P-EXIT-кривых), что в свою очередь говорит о недостатке конструктивных методов построения высокоэффективных кодовых конструкций с гарантированными свойствами.

Наряду с построением конструкций МПП-кодов важной и актуальной задачей является изучение вероятности ошибки декодирования. Это связано как с тем, что не всегда возможно промоделировать длинный МПП-код до нужной вероятности ошибки, так и с тем, что получение границ на вероятность ошибочного декодирования позво-

ляет оценить эффект от использования МПП-кодов в качестве компонент составных кодовых конструкций.

Существует небольшое число работ, где рассматривалось неасимптотическое поведение МПП-кодов. В статье [48] исследовалось поведение МПП-кодов конечной длины в области “начала водопада” (таких отношений сигнал-шум, где начинается уменьшение выходной вероятности ошибки на кодовое слово после декодирования). В работах [28], [54], [64] для описания ошибок декодирования были использованы различные комбинаторные методики. Такой подход позволил авторам получить оценки для средней вероятности ошибки на блок и на бит при использовании итеративных алгоритмов декодирования. Большинство рассмотренных выше работ оперируют только с двоичным стирающим каналом и алгоритмами декодирования с малой сложностью (например, с мажоритарным или алгоритмом “распространения доверия”). Лишь небольшое число работ посвящено каналам с ошибками.

Таким образом, анализируя степень проработанности проблемы построения, декодирования и анализа эффективности МПП-кодов следует отметить, что хотя на сегодняший день представлено большое число конструкций длинных МПП-кодов и алгоритмов их декодирования, открытыми и актуальными остаются вопросы разработки алгебраических и комбинаторных методов построения МПП-кодов, допускающих их эффективное декодирование алгоритмами

“распространения доверия” а также задачи теоретической оценки помехоустойчивости МПП-кодов конечных длин.

Еще одним классом кодов, которые используются в современных телекоммуникационных стандартах, являются полярные коды.

Данный класс кодов был предложен Ариканом в [15]. Основной результат данной работы заключается в том, что в ней было строго доказано, что полярные коды могут достигать пропускной способности любых симметричных дискретных каналов без памяти с двоичным входным алфавитом при их декодировании алгоритмом последовательного исключения (англ. Succesive Cancellation), при условии, что длина блока стремится к бесконечности. Основным недостатком SC-декодирования является относительно низкая эффективность (с точки зрения вероятности ошибки на блок) для фиксированной длины кода.

Основное усилие исследователей было направлено на поиск более эффективных алгоритмов декодирования полярных кодов, которые бы позволили реализовать их потенциальные корректирующие свойства. В частности, в работах [47; 57] был предложен списочный вариант SC. В работах [10; 27; 31; 32; 34] был предложен подход обобщенного декодирования полярных кодов, что позволяет уменьшить число операций декодирования без существенного ухудшения корректирующих свойств. Еще одно направление исследований направлено на решение проблемы пространственной сложности декодиро-

вания. Алгоритм последовательного исключения с инвертированием бит был впервые представлен в [7], а в работе было предложено его обобщение [18] для списочного декодирования.

Анализируя степень проработанности проблемы построения эффективных и низкоресурсных алгоритмов декодирования полярных кодов следует отметить, что в основном исследователи решали две параллельные задачи — снижение пространственной сложности списочных декодеров за счет увеличения вычислительной сложности (декодеры на основе инвертирования) и снижение вычислительной сложности либо за счет роста пространственной (стековые алгоритмы), либо за счет быстрого декодирования обобщенных узлов дерева полярного кода. Вместе с тем достаточно слабо проработана проблема совместной пространственно-вычислительной оптимизации декодеров полярных кодов.

Помимо блоковых кодов, также существуют сверточные коды, использование которых в ряде приложений оказывается более эффективным. Сверточные коды были предложены П. Элайесом в 1955 [26]. В 1967 г. Э. Витерби предложил относительно простой алгоритм декодирования сверточных кодов, реализующий максимальное правдоподобие [61] и минимизирующий вероятность ошибки на блок. В 1974 году был предложен алгоритм декодирования BCJR [50], минимизирующий вероятность ошибки на бит (символ). Систематические рекурсивные сверточные коды ялвяются основной компонентой

Турбо-кодов [17], широко используемым в настоящее время в телекоммункационных стандартах [13]. Именно использование сверточных кодов в качестве компонент, а не в качестве самостоятельных кодовых конструкций, определило направление исследований, связанное в первую очередь с теоретическим анализом помехоустойчивости данных кодов. Ключевым математическим аппаратом в этом случае служат цепи Маркова [4; 35; 62]. Однако следует отметить, что использование данного аппарата приводит к достаточно грубым оценкам эффективности сверточных кодов (вероятности ошибки на блок и на бит). В связи с этим актуальной становится задача построения нового математического аппарата теоретического анализа эффективности сверточных кодов, который с одной стороны давал бы достаточно точные оценки, а с другой — был бы вычислительно эффективным и реализуемым на практике.

Не всегда удается или не всегда целесообразно организовывать систему передачи по сценарию "точка-точка". В частности, для рассмотренного выше сценария массового межмашинного взаимодействия это бы означало наличие около 1 миллиона одиночных линий между конечным устройством и станцией, принимающей информацию от этих устройств. В этом и подобном ему случаях предпочтительнее воспользоваться другой парадигмой: методами множественного доступа [3]. В этом случае предполагается, что множество абонентов/устройств используют единую линию (канал передачи дан-

ных) для отправки информации на базовую станцию (другому абоненту или узлу сети). В зависимости от того, каким образом выстроена модель множественного доступа к единому частотно-временному ресурсу (каналу передачи данных), выделяют различные методы множественного доступа. В первую очередь, методы разделяются на ортогональные и неортогональные.

Ортогональные методы множественного доступа подразумевают разделение канала между абонентами: это может быть частотное (FDMA) [45], временное (TDMA) [46], частотно-временное (TFDMA) [20] и кодовое разделения (CDMA) [33]. Ортогональные методы множественного доступа используются в стандарте IEEE 802.16 (WiMAX) [2], IEEE 802.11ax (беспроводная локальная сеть) [5], IEEE 802.20 [19], нисходящая связь (downlink) в 4G LTE [22] и др.

Неортогональные методы множественного доступа подразумевают отсутствие разделения канальных ресурсов между пользователями. Вместо того, чтобы делить ресурсы, в таких системах разрешают коллизии, возникающие при передаче информации от абонентов на базовую станцию. Оказывается, что при таком подходе можно существенно увеличить объем передаваемого трафика по сравнению с методами ортогонального доступа при одном и том же качестве обслуживания [21]. Одним из первых примеров системы неортогонального множественного доступа является сеть ALOHA [6]. На сегодняшний день существует множество моделей неортогонально-

го множественного доступа, в первую очередь различающихся методами доступа к каналу и алгоритмами разрешения коллизий. В частности, если устройство имеет возможность прослушивать канал (несущую) то выделяют методы множественного доступа к контролем несущей (CSMA) [9]. Методы неортогонального множественного доступа стали неотъемлемой частью современных телекоммуникационных стандратов. В частности, они являются частью протоколов канального уровня в 5G (mMTC) [51], нового стандарта телевещания в США ATSC 3.0 [12], используются в восходящей связи (uplink) от устройств к базовой станции в стандарте 4G LTE [14] и др. Очевидно, что во всех перспективных системах передачи информации, которые должны обеспечивать одновременную работу большого числа абонентов, для доступа к радиоресурсу будут использованы преимущественно методы неортогонального множественного доступа.

Отметим, что большинство широко известных кодовых конструкций, которые используются в классических многопользовательских каналах, например системы на основе кодового разделения (CDMA), разделения скоростей [55], чередования [36], предполагают координирование передачи между пользователями. Кроме того, параметры таких схем, такие как разделяющая последовательность, кодовые скорости, графы Таннера кодов и т. д., зависят от числа пользователей в системе. Координированная передача и дополнительные ограничения влекут за собой усложнение архитектуры сети множественного

доступа и протоколов обмена данными. Таким образом, классические системы множественного доступа оказываются неприменимыми для сценариев, где предполагается обмен короткими пакетами данных между большим числом абонентов с ограниченными вычислительными ресурсами (сценарии массового межмашинного взаимодействия и Интернета вещей). Для данных сценариев требуется разрабатывать специальные простые протоколы обмена данными, предусматривающие отсутствие координации между устройствами.

Следует также отметить, что развитие систем множественного доступа должно сопровождаться развитием методов асимметричной криптографии, используемых для шифрования данных в этих системах. Связано это в первую очередь с тем, что при использовании общего канала связи абонент не должен иметь возможность прочесть ту информацию, которую другой абонент отправил на базовую станцию. Это препятствует передаче общего ключа, который используется в симметричных схемах шифрования и в целом делает использование симметричных шифров затруднительным в данном сценарии. Поэтому для организации защищенной передачи даннных более эффективным является подход, когда все пользователи могут использовать единый ключ шифрования сообщений, но только базовая станция имеет возможность осуществлять дешифрование. Таким образом, мы приходим к методам асимметричной криптографии.

Методы теории помехоустойчивого кодирования давно исполь-

зуются в криптографии. С их помощью были построены одни из первых криптосистем с открытым ключом [44] и системы цифровой подписи [37]. Однако на практике кодовые криптосистемы применяются значительно реже алгебраических криптосистем, основанных на задачах факторизации [56] и вычисления дискретного логарифма [25]. Хотя кодовые криптосистемы выигрывают у алгебраических по времени шифрования/расшифрования [60], их использование в значительной степени ограничивается рядом объективных и субъективных факторов.

Во-первых, алгебраические системы, возникли несколько раньше кодовых и сразу прошли через многочисленные испытания их безопасности. Последнее обстоятельство является в условиях отсутствия доказательной стойкости криптосистем с открытым ключом определенной гарантией безопасности.

Во-вторых, для первых кодовых криптосистем (система Мак-Элиса) было характерно наличие открытого ключа, существенно более длинного, чем для алгебраических систем (например, системы RSA).

В дальнейшем, исследования кодовых криптосистем позволили существенно уменьшить размер открытого ключа [53], [11], а разработка новых методов решения задачи факторизации [38] заставила увеличить длину открытого ключа алгебраических криптосистем настолько, что эти величины открытых ключей стали соизмеримы [16].

Следует отметить общую черту всех исследований, направленных на сокращение размеров публичного ключа. Суть улучшений состоит в том, что исходный код Гоппы заменяется на другой класс кодов, допускающих более компактное представление. При этом безопасность криптосистемы Мак-Элиса и всех такого рода улучшений не основана на NP-сложной проблеме декодирования по максимуму правдоподобия, так как в рамках криптосистемы Мак-Элиса предполагается исправлять только ошибки веса до $d/2$, где d — минимальное расстояние кода. Такие алгоритмы называются *декодированием до половины минимального расстояния* или *декодированием HMD*. Следует обратить внимание, что неизвестно, является ли декодирование HMD NP-трудной задачей (или нет). Некоторые оценки сложности декодирования HMD можно найти в [43], [23]. При этом отсутствуют исследования, направленные на разработку таких криптосистем, в которых безопасность схемы определяется не декодированием векторов малого веса (HMD), а определяется сложностью декодирования максимального правдоподобия.

Личный вклад автора

Все результаты и положения, выносимые на защиту, получены автором лично. Автором разработана концепция синтеза проверочных матриц кодов с малой плотностью проверок на четность, совмещающая использование некоторой заданной алгебраической структуры с детерминированными свойствами (в первую очередь дистант-

ными и свойствами, связанными со структурой циклов в протографе Таннера) с циркулянтными матрицами перестановок. Автором впервые проанализирована связь между минимальным расстоянием таких кодов и свойством циркулянтных матриц. На основе полученных результатов были предложены методики выбора матриц циклических сдвигов, гарантирующих строгое увеличение минимального расстояния.

Анализируя степень проработанности проблемы построения эффективных и низкоресурсных алгоритмов декодирования полярных кодов, автором был предложен новый класс декодеров, совмещающих подход с инвертированием информационных символов и быстрым списочным декодированием поддеревьев полярного кода.

Автором предложен новый математический аппарат исследования корректирующих свойств сверточных кодов, основанный на спектре активных расстояний, который позволил получить аналитические оценки распределения длин пакетов ошибок на выходе декодера Витерби, а также границы вероятности ошибки на блок.

Автором разработана новая модель передачи данных в системах неортогонального множественного доступа на базе векторного дизъюнктивного канала и получена оценка ее пропускной способности.

Автором был предложен ряд модификаций оригинальной криптосистемы Мак-Элиса, отличительной чертой которых является све-

дение задачи декодирования зашифрованного сообщения к задаче декодирования линейного кода по максимальному правдоподобию.

Личный вклад также отражен в достаточном числе публикаций в рецензируемых и индексируемых изданиях, в которых соискатель является основным автором.

Научная новизна

В работе предложены новые конструкции МПП-кодов. Данные кодовые конструкции основаны на подходе, предполагающем одновременное использование двух конструкций: матрицы малого размера, построенной алгебраическими и/или комбинаторными методами и матриц перестановок, которые используются для получения требуемой длины кода. В частности, в качестве алгебраических конструкций в данной работе рассматриваются системы троек Штейнера, а также коды с повторением. С помощью данного подхода удалось построить новые семейства высокоскоростных (при использовании систем троек Штейнера) и низкоскоростных (при использовании кода с повторением) кодов, которые допускают эффективное хранением а также показывают высокую эффективность (с точки зрения вероятности ошибки на блок в зависимости от отношения сигнал-шум) при их декодировании алгоритмом "распространения доверия". Кроме того, для регулярных МПП-кодов предложен новый подход оценки их экспоненты вероятности ошибки при декодировании по максимуму правдоподобия. Данный подход основан на использовании теоре-

мы Хаймана, используемой для поиска корней полинома численными методами.

Предложен новый математический аппарат для исследования сверточных кодов. Данный аппарат основан на впервые введенном понятии спектра активных расстояний. Показано, как использование данного аппарата позволяет оценить распределение длин пакетов ошибок на выходе декодера Витерби, а также теоретически оценить вероятность ошибки на блок при передаче информации через двоичный симметричный канал без проведения моделирования сверточных кодов.

Предложен новый алгоритм декодирования полярных кодов, основанный на списочном декодировании с инвертированием символов и быстром списочном декодировании некоторых подкодов полярного кода. Данный алгоритм основан на предложенном в диссертационной работе новом методе построения критического множества (множества информационных символов, инвертирование которых с наибольшей вероятностью приведет к правильному декодированию). Особо следует отметить, что данный метод построения критического множества пригоден как для векторного (с декодированием подкодов), так и для посимвольного декодирования и при этом в вычислениях используются только простейшие операции. Разработанный алгоритм декодирования не уступает классическому декодеру Тала-Варди, в то время как его пространственная и вычислительная

сложности существенно ниже.

Предложен новый метод организации некоординированного неортогонального множественного доступа, ориентированный на передачу коротких пакетов данных от множества устройств на базовую станцию. Для данного метода получены оценки на пропускную способность, а также показано, как известные конструкции перемеженных двоичных кодов и кодов Рида-Соломона могут быть использованы для разрешения коллизий, возникающих при передаче данных.

Разработаны новые конструкции криптографических систем с открытым ключом. Данные конструкции базируются на известной криптосистеме Мак-Элиса, основанной на трудной задаче декодирования линейного кода с произвольной структурой. Новым является подход к построению такого рода криптосистем — в отличие от существующих подходов, основная идея которых состоит в замене кода Гоппы на другую кодовую конструкцию, позволяющую компактно описать публичный ключ, предложенный в диссертационной работе подход предполагает изменение самой структуры открытого ключа. Основной целью данного изменения является усложнение атаки по информационным совокупностям, которая для кодовых криптосистем считается одной из наиболее эффективных. В диссертационной работе предложен ряд криптосистем, основанных на описанном выше подходе. Кроме того, сформулирована новая научная задача поиска кодовых конструкций, для которых возможно дать полино-

миальное описание множества исправимых ошибок веса, большего чем половина кодового расстояния. Кроме того, требуется наличие эффективного полиномиального алгоритма исправления ошибок из данного множества.

Все полученные результаты на момент их публикации являлись новыми.

Методология и методы исследования

Диссертационное исследование базируется на методологии системного анализа, а также на методах и теории проектирования телекоммуникационных систем, теориях математического моделирования, дискретной математики, математического анализа, теории информации, теории кодирования, теории вероятностей и математической статистики.

На защиту выносятся следующие основные результаты и положения:

1. Разработанный подход к построению МПП-кодов, который базируется на совместном использовании некоторой заданной алгебраической структуры (систем троек Штейнера, кодов с повторением) с детерминированными свойствами и матрицами перестановок позволяют получать ансамбли МПП-кодов с гарантированным минимальным расстоянием, что улучшает корректирующие характеристики кодов при малой вероятности ошибки.

2. Разработанный метод оценки экспоненты вероятности ошибки регулярных МПП-кодов, при их декодировании по максимуму правдоподобия позволяет строить границу снизу на вероятность ошибочного декодирования данного класса кодов, тем самым демонстрируя их "предельные" корректирующие свойства.

3. Разработанный математический аппарат исследования свойств сверточных кодов, основанный на спектре активных расстояний, позволяет без проведения имитационного моделирования оценивать вероятность ошибочного декодирования сверточных кодов в двоичном симметричном канале при любых входных вероятностях ошибки.

4. Разработанный алгоритм локального исправления стираний для сверточных кодов, который сводит задачу исправления стираний к решению системы линейных уравнений над конечным полем, реализует потенциальные корректирующие свойства сверточных кодов.

5. Быстрый алгоритм декодирования полярных кодов, основанный на построении критического множества инверсий информационных символов и быстром списочном декодировании некоторых специальных подкодов полярных кодов, имеет эффективность посимвольного списочного декодера, но имеет при

этом существенно меньшие пространственную и вычислительную сложности.

6. Предложенный метод организации некоординированного неортогонального множественного доступа в векторном дизъюнктивном канале позволяет некоординированно передавать короткие пакеты бит на базовую станцию с существенно большей пропускной способностью, чем слотированная ALOHA.

7. Методы защиты информации, основанные на базе системы Мак-Элиса, использующие модифицированные публичные ключи, затрудняющие их анализ с использованием декодирования по информационным совокупностям, обладают существенно меньшими длинами публичных ключей, чем в исходной системе Мак-Элиса.

Апробация работы

Основные результаты диссертации докладывались на следующих конференциях:

1. Международная конференция IEEE International Conference on Communications (2018, Канзас-сити, США). Тема доклада - "Signal-code construction based on interleaved reed-solomon codes for multiple access system over vector-disjunctive channel";

2. Международная конференция IEEE International Symposium

on Information Theory and its Applications (2018, Сингапур). Тема доклада - "Novel signal-code construction for multiple access system over vector-disjunctive channel";

3. Международная конференция IEEE International Symposium on Information Theory and its Applications (2020, онлайн). Тема доклада - "Theoretical Estimates of Burst Error Probability for Convolutional Codes";

4. Международная конференция IEEE International Symposium on Information Theory and its Applications (2020, онлайн). Тема доклада - "Upper and Lower Estimates of Frame Error Rate for Convolutional Codes";

5. Международная конференция 16th Canadian Workshop on Information Theory (2019, Гамильтон, Канада). Тема доклада - "On the performance of slotted vector-disjunctive channel";

6. Международная конференция IEEE International Conference on Computer, Information and Telecommunication Systems (2019, Пекин, КНР). Тема доклада - "On the Asymptotic Capacity of Slotted Multiple Access Channel";

7. Международная конференция 1st International Workshop on Code-Based Cryptography (2020, онлайн). Тема доклада - "A new code-based cryptosystem";

8. Международная конференция IEEE International Black Sea Conference on Communications and Networking (2018, Батуми. Грузия). Тема доклада - ”On the Maximal Achievable Rate for Signal-Code Construction Based on Interleaved Reed-Solomon Codes for Multiple Access System Over Vector-Disjunctive Channel”;

9. Международная конференция IEEE International Black Sea Conference on Communications and Networking (2019, Сочи, Россия). Тема доклада - ”Signal-Code Construction Based on Codes on Gilbert-Varshamov Bound for Multiple Access System over Vector-Disjunctive Channel”;

10. Международная конференция 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (2019, Дублин, Ирландия). Тема доклада - ”On the capacity estimation of a slotted multiuser communication channel”;

11. Международная конференция XVI International Symposium Problems of Redundancy in Information and Control Systems (2019, Москва, Россия). Тема доклада - ”On the capacity estimation of a slotted multiuser communication channel with noise”.

Кроме того, основные результаты диссертации были представлены на следующих семинарах:

1. Семинар по теории кодирования Института проблем передачи информации РАН (Москва, руководитель - Л.А. Бассалыго);

2. Семинар по теории кодирования и кодовой криптографии Сколковского института науки и технологий (Сколтех) (Москва, руководитель - Г.А. Кабатянский);

3. Семинар "Коды, исправляющие ошибки, и постквантовая криптография" Института Электроники и Математики им. А. Н. Тихонова, Национального Исследовательского Университета Высшая Школа Экономики (Москва, руководитель - Е.А. Крук).

Все предложенные алгоритмы и методы были реализованы программно, их поведение было исследовано методами имитационного моделирования, результаты которого были сопоставлены с ранее опубликованными.

Публикации

Работы, опубликованные автором в рецензируемых научных изданиях, входящих в международную систему цитирования Scopus:

1. Ivanov F., Miroshnik V., Krouk E. "Improved Generalized Successive Cancellation List Flip Decoder of Polar Codes with Fast Decoding of Special Nodes" // Journal of Communications and Networks. — 2021. — V. 23. — P. 417—432.

2. A new code-based cryptosystem / F. Ivanov, E. Krouk, G. Kabatansky, N. Rumenko // Code-Based Cryptography Workshop. — Springer. 2020. — P. 41—49.

3. Ivanov F., Kreshchuk A., Zyablov V. On the local erasure correction capacity of convolutional codes // 2018 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2018. — P. 296—300.

4. Ivanov F., Rybin P. Novel Signal-Code Construction for Multiple Access System over Vector-Disjunctive Channel // 2018 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2018. — C. 560—564.

5. Ivanov F., Rybin P. Signal-Code Construction Based on Interleaved Reed-Solomon Codes for Multiple Access System over Vector-Disjunctive Channel // 2018 IEEE International Conference on Communications Workshops (ICC Workshops). — IEEE. 2018. — C. 1—5.

6. Ivanov F., Rybin P. On the Asymptotic Capacity of Slotted Multiple Access Channel // 2019 International Conference on Computer, Information and Telecommunication Systems (CITS). — IEEE. 2019. — P. 1—5.

7. Ivanov F., Rybin P., Afanassiev V. On the Performance of Slotted Vector-Disjunctive Channel // 2019 16th Canadian Workshop on Information Theory (CWIT). — IEEE. 2019. — P. 1—5.

8. On the Capacity Estimation of a Slotted Multiuser Communication Channel / F. Ivanov, A. Kreschuk, V. Afanassiev // 2019 11th

International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). — IEEE. 2019. — P. 1—5.

9. On the Capacity Estimation of a Slotted Multiuser Communication Channel with Noise / F. Ivanov, A. Kreschuk, V. Afanassiev, P. Rybin // 2019 XVI International Symposium"Problems of Redundancy in Information and Control Systems"(REDUNDANCY). — IEEE. 2019. — P. 27—31.

10. Rybin P., Ivanov F. On estimation of the error exponent for finite length regular graph-based ldpc codes // Journal of Communications Technology and Electronics. — 2018. — V. 63, no. 12. — P. 1518—1523.

11. Smeshko A., Ivanov F. Signal-Code Construction Based on Codes on Gilbert-Varshamov Bound for Multiple Access System over Vector Disjunctive Channel // 2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom). — IEEE. 2019. — P. 1—3.

12. Smeshko A., Ivanov F., Zyablov V. Theoretical Estimates of Burst Error Probability for Convolutional Codes // 2020 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2020. — P. 136—140.

13. Smeshko A., Ivanov F., Zyablov V. Upper and Lower Estimates of Frame Error Rate for Convolutional Codes // 2020 International Symposium on Information Theory and Its Applications (ISITA). — IEEE. 2020. — P. 160—164.

14. Иванов Ф. И. Специальный класс квазициклических кодов с малой плотностью проверок, основанный на кодах с повторением и матрицах перестановок // Проблемы передачи информации. — 2017. — Т. 53, №3. — С. 229—241.

15. Иванов Ф. И., Зяблов В. В. Коды с малой плотностью проверок, основанные на системах троек Штейнера и матрицах перестановок. // Проблемы передачи информации. — 2013. — Т. 49, №4. — С. 333—347.

16. О новых задачах в асимметричной криптографии, основанной на помехоустойчивом кодировании. / Ф. И. Иванов, В. В. Зяблов, Е. А. Крук, В. Р. Сидоренко // Проблемы передачи информации. — 2022. — Т. 58, №2. — С. 92— 111.

17. Смешко А. А., Иванов Ф. И., Зяблов В. В. Теоретические и экспериментальные оценки сверху и снизу для эффективности сверточных кодов в двоичном симметричном канале. // Проблемы передачи информации. — 2022. — Т. 58, №2. — С. 24—40.

Публикации автора в других изданиях:

18. Оценка пропускной способности многопользовательского векторного дизъюнктивного канала для произвольных входных распределений / В.С. Дыренков, Н.М. Шевель, Ф.И. Иванов, А.А. Крещук // Информационные процессы. — 2020. — Т. 20, №2. — С. 133—141.

Общие выводы исследования

1. Предложенные конструкции МПП-кодов, базирующиеся на общем подходе - совместное использование некоторой заданной алгебраической структуры с детерминированными свойствами (в первую очередь дистантными и свойствами, связанными со структурой циклов в протографе Таннера) и матриц перестановок, используемыми для получения кодов требуемой длины, позволяют получить длинные коды с заданным минимальным расстоянием, что позволяет предположить достаточно низкий уровень "полки". При этом корректирующие свойства полученных кодов не уступают МПП-кодам, которые базируются на оптимизации методом эволюции плотностей или P-EXIT кривых. В то же время алгебраический подход, используемый при построении кодов, позволяет оптимизировать процедуры хранения проверочных матриц.

2. Предложенный в исследовании подход, позволяющий оценить

экспоненту вероятности ошибки регулярных МПП-кодов при декодировании этих кодов по максимуму правдоподобия, позволяет заключить, что несмотря на широкое практическое использование МПП-кодов в приложениях, их потенциальные корректрующие характеристики уступают произвольным двоичным кодам.

3. Предложенный в исследовании математический аппарат исследования корректирующих свойств сверточных кодов, основанный на спектре активных расстояний позволил получить аналитические оценки распределения длин пакетов ошибок на выходе декодера Витерби, а также границы вероятности ошибки на блок. На основе проведенного исследования можно сделать вывод о том, что предложенный в диссертационной работе аналитический метод оценки корректирующих свойств сверточных кодов позволяет получить точные значения вероятности ошибки на блок при малых входных вероятностях ошибки, для которых получение значений методами моделирования затруднительно. При этом предложенный метод имеет линейную сложность по длине кода и не зависит от вероятности ошибки в канале.

4. На основе анализа предложенного для полярных кодов нового критерия построения критического множества, используемого

в составе списочного декодера на основе инвертирования бит, был получен класс метрик, которые допускают как посимвольное, так и векторное вычисление. В частности было показано, как полученный метод построения критического множества может быть распространен на случай обобщенного списочного декодирования полярных кодов, где на каждом этапе вместо значения одного символа, принимается решение сразу по группе символов, образующих легко декодируемый подкод. Исследования разработанного на основе предложенной метрики обобщенного списочного декодера с инвертированием бит показали, что как символьный, так и обобщенный декодер, основанные на новой метрике, не уступают по своим корректирующим характеристикам лучшим на сегодняшний момент декодерам полярных кодов, обладая при этом существенно меньшей сложностью реализации.

5. Исследования новой модели передачи данных в системах неортогонального множественного доступа на базе векторного дизъюнктивного канала и оценки ее пропускной способности показали, что эффективность предложенной модели передачи существенно выше, чем у модели слотированной ALOHA.

6. Была сформулирована задача разрешения коллизий, которые возникают при передаче данных от группы пользователей на

базовую станцию в предложенной модели канала. Исследования свойств кодов, которые возможно применять для разрешения коллизий выявили преимущества использования перемеженных двоичных и недвоичных кодов по сравнению с классическими двоичными и недвоичными кодами без перемежения. В то же время корректирующие свойства предложенных кодовых конструкций существенно уступают потенциальным корреккктирующим свойствам кодов, которые лежат на границе пропускной способности векторного дизъюнктивного канала.

7. Был предложен ряд модификаций оригинальной криптосистемы Мак-Элиса, основной особенностью и отличительной чертой которых является то, что в отличие от классического подхода, где исходный код Гоппы заменяется на другой класс кодов, позволяющих дать компактное описание публичного ключа, в данной диссертационной работе предложено модифицировать саму структуру публичного и приватного ключей, что приводит к тому, что для извлечения информации о зашифрованном сообщении необходимо решать задачу декодирования в смежном классе кода, что иначе говоря равносильно поиску вектора ошибки не наименьшего возможного веса. Анализ свойств разработанных криптосистем показал, что для них неприменим наиболее эффективный метод атаки на классическую криптосистему Мак-Элиса — атака по информационным совокупностям.

Ввиду этого возможно существенно сократить длину публичного ключа при сохранении заданного уровня стойкости криптосистемы.

Цитированная литература

1. 5G: A tutorial overview of standards, trials, challenges, deployment, and practice / M. Shafi [и др.] // IEEE journal on selected areas in communications. — 2017. — Т. 35, № 6. — С. 1201—1221.

2. A survey on mobile WiMAX [wireless broadband access] / B. Li [и др.] // IEEE Communications magazine. — 2007. — Т. 45, № 12. — С. 70—75.

3. A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends / Z. Ding [и др.] // IEEE Journal on Selected Areas in Communications. — 2017. — Т. 35, № 10. — С. 2181—2195.

4. A technique to evaluate an exact formula for the bit error rate of convolutional codes in case of finite length words / F. Chiaraluce [и др.] // TENCON'97 Brisbane-Australia. Proceedings of IEEE TENCON'97. IEEE Region 10 Annual Conference. Speech and Image Technologies for Computing and Telecommunications (Cat. No. 97CH36162). Т. 1. — IEEE. 1997. — С. 113—116.

5. A tutorial on IEEE 802.11 ax high efficiency WLANs / E. Khorov [и др.] // IEEE Communications Surveys & Tutorials. — 2018. — Т. 21, № 1. — С. 197—216.

6. *Abramson N.* The ALOHA system: Another alternative for computer communications // Proceedings of the November 17-19, 1970, fall joint computer conference. — 1970. — С. 281—285.

7. *Afisiadis O.*, *Balatsoukas-Stimming A.*, *Burg A.* A low-complexity improved successive cancellation decoder for polar codes // 2014 48th Asilomar Conference on Signals, Systems and Computers. — IEEE. 2014. — С. 2116—2120.

8. *Ahamed M. M.*, *Faruque S.* 5G backhaul: requirements, challenges, and emerging technologies // Broadband Communications Networks: Recent Advances and Lessons from Practice. — 2018. — Т. 43.

9. *Akyildiz I. F.*, *Wang X.* A survey on wireless mesh networks // IEEE Communications magazine. — 2005. — Т. 43, № 9. — S23—S30.

10. *Alamdar-Yazdi A.*, *Kschischang F. R.* A simplified successive-cancellation decoder for polar codes // IEEE communications letters. — 2011. — Т. 15, № 12. — С. 1378—1380.

11. Algebraic cryptanalysis of McEliece variants with compact keys / J.-C. Faugere [и др.] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. — Springer. 2010. — С. 279—298.

12. An overview of the ATSC 3.0 physical layer specification / L. Fay [и др.] // IEEE Transactions on Broadcasting. — 2016. — Т. 62, № 1. — С. 159—171.

13. An overview of turbo codes and their applications / C. Berrou [и др.] // The European Conference on Wireless Technology, 2005. — IEEE. 2005. — С. 1—9.

14. Application of non-orthogonal multiple access in LTE and 5G networks / Z. Ding [и др.] // IEEE Communications Magazine. — 2017. — Т. 55, № 2. — С. 185—191.

15. *Arikan E.* Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels // IEEE Transactions on Information Theory. — 2009. — Т. 55, № 7. — С. 3051—3073.

16. *Barker E.*, *Dang Q.* Nist special publication 800-57 part 1, revision 4 // NIST, Tech. Rep. — 2016. — Т. 16.

17. *Berrou C.*, *Glavieux A.* Near optimum error correcting coding and decoding: Turbo-codes // IEEE Transactions on communications. — 1996. — Т. 44, № 10. — С. 1261—1271.

18. Bit-flip algorithm for successive cancellation list decoder of polar codes / F. Cheng [и др.] // IEEE Access. — 2019. — Т. 7. — С. 58346—58352.

19. *Bolton W.*, *Xiao Y.*, *Guizani M.* IEEE 802.20: mobile broadband wireless access // IEEE Wireless Communications. — 2007. — Т. 14, № 1. — С. 84—95.

20. *Buranapanichkit D.*, *Andreopoulos Y.* Distributed time-frequency division multiple access protocol for wireless sensor networks // IEEE wireless communications letters. — 2012. — Т. 1, № 5. — С. 440—443.

21. *Cover T.* An achievable rate region for the broadcast channel // IEEE Transactions on Information Theory. — 1975. — Т. 21, № 4. — С. 399—404.

22. *Dahlman E.*, *Parkvall S.*, *Skold J.* 4G: LTE/LTE-advanced for mobile broadband. — Academic press, 2013.

23. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding / A. Becker [и др.] // Annual international conference on the theory and applications of cryptographic techniques. — Springer. 2012. — С. 520—536.

24. *Dielissen J.*, *Hekstra A.*, *Berg V.* Low cost LDPC decoder for DVB-S2 // Proceedings of the Design Automation & Test in Europe Conference. Т. 2. — IEEE. 2006. — С. 1—6.

25. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithms // IEEE transactions on information theory. — 1985. — Т. 31, № 4. — С. 469—472.

26. *Elias P.* Coding for noisy channels // IRE Conv. Rec. — 1955. — Т. 3. — С. 37—46.

27. Fast polar decoders: Algorithm and implementation / G. Sarkis [и др.] // IEEE Journal on Selected Areas in Communications. — 2014. — Т. 32, № 5. — С. 946—957.

28. Finite-length analysis of low-density parity-check codes on the binary erasure channel / C. Di [и др.] // IEEE Transactions on Information theory. — 2002. — Т. 48, № 6. — С. 1570—1579.

29. *Gallager R.* Low-density parity-check codes // IRE Transactions on information theory. — 1962. — Т. 8, № 1. — С. 21—28.

30. *Gamage H.*, *Rajatheva N.*, *Latva-Aho M.* Channel coding for enhanced mobile broadband communication in 5G systems // 2017 European conference on networks and communications (EuCNC). — IEEE. 2017. — С. 1—6.

31. *Giard P.*, *Burg A.* Fast-SSC-flip decoding of polar codes // 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). — IEEE. 2018. — С. 73—77.

32. *Hanif M.*, *Ardakani M.* Fast successive-cancellation decoding of polar codes: Identification and decoding of new nodes // IEEE Communications Letters. — 2017. — Т. 21, № 11. — С. 2360—2363.

33. *Hara S.*, *Prasad R.* Overview of multicarrier CDMA // IEEE communications Magazine. — 1997. — Т. 35, № 12. — С. 126—133.

34. *Hashemi S. A.*, *Condo C.*, *Gross W. J.* Simplified successive-cancellation list decoding of polar codes // 2016 IEEE International Symposium on Information Theory (ISIT). — IEEE. 2016. — С. 815—819.

35. *Herro M.*, *Hu L.*, *Nowack J.* Bit error probability calculations for convolutional codes with short constraint lengths on very noisy channels // IEEE Transactions on Communications. — 1988. — Т. 36, № 7. — С. 885—888. — DOI: 10.1109/26.2819.

36. Interleave division multiple-access / L. Ping [и др.] // IEEE transactions on wireless communications. — 2006. — Т. 5, № 4. — С. 938—947.

37. *Kabatianskii G.*, *Krouk E.*, *Smeets B.* A digital signature scheme based on random error-correcting codes // IMA International Conference on Cryptography and Coding. — Springer. 1997. — С. 161—167.

38. *Kocher P. C.* Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Annual International Cryptology Conference. — Springer. 1996. — С. 104—113.

39. *Li S.*, *Da Xu L.*, *Zhao S.* 5G Internet of Things: A survey // Journal of Industrial Information Integration. — 2018. — Т. 10. — С. 1—9.

40. Low-complexity LDPC decoder for 5G URLLC / J.-C. Liu [и др.] // 2018 IEEE Asia Pacific Conference on Postgraduate Research in Microelectronics and Electronics (PrimeAsia). — IEEE. 2018. — С. 43—46.

41. Low-rate PBRL-LDPC codes for URLLC in 5G / X. Wu [и др.] // IEEE Wireless Communications Letters. — 2018. — Т. 7, № 5. — С. 800—803.

42. *MacKay D. J.* Good error-correcting codes based on very sparse matrices // IEEE transactions on Information Theory. — 1999. — Т. 45, № 2. — С. 399—431.

43. *May A.*, *Meurer A.*, *Thomae E.* Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$ // International Conference on the Theory and Application of Cryptology and Information Security. — Springer. 2011. — С. 107—124.

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

45. *Myung H. G.*, *Lim J.*, *Goodman D. J.* Single carrier FDMA for uplink wireless transmission // IEEE Vehicular Technology Magazine. — 2006. — Т. 1, № 3. — С. 30—38.

46. *Nelson R.*, *Kleinrock L.* Spatial TDMA: A collision-free multihop channel access protocol // IEEE Transactions on communications. — 1985. — Т. 33, № 9. — С. 934—944.

47. *Niu K.*, *Chen K.* CRC-aided decoding of polar codes // IEEE Communications Letters. — 2012. — Т. 16, № 10. — С. 1668—1671.

48. *Noor-A-Rahim M.*, *Nguyen K. D.*, *Lechner G.* Finite length analysis of LDPC codes // 2014 IEEE Wireless Communications and Networking Conference (WCNC). — IEEE. 2014. — С. 206—211.

49. On the performance of polar codes for 5G eMBB control channel / S. A. Hashemi [и др.] // 2017 51st Asilomar Conference on Signals, Systems, and Computers. — IEEE. 2017. — С. 1764—1768.

50. Optimal decoding of linear codes for minimizing symbol error rate (corresp.) / L. Bahl [и др.] // IEEE Transactions on information theory. — 1974. — Т. 20, № 2. — С. 284—287.

51. Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges / S. R. Islam [и др.] // IEEE Communications Surveys & Tutorials. — 2016. — Т. 19, № 2. — С. 721—742.

52. Protograph-based raptor-like LDPC codes / T.-Y. Chen [и др.] // IEEE Transactions on Communications. — 2015. — Т. 63, № 5. — С. 1522—1532.

53. Reducing key length of the McEliece cryptosystem / T. P. Berger [и др.] // International Conference on Cryptology in Africa. — Springer. 2009. — С. 77—97.

54. *Richardson T.*, *Urbanke R.* Finite-length density evolution and the distribution of the number of iterations for the binary erasure channel // unpublished.[Online]. Available: http://lthcwww. epfl. ch/RiU02. ps. — 2003.

55. *Rimoldi B.*, *Urbanke R.* A rate-splitting approach to the Gaussian multiple-access channel // IEEE Transactions on Information Theory. — 1996. — Т. 42, № 2. — С. 364—375.

56. *Rivest R. L.*, *Shamir A.*, *Adleman L.* A method for obtaining digital signatures and public-key cryptosystems // Communications of the ACM. — 1978. — Т. 21, № 2. — С. 120—126.

57. *Tal I.*, *Vardy A.* List decoding of polar codes // Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on. — IEEE. 2011. — С. 1—5.

58. *Tsatsaragkos I.*, *Paliouras V.* A reconfigurable LDPC decoder optimized for 802.11 n/ac applications // IEEE Transactions on Very Large Scale Integration (VLSI) Systems. — 2017. — Т. 26, № 1. — С. 182—195.

59. Use cases and scenarios of 5G integrated satellite-terrestrial networks for enhanced mobile broadband: The SaT5G approach / K. Liolis [и др.] // International Journal of Satellite Communications and Networking. — 2019. — Т. 37, № 2. — С. 91—112.

60. *Véron P.* Code based cryptography and steganography // International Conference on Algebraic Informatics. — Springer. 2013. — С. 9—46.

61. *Viterbi A.* Error bounds for convolutional codes and an asymptotically optimum decoding algorithm // IEEE transactions on Information Theory. — 1967. — Т. 13, № 2. — С. 260—269.

62. *Yoshikawa H.* Theoretical analysis of bit error probability for punctured convolutional codes // 2012 International Symposium on Information Theory and its Applications. — 2012. — С. 658—661.

63. *Yuan Y.*, *Zhao X.* 5G: Vision, scenarios and enabling technologies // ZTE communications. — 2015. — Т. 13, № 1. — С. 3—10.

64. *Zhang J.*, *Orlitsky A.* Finite-length analysis of LDPC codes with large left degrees // Proceedings IEEE International Symposium on Information Theory, — IEEE. 2002. — С. 3.