МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА

На правах рукописи

Высоцкая Виктория Владимировна

Анализ постквантовых схем электронной подписи, построенных на кодах, исправляющих ошибки

2.3.6. Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата физико-математических наук

Москва — 2025

Диссертация подготовлена на кафедре информационной безопасности факультета вычислительной математики и кибернетики МГУ имени М. В. Ломоносова.

Научный руководитель — *Чижов Иван Владимирович*,
кандидат физико-математических наук

Официальные оппоненты — *Вороненко Андрей Анатольевич*,
доктор физико-математических наук, профессор, факультет вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», профессор кафедры математической кибернетики

— *Кабатянский Григорий Анатольевич*,
доктор физико-математических наук, Сколковский институт науки и технологий, вице-президент по науке и академическому сотрудничеству

— *Гашков Сергей Борисович*,
доктор физико-математических наук, профессор, механико-математический факультет ФГБОУ ВО «Московский государственный университет имени М.В. Ломоносова», профессор кафедры дискретной математики

Защита состоится «26» ноября 2025 г. в 16 часов 45 минут на заседании диссертационного совета МГУ.012.3 Московского государственного университета имени М.В. Ломоносова по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, механико-математический факультет, аудитория 1408.

E-mail: vasenin@msu.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на портале:
https://dissovet.msu.ru/dissertation/3544.

Автореферат разослан « » 2025 г.

Ученый секретарь
диссертационного совета,
кандидат физико-математических наук А.В. Галатенко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Диссертационная работа посвящена решению задачи построения электронных подписей на основе кодов, исправляющих ошибки. Электронные подписи представляют собой тройку алгоритмов: генерации ключей, генерации подписи и проверки подписи. Они решают задачи контроля целостности, проверки авторства и неотказуемости от него.

Актуальность. Стойкость стандартизованных криптографических алгоритмов, используемых по всему миру, основана на сложности нескольких задач из теории чисел. Обычно это задачи дискретного логарифмирования или факторизации. Однако в 1994 году П. Шор показал[1], что квантовые компьютеры могут взломать все схемы, построенные таким образом. В 2001 году алгоритм Шора был реализован[2] на квантовом компьютере с 7 кубитами. С тех пор стали разрабатываться все более и более мощные квантовые компьютеры, что представляет реальную угрозу современной криптографии с открытым ключом.

Существует несколько областей, на которых могут основываться постквантовые криптографические схемы. Примерами таких областей являются целочисленные решетки, коды, исправляющие ошибки, хэш-функциии, многомерные квадратичные системы, а также симметричное шифрование и шифрование на основе изогений эллиптических кривых. Тем не менее построенные схемы требуют исследования стойкости, в том числе к атакам с использованием квантовых компьютеров.

Сложные задачи, на которых основаны постквантовые алгоритмы, изучены хуже по сравнению с теми, что лежат в основе классических криптосхем. Поэтому вероятность успешной атаки на новые схемы выше. Однако из существующих атак на квантовых компьютерах на такие схемы лучшим является алгоритм Гровера[3], дающий корневую оценку сложности. Поэтому они внушают больше доверия, нежели схемы, подверженные полиномиальным атакам Шора. Но при этом некоторые задачи, считающиеся постквантовыми, оказываются нестойкими даже к атакам на классических компьютерах. Так, например, базовая задача SIDH на изогениях, которая некоторое время считалась сложной, была атакована в работе 2022 года[4]. Это, в свою очередь, свидетельствует об отсутствии стойкости схем, доказательства безопасности которых сводились к сложности этой задачи. Так что в настоящее время остро стоит задача поиска лучшего подхода.

Коды, исправляющие ошибки, как математический объект имеют историю длиною более 70-ти лет. Однако с точки зрения криптографии они стали рассматриваться только спустя десятилетия, после предложения в 1978 году Ро-

[1] P. W. Shor. «Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer». В: *SIAM Journal on Computing* 26.5 (1997), с. 1484—1509.

[2] L. M. K. Vandersypen и др. «Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance». В: *Nature* 414 (2001), с. 883—887.

[3] L. K. Grover. «A fast quantum mechanical algorithm for database search». В: *Proc. 28th Annual ACM Symposium on the Theory of Computation* (1996), с. 212—219.

[4] W. Castryck и T. Decru. «An efficient key recovery attack on sidh (preliminary version)». В: *IACR Cryptology ePrint Archive* (2022), с. 15.

бертом Мак-Элисом своей криптосистемы[5]. Но даже после этого долгое время не было попыток стандартизовать кодовые схемы. Наконец в 2016 году Национальный Институт Стандартов и Технологий США (NIST) объявил[6] открытый конкурс на новый постквантовый стандарт США. В этом конкурсе участвовали алгоритмы шифрования с открытым ключом, схемы цифровых подписей и схемы распределения ключей, среди которых были и варианты, построенные на кодах.

Результаты получились неоднозначными. Большое число поданных схем оказались подвержены атакам на классическом вычислителе. Среди них были и все 3 схемы электронной подписи на кодах, исправляющих ошибки[7]: pqsigRM[8], RaCoSS-R[9], RankSgn[10]. Первая была позже доработана[11], но все равно оказалась уязвимой. Другие схемы, которые остаются стойкими, имеют неоптимальные эксплуатационные параметры и потенциально могут быть атакованы в будущем.

Поэтому, несмотря на объявление победителей, параллельно был запущен еще один дополнительный конкурс, нацеленный исключительно на алгоритмы электронной подписи. Уже к июлю 2023 года был опубликован список из 40 новых претендентов. Схем на кодах, исправляющих ошибки, на первом раунде было 6: CROSS[12], Enhanced pqsigRM[13], FuLeeca[14], LESS[15], MEDS[16] и Wave[17]. Схемы CROSS и LESS прошли во 2 раунд и имеют возможность в дальнейшем быть стандартизованными.

Параллельно с конкурсом NIST в России также начался процесс выбора постквантовой схемы электронной подписи. Схемы на основе кодов были выбраны Техническим комитетом по стандартизации «Криптографические и защитные механизмы»(ТК 26)[18] как одно из направлений разработки проектов

---

[5] R. J. McEliece. «A public-key cryptosystem based on algebraic coding theory». В: *The Deep Space Network Progress Report* 42.44 (1978), с. 114—116.

[6] NIST. *Calls for proposals*. 2017. URL: `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`.

[7] D. Moody. «Status report on the first round of the NIST post-quantum cryptography standardization process». В: *NIST report* (2019), с. 1—27.

[8] W. Lee и др. «Post quantum signature scheme based on modified Reed-Muller code pqsigRM». В: *NIST proposal* (2017), с. 1—35.

[9] P. S. Roy и др. «Supporting documentation of RaCoSS (Random Code-based Signature Scheme)». В: *NIST proposal* (2017), с. 1—26.

[10] N. Aragon и др. «Ranksign — a signature proposal for the NIST's call». В: *NIST proposal* (2017), с. 1—22.

[11] Y.-W. Lee и др. «A modified pqsigRM: RM code-based signature scheme». В: *IACR Cryptology ePrint Archive* (2018), с. 18.

[12] M. Baldi и др. «Codes and Restricted Objects Signature Scheme (CROSS)». В: *NIST proposal* (2023), с. 1—59.

[13] J. Cho и др. *Enhanced pqsigRM: code-based digital signature scheme with short signature and fast verification for post-quantum cryptography*. Тех. отч. 2023, с. 1—28.

[14] S. Ritterhoff и др. «FuLeeca». В: *NIST proposal* (2023), с. 1—29.

[15] M. Baldi и др. «LESS: Linear Equivalence Signature Scheme». В: *NIST proposal* (2023), с. 1—37.

[16] T. Chou и др. «Matrix Equivalence Digital Signature (MEDS)». В: *NIST proposal* (2023), с. 1—29.

[17] G. Banegas и др. «Wave». В: *NIST proposal* (2017), с. 1—51.

[18] *Технический комитет 26 по стандартизации «Криптографическая защита информации»*. URL: `https://tc26.ru`.

российских национальных стандартов постквантовых криптографических алгоритмов. Диссертационная работа мотивирована задачами, которые возникли в процессе работ, проводимых в рамках ТК 26.

Помимо России, процессы по выбору и стандартизации постквантовых алгоритмов идут и в других странах. Так, например, в 2021–2025 годах в Южной Корее проводился конкурс KpqC[19]. Аналогичные инициативы реализуются и в рамках международных организаций по стандартизации, таких как ISO[20] и IETF[21].

Исторически синтез электронной подписи на основе кодов продвигался не очень удачно. На протяжении длительного времени атаки на все предложенные схемы подписей строились столь быстро, что возникло опасение, что такие схемы вообще невозможно создать[22]. Одним из первых успешных вариантов можно назвать схему KKS[23], которая была предложена Г. Кабатянским, Е. Круком и Б. Смитом в 1997 году. Однако, согласно дальнейшим исследованиям[24], схема является стойкой только при одноразовом использовании.

Прорывом стало предложение Н. Куртуа, М. Финиаша и Н. Сендриера инвертировать порядок алгоритмов в схеме шифрованя, то есть использовать алгоритм расшифрования в качестве алгоритма генерации подписи и шифрования для ее проверки. Эта идея была представлена в 2001 году и в дальнейшем получила название CFS[25]. Позже Л. Далло предложил доказуемо стойкую версию этой подписи, известную как mCFS[26]. В диссертации эти схемы отождествлены под названием CFS.

Классическими примерами схем шифрования на основе кодов являются криптосистемы Р. Мак-Элиса[27] и Х. Нидеррайтера[28]. В первом случае код задан своей порождающей, а во втором — проверочной матрицей. Соответственно, стойкость схем первого типа сводится к сложности решения задачи декодирования, а второго типа — к сложности задачи синдромного декодирования. Эти

---

[19] D. J. Bernstein и др. «Report on evaluation of KpqC Round-2 candidates». В: *IACR Cryptology ePrint Archive* December (2024).

[20] PQCRYPTO. *Post-quantum cryptography for long-term*. URL: `https://web.archive.org/web/20250210182614/https://www.iso.org/organization/5984715.html` (дата обр. 10.02.2025).

[21] IETF. *Post-Quantum Cryptography*. URL: `https://web.archive.org/web/20250422202535/https://wiki.ietf.org/group/sec/PQCAgility` (дата обр. 22.04.2025).

[22] J. Stern. «Can one design a signature scheme based on error-correcting codes?» В: *Lecture Notes in Computer Science* 917 (1995), с. 424—426.

[23] G. Kabatianskii, E. Krouk и B. Smeets. «A digital signature scheme based on random error-correcting codes». В: *Crytography and Coding. Cryptography and Coding 1997. Lecture Notes in Computer Science* 1355 (1997), с. 161—167.

[24] P.-L. Cayrel, A. Otmani и D. Vergnaud. «On Kabatianskii–Krouk–Smeets signatures». В: *Arithmetic of Finite Fields. WAIFI 2007. Lecture Notes in Computer Science*. Т. 4547. 2007, с. 237—252.

[25] N. Courtois, M. Finiasz и N. Sendrier. «How to achieve a McEliece-based digital signature scheme». В: *Advances in Cryptology — ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science*. Т. 2248. 2001, с. 157—174.

[26] L. Dallot. «Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme». В: *Research in Cryptology. WEWoRC 2007. Lecture Notes in Computer Science*. Т. 4945. 2008, с. 65—77.

[27] R. J. McEliece. «A public-key cryptosystem based on algebraic coding theory». В: *The Deep Space Network Progress Report* 42.44 (1978), с. 114—116.

[28] H. Niederreiter. «Knapsack-type cryptosystems and algebraic coding theory». В: *Problems of Control and Information Theory* 15.2 (1986), с. 159—166.

задачи эквивалентны по сложности, таким образом схемы на них эквивалентны по уровню стойкости.

Задачи декодирования и синдромного декодирования для кодов общего вида являются NP-полными как задачи разрешимости и NP-трудными как задачи поиска[29,30]. Это гарантирует стойкость криптографических схем, построенных на таких кодах. Также пока остаются стойкими схемы, построенные с использованием кодов, которые предложил В. Д. Гоппа[31].

Однако в общем случае криптосистемы на основе выделенных классов линейных кодов могут быть подвержены атакам, поскольку замена кода приводит к модификации постановки задачи. Поэтому при синтезе схем на кодах, исправляющих ошибки, обычно выбирают базовый код с эффективным алгоритмом декодирования, но маскируют его под код общего вида, все известные алгоритмы для которого экспоненциальны. Маскировка может осуществляться при помощи умножения на одну (криптосистема Богданова–Ли[32]) или две матрицы (криптосистемы Мак-Элиса[33] и Нидеррайтера[34]), которые становятся частью секретного ключа криптосистемы.

Тем не менее, известны случаи, когда секретный ключ такого вида (или эквивалентный ему) удавалось восстановить по открытым данным. Так криптосистема Мак-Элиса на кодах Рида–Маллера была атакована в работах Л. Миндера, А. Шокроллахи[35] и М. Бородина, И. Чижова[36]. Построены атаки на эту же криптосистему и на кодах Рида–Соломона[37,38]. Проблемы со стойкостью оказались и у вариантов на основе других классов кодов[39,40,41,42].

Одним из подходов к дополнительному сокрытию структуры кода с сохранением его эффективности является переход к некоторому его подкоду. При

---

[29] E. R. Berlekamp, R. J. McEliece и H. C. A. van Tilborg. «On the inherent intractability of certain coding problems». В: *IEEE Transactions on Information Theory* 24.3 (1978), с. 384—386.

[30] S. Barg. «Some new NP-complete coding problems». В: *Probl. Peredachi Inf.* 30.3 (1994), с. 23—28.

[31] В. Д. Гоппа. «Новый класс линейных корректирующих кодов». В: *Пробл. передачи информ.* 6.3 (1970), с. 24—30.

[32] A. Bogdanov и C. H. Lee. «Homomorphic encryption from codes». В: *arXiv* (2011), с. 18.

[33] R. J. McEliece. «A public-key cryptosystem based on algebraic coding theory». В: *The Deep Space Network Progress Report* 42.44 (1978), с. 114—116.

[34] H. Niederreiter. «Knapsack-type cryptosystems and algebraic coding theory». В: *Problems of Control and Information Theory* 15.2 (1986), с. 159—166.

[35] L. Minder и A. Shokrollahi. «Cryptanalysis of the Sidelnikov cryptosystem». В: *LNCS (Advances in Cryptology — EUROCRYPT 2007)* 4515 (2007), с. 347—360.

[36] М. А. Бородин и И. В. Чижов. «Эффективная атака на криптосистему Мак-Элиса, построенную на основе кодов Рида–Маллера». В: *Дискретная Математика* 26.1 (2014), с. 10—20.

[37] В. М. Сидельников и С. О. Шестаков. «О системе шифрования, построенной на основе обобщенных кодов Рида–Соломона». В: *Дискрет. матем.* 4.3 (1992), с. 57—63.

[38] A. Couvreur и др. «Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes». В: *Designs, Codes and Cryptography* 73.2 (2014), с. 641—666.

[39] A. Couvreur, I. Márquez-Corbella и R. Pellikaan. «Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes». В: *Coding Theory Appl.ications. CIM Ser. Math. Sci.* 3 (2015), с. 133—140.

[40] И. В. Чижов и М. А. Бородин. «Классификация произведений Адамара подкодов коразмерности 1 кодов Рида–Маллера». В: *Дискретная Математика* 32.1 (2020), с. 115—134.

[41] И. Чижов. «Полная классификация произведений Адамара подкодов коразмерности 1 кодов Рида–Маллера». В: *Вестн. Моск. Ун-та* 15.1 (2024), с. 57—70.

[42] A. Couvreur, A. Otmani и J.-P. Tillich. «Polynomial time attack on wild McEliece over quadratic extensions». В: *IEEE Transactions on Information Theory* 63.1 (2017), с. 404—427.

этом стоит учитывать, что многие предложенные системы на основе подкодов также оказались уязвимыми. Так, в своих работах К. Вишебринк построил[43,44] эффективные атаки на некоторые особые случаи криптосистемы Бергера–Луадро[45], основанной на подкодах кодов Рида–Соломона. Криптосистема Мак-Элиса, построенная на подкодах алгебраических геометрических кодов, была атакована в работе 2015 года[46]. А позже И. Чижову и М. Бородину удалось[47] редуцировать стойкость криптосистемы на подкодах кодов Рида–Маллера коразмерности один до стойкости схемы на полных кодах, где под коразмерностью понимается количество векторов, отсутствующих в базисе кода. Тем не менее аналогичных результатов для подкодов кодов Рида–Маллера больших коразмерностей получено не было.

Еще одним способом усиления стойкости схемы с сохранением структуры кодов является вариант, предложенный в 1994 году В. Сидельниковым[48] для кодов Рида–Маллера. Криптосистемы такого типа используют не одну, а несколько копий кода. Матрицы таких кодов объединены по столбцам. Несмотря на то, что этот подход позволил избежать прямого переноса атак, направленных на вариант с одной копией кода Рида–Маллера, в работе И. Чижова, С. Конюхова и А. Давлетшиной был предложен[49] специальный алгоритм восстановления секретного ключа и для модифицированной схемы. Работы А. Отмани, Э. Калачи[50] и И. Чижова, Е. Поповой[51] решают эту же задачу для варианта криптосистемы, в которой используются одновременно код Рида–Маллера и линейный код общего вида. Приведенные атаки работают при выполнении типичного условия, которое, согласно работе И. Чижова[52], будет выполнено для случайного кода с вероятностью близкой к 1. Однако полностью вопрос применимости конструкции Сидельникова не закрыт, поскольку она не была доисследована для других классов кодов, для которых могут найтись потенциально стойкие коды

[43] C. Wieschebrink. «An attack on a modified niederreiter encryption scheme». В: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 3958 (2006), с. 14—26.

[44] C. Wieschebrink. «Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes». В: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 6061 (2010), с. 61—72.

[45] T. P. Berger и P. Loidreau. «How to mask the structure of codes for a cryptographic use». В: *Designs, Codes, and Cryptography* 35.1 (2005), с. 63—79.

[46] A. Couvreur, I. Márquez-Corbella и R. Pellikaan. «Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes». В: *Coding Theory Appl.ications. CIM Ser. Math. Sci.* 3 (2015), с. 133—140.

[47] И. В. Чижов и М. А. Бородин. «Классификация произведений Адамара подкодов коразмерности 1 кодов Рида–Маллера». В: *Дискретная Математика* 32.1 (2020), с. 115—134.

[48] В. М. Сидельников. «Открытое шифрование на основе двоичных кодов Рида–Маллера». В: *Дискрет. матем.* 6.2 (1994), с. 3—20.

[49] И. В. Чижов, С. А. Конюхов и А. М. Давлетшина. «Эффективная структурная атака на криптосистему Мак-Элиса–Сидельникова». В: *International Journal of Open Information Technologies* 8.7 (2020), с. 1—10.

[50] A. Otmani и H. T. Kalachi. «Square code attack on a modified Sidelnikov cryptosystem». В: *Lecture Notes in Computer Science* 9084 (2015), с. 173—183.

[51] И. В. Чижов и Е. А. Попова. «Структурная атака на криптосистемы типа Мак-Элиса–Сидельникова, построенной на основе комбинирования случайных кодов с кодами Рида–Маллера». В: *International Journal of Open Information Technologies* 8.6 (2020), с. 24—33.

[52] И. В. Чижов. «Квадрат Адамара последовательно соединенных линейных кодов». В: *Дискретная математика* 3 (2023), с. 100—124.

специального вида.

Выбор класса кодов может существенно улучшить эффективность схемы. Так квазициклические коды позволяют критически сократить размер открытого ключа, поскольку для хранения каждой циклической подматрицы достаточно хранения одной ее строки. Такой подход был отражен в рамках конкурса NIST в схемах QC-MDPC[53] и LEDAcrypt[54], предлагающих схемы шифрования и механизм инкапсуляции ключа на кодах со средней и малой плотностью проверок на четность (QC-MDPC и QC-LDPC кодах, соответственно). Первая схема в первый же год подверглась атаке по времени, восстанавливающей секретный ключ за $O(2^{28})$ битовых операций вместо $O(2^{256})$ заявленных. Вторая работа дошла до второго раунда конкурса, но далее была отклонена из-за появления работы[55], обнаружившей большой класс слабых ключей, уязвимых к раскрытию. Еще две схемы, эксплуатировавшие квазициклическую структуру кодов, BIKE[56] и HQC[57], дошли до 4 раунда конкурса, а модифицированная версия последней[58] в 2025 году стала победителем.

В 2020 году на конференции CTCrypt'20 было высказано предложение[59] использовать QC-LDPC коды для построения электронной подписи. Для решения этой задачи авторы работы подставили алгоритм генерации квазициклических ключей из схемы LEDAcrypt[60] в классическую схему подписи CFS. Однако изменение параметров для адаптации схемы шифрования под схему подписи привело к росту параметров, для которых выросло время внутреннего алгоритма генерации вспомогательной невырожденной квазициклической матрицы. Оптимизация этого алгоритма могла бы поспособствовать повышению эффективности всей схемы подписи.

Другой подход к построению схемы электронной подписи на кодах, исправляющих ошибки, заключается в применении преобразования Фиата–Шамира[61] к некоторому протоколу идентификации. В качестве такого протокола можно использовать схемы Я. Штерна[62], А. Джаина и др.[63], CVE[64] и прочие. Такой

---

[53] E. Eaton и A. Parent. *QC-MDPC KEM: a key encapsulation mechanism based on the QC-MDPC McEliece encryption scheme*. Тех. отч. 2017, с. 1—51.

[54] M. Baldi и др. «LEDAkem: a post-quantum key encapsulation mechanism based on QC-LDPC codes». В: *NIST proposal* (2017), с. 1—22.

[55] D. Apon и др. «Cryptanalysis of LEDAcrypt». В: *Advances in Cryptology – CRYPTO 2020. CRYPTO 2020. Lecture Notes in Computer Science* 12172 (2020), с. 389—418.

[56] N. Aragon и др. «Bike: Bit Flipping Key Encapsulation». В: *NIST proposal* (2017), с. 1—74.

[57] J.-C. Deneuville и др. «Hamming Quasi-Cyclic (HQC)». В: *NIST proposal* (2017), с. 1—62.

[58] C. A. Melchor и др. «Hamming Quasi-Cyclic (HQC)». В: *NIST proposal* (2019), с. 1—47.

[59] E. D. Fiallo. «A digital signature scheme mCFSQC-LDPC based on QC-LDPC codes». В: *Mat. Vopr. Kriptogr.* 12.4 (2021), с. 99—113.

[60] M. Baldi и др. «LEDAcrypt: Low-dEnsity parity-check coDe-bAsed cryptographic systems». В: *NIST proposal* (2019), с. 1—83.

[61] A. Fiat и A. Shamir. «How to prove yourself: practical solutions to identification and signature problems». В: *Advances in Cryptology — CRYPTO' 86. CRYPTO 1986. Lecture Notes in Computer Science*. Т. 263. 1987, с. 186—194.

[62] J. Stern. «A new identification scheme based on syndrome decoding». В: *CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science*. Т. 773. 1994, с. 13—21.

[63] A. Jain и др. «Commitments and efficient zero-knowledge proofs from learning parity with noise». В: *Lecture Notes in Computer Science* 7658 LNCS (2012), с. 663—680.

[64] P.-L. Cayrel, P. Véron и S. M. el Yousfi Alaoui. «A zero-knowledge identification scheme based on the

подход позволяет отказаться от использовать алгоритма декодирования, что дает возможность использования в схеме произвольный линейный код, а не ограничиваться узкими классами кодов с эффективными алгоритмами декодирования.

Несмотря на то, что подпись на основе схемы идентификации Штерна неоднократно упоминалась в литературе, ее полное описание до сих пор не было представлено. Например, в обзоре Р. Овербека и Н. Сендриера[65] лишь отмечена возможность построения такой подписи, но сам алгоритм не приведен. В одной работе 2019 года[66] схема сформулирована с ошибкой, что приводит к значительному снижению уровня стойкости по сравнению с ожидаемым значением. Корректное, но краткое описание схемы можно найти в работе С. Эль Юсфи Алауи и др.[67]

Обоснование стойкости такой схемы подписи упоминается в работе Д. Пуаншеваля и Я. Штерна[68]. В этой статье представлена так называемая лемма разветвления (Forking lemma). Авторы утверждают ее применимость к доказательству стойкости подписи Штерна, однако этот факт не был доказан ни в данной работе, ни в последующих. При этом наличие доказательства стойкости позволило бы существенно продвинуть исследования в области построения схем электронной подписи на основе кодов, исправляющих ошибки. Это связано с тем, что стойкость такой электронной подписи не только исключает возможность структурных атак, но и строго сводится к исходной NP-трудной задаче. В работе автором предложено такое доказательство.

Цели и задачи диссертационной работы: анализ методов построения схем электронной подписи на основе кодов, исправляющих ошибки, путем исследования их структурных свойств, а также рассмотрение подходов, не зависящих от конкретного класса кодов.

Для достижения поставленной цели были решены следующие задачи:

1. исследовать стойкость электронной подписи CFS на подкодах кодов Рида–Маллера;
2. исследовать возможность эффективного построения электронной подписи CFS на основе квазициклических кодов;
3. исследовать стойкость электронной подписи CFS на основе конструкции Сидельникова;
4. разработать новую схемы электронной подписи на основе кодов, исправляющих ошибки, стойкость которой не зависела бы от структуры используемого кода.

---

q-ary syndrome decoding problem». В: *Lecture Notes in Computer Science* 6544 LNCS (2011), с. 171—186.

[65] R. Overbeck и N. Sendrier. *Code-based cryptography.* 2009.

[66] P. S. Roy, K. Morozov и K. Fukushima. «Evaluation of code-based signature schemes». В: *IACR Cryptology ePrint Archive* (2019), с. 22.

[67] S. M. el Yousfi Alaoui и др. «Code-based identification and signature schemes in software». В: *Lecture Notes in Computer Science* 8128 LNCS (2013), с. 122—136.

[68] D. Pointcheval и J. Stern. «Security proofs for signature schemes». В: *Advances in Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science* 1070 (1996), с. 387—398.

Положения, выносимые на защиту:

1. Метод описания структурных свойств подкодов кода Рида–Маллера, схема подписи CFS на которых является стойкой к известному типу атак. Способы построения таких подкодов и метод оценки их доли.

2. Два эффективных алгоритма построения невырожденных квазициклических матриц, необходимых для эффективной реализации схемы подписи CFS на квазициклических кодах.

3. Метод получения нижней оценки мощности множества открытых ключей схемы подписи CFS, построенной на основе конструкции Сидельникова. Описание структуры множества секретных ключей на кодах общего вида и обобщенных кодах Рида–Соломона, схема подписи на которых подвержена атакам, разделяющим копии кода. Метод построения секретных ключей подписи CFS с использованием обобщенных кодов Рида–Соломона, позволяющий избежать известных атак.

4. Схема электронной подписи, стойкость которой не зависит от сложности задач на известном классе кодов. Обоснование стойкости построенной подписи.

Научная новизна. В диссертации получены следующие новые результаты.

1. Описаны структурные свойства подкодов кода Рида–Маллера $RM(2, m)$, устойчивых к атакам, применимым к полному коду. Описаны структурные свойства подкодов кода $RM(r, m)$, обеспечивающих стойкость к известным структурным атакам на полный код, и построен алгоритм их генерации. Получена оценка доли стойких подкодов кода $RM(r, m)$ с ростом параметра m.

2. Доказаны связи между невырожденностью квазициклической матрицы, соответствующей матрицы над факторкольцом $\mathbb{F}_2[x]/(x^r - 1)$ и матрицы, состоящей из весов соответствующих многочленов. Получены нижние оценки доли невырожденных матриц среди всех матриц заданного размера над факторкольцом $\mathbb{F}_2[x]/(f(x))$. Разработаны эффективные алгоритмы вычисления определителя над факторкольцом $\mathbb{F}_2[x]/(f(x))$ и алгоритм генерации невырожденных матриц с равномерным распределением на множестве всех невырожденных матриц заданного размера. Предложена и теоретически обоснована специализированная версия алгоритма генерации для случая, когда $f(x) = x^r - 1$.

3. Получена оценка снизу на мощность множества открытых ключей схемы подписи CFS, построенной на основе конструкции Сидельникова. Описана структура классов эквивалентности секретных ключей схемы через группы автоморфизмов линейного кода и его квадрата. Уточнена структура классов эквивалентности для случая, когда в схеме используется обобщенный код Рида–Соломона. Выделены три класса ключей схемы подписи,

такие что квадрат кода, задающего открытый ключ, не раскладывается в прямое произведение квадратов базовых кодов.

4. Построена схема электронной подписи на основе протокола идентификации Штерна. Доказана теорема о стойкости подписи к экзистенциальной подделке при атаке с выбором сообщения (модель EUF-CMA).

Методология и методы исследования. В рамках исследования применяется математический аппарат и подходы различных разделов математики, таких как теория кодирования, комбинаторная теория вероятностей, теория алгоритмов, теория сложности вычислений, теория графов.

Степень достоверности. Достоверность полученных результатов обеспечивается через строгие математические формулировки и доказательства теорем. Научные результаты автора опубликованы в открытой печати, прошли апробацию на международных конференциях и научных семинарах. Все результаты, выносимые автором на защиту, получены самостоятельно.

Соответствие диссертации паспорту научной специальности. Тема, объект и предмет исследований диссертации соответствуют паспорту специальности 2.3.6. (Методы и системы защиты информации, информационная безопасность, физико-математические науки) по направлению:

11. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.

15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

19. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Апробация результатов. Результаты, полученные в диссертации, докладывались на международных конференциях и научно-исследовательских семинарах:

- семинаре «Математические методы криптографического анализа» кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2020 год;
- IX международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2020), Московская область, 15–17 сентября, 2020 год;
- международной научно-практической конференции РусКрипто 2021, Солнечногорск, 23–26 марта, 2021 год;
- научном семинаре кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2021 год;

- научном семинаре кафедры информационной безопасности факультета вычислительной математики и кибернетики Московского государственного университета им. М.В. Ломоносова, 2022 год;
- XIII международной научной конференции «Современные тенденции в криптографии» (CTCrypt 2024), Петрозаводск, 3–6 июня, 2024 год.

Публикации по теме исследования. Основные результаты диссертационной работы опубликованы в 5 печатных работах (общим объемом 4.88 п.л.), из них 4 работы (объемом 4.69 п.л.) в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index». Список работ приведен в конце автореферата.

Теоретическая значимость. Проведенное исследование позволило получить результаты, углубляющие математические подходы к построению и обоснованию стойкости криптографических схем, основанных на кодах, исправляющих ошибки.

В рамках изучения схемы электронной подписи CFS, основанной на подкодах кодов Рида–Маллера, был проведен анализ структуры квадратов Адамара этих подкодов путем сведения задачи к задаче из теории графов. Анализ комбинаторных свойств позволил оценить долю подкодов, которые не подвержены известным атакам. Совокупность полученных результатов обеспечила формализованное описание структурных характеристик подкодов, применение которых в данной криптографической схеме обеспечивает стойкость за счет отличия от полного кода Рида–Маллера и сохраняет эффективность благодаря унаследованному алгоритму декодирования.

Применение теории полей и фактор-колец позволило провести расширенное исследование линейных свойств квазициклических матриц, представляющих интерес в силу обеспечиваемого ими существенного сокращения размера открытого ключа в схеме электронной подписи CFS. Полученные результаты наряду с анализом комбинаторных характеристик множества квазициклических матриц позволили разработать эффективные алгоритмы генерации ключей этой схемы.

Исследование алгебраических свойств конкатенированных кодов позволило, с одной стороны, получить оценки мощности множества открытых ключей соответствующей схемы электронной подписи CFS, а с другой — описать структуру множества секретных ключей. Особенности строения обобщенных кодов Рида–Соломона дали возможность уточнить полученные результаты и выделить подклассы секретных ключей, обладающих стойкостью к известным атакам.

Схема электронной подписи на основе протокола идентификации Штерна была синтезирована с целью преодоления ограничений подходов, в которых криптографическая стойкость существенно зависит от структуры используемого кода. Основной задачей являлось построение схемы, для которой возможно строгое обоснование стойкости, не опирающееся на практические знания о су-

ществующих атаках. Обоснование оценки уровня стойкости разработанной конструкции опирается на методы сведения к вычислительно сложным задачам и вероятностные оценки, применяемые в соответствующих моделях нарушителя.

Практическая значимость. Внедрение разработанной в диссертации схемы электронной подписи в средства защиты информации решает практическую задачу обеспечения аутентификации и целостности сообщения, подтверждения авторства и неотказуемости от него в таких прикладных системах, как службы электронной почты, облачные хранилища, системы электронного документооборота, мессенджеры и другие системы асинхронной передачи сообщений, а также распределенные реестры и блокчейн-платформы. Особая актуальность предлагаемого решения обусловлена их стойкостью к атакам, реализуемым с использованием квантовых вычислений. Полученные обоснованные оценки уровня информационной безопасности позволяют осуществлять выбор безопасных значений параметров.

Полученные результаты, связанные с анализом использования специальных классов кодов в схеме подписи CFS, позволяют обоснованно оценить их применимость с точки зрения криптографической стойкости и вычислительной эффективности, а также выработать практические рекомендации для реализаций на их основе. Результаты диссертации также могут войти в состав учебных пособий и быть частью лекционных курсов.

Разработанная схема подписи на основе схемы идентификации Штерна рассматривается в Техническом комитете 26 как вариант будущего постквантового стандарта.

Структура и объем диссертации. Диссертационная работа состоит из введения, вспомогательного раздела, четырех глав, заключения, списка литературы и одного приложения. Общий объем диссертации 159 страниц, включая 6 рисунков, 4 таблицы, 4 алгоритма и 1 приложение. Список литературы включает 84 наименования на 9 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

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

Раздел **Обозначения, определения и общие сведения** устанавливает основные обозначения и формулирует определения, относящиеся к теории кодов, исправляющих ошибки.В нем вводятся понятия линейной зависимости и обратимости матриц в кольце, а также перечислены некоторые специальные виды матриц.

Формулируются определения линейных и дуальных кодов, их параметров, способов задания и операций над ними. Задаются классы кодов, которые (или производные от которых) изучаются в рамках диссертационной работы: квазициклические коды, коды Рида–Маллера, обобщенные коды Рида–Соломона. Также приведены некоторые сведения о этих кодах и их свойства.

Приведена формальная модель протокола электронной подписи, изложено описание оригинальной схемы CFS[69], а также рассмотрены особенности ее построения в случае использования квазициклических кодов вместо кодов Гоппы и при формировании ключей на основе конструкции Сидельникова. Описан протокол идентификации Штерна[70], который может быть использован в качестве основы для построения схемы электронной подписи[71].

Кроме того, в этом разделе представлен перечень вычислительных задач, обладающих доказанной алгоритмической сложностью либо не имеющих известных эффективных решений и, как следствие, рассматриваемых в качестве основы для построения криптографических схем.

В **Главе 1** исследуется структура ключей электронной подписи CFS на основе подкодов кодов Рида–Маллера. Следуя результатам работы И. Чижова и М. Бородина[72], подкоды, квадрат Адамара которых совпадает с квадратом соответствующего кода Рида–Маллера, считаются небезопасными для внедрения в криптографическую схему. Это обусловлено тем, что атака на такую схему за полиномиальное время сводится к атаке на схему, построенную на полном коде Рида–Маллера, для которой уже известны эффективные структурные атаки. Для описания таких подкодов вводится термин *стабильные подкоды*. С целью выявления подкодов, потенциально пригодных для криптографического применения, рассматриваются так называемые *нестабильные подкоды*, базис которых получен исключением из стандартного базиса кода Рида–Маллера, заданного векторами значения мономов

$$1, x_1, x_2, \ldots, x_m, x_1x_2, \ldots, x_{m-1}x_m, \ldots, x_1x_2\ldots x_r, \ldots, x_{m-r+1}x_{m-r+2}\ldots x_m,$$

$q(m,r)$ мономов старшей степени. Стабильные подкоды можно представить как линейную оболочку объединения кода Рида–Маллера порядка $r-1$ с набором из $w(m,r)$ векторов порядка r, где между величинами $q(m,r)$ и $w(m,r)$ существует взаимно однозначное соответствие.

С практической точки зрения важна задача определения минимального значения $q(m,r)$, при котором квадрат подкода совпадает с квадратом полного кода, что означает потерю стойкости. В эквивалентной дуальной постановке необходимо максимизировать параметр $w(m,r)$. Знание этих величин позволяет конструировать безопасные подкоды, удаляя из стандартного базиса $q(m,r)+1$ вектор максимальной степени.

В Разделе 1.1 рассматривались подкоды кодов Рида–Маллера порядка 2.

---

[69] N. Courtois, M. Finiasz и N. Sendrier. «How to achieve a McEliece-based digital signature scheme». В: *Advances in Cryptology — ASIACRYPT 2001. ASIACRYPT 2001. Lecture Notes in Computer Science*. Т. 2248. 2001, с. 157—174.

[70] J. Stern. «A new identification scheme based on syndrome decoding». В: *CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science*. Т. 773. 1994, с. 13—21.

[71] A. Fiat и A. Shamir. «How to prove yourself: practical solutions to identification and signature problems». В: *Advances in Cryptology — CRYPTO' 86. CRYPTO 1986. Lecture Notes in Computer Science*. Т. 263. 1987, с. 186—194.

[72] И. В. Чижов и М. А. Бородин. «Классификация произведений Адамара подкодов коразмерности 1 кодов Рида–Маллера». В: *Дискретная Математика* 32.1 (2020), с. 115—134.

В этом случае было получено полное описание структуры подкодов, а также было найдено значение $w(m, 2)$.

Теорема 1. *Для любого $m \geqslant 4$ верно, что*

$$w(m, 2) = \frac{m(m-3)}{2}.$$

Также было показано следующее структурное свойство.

Теорема 2. *Удаление любых m мономов степени 2 из базиса кода $\mathsf{RM}(2, m)$ гарантировано дает стабильный подкод. Удаление $m+1$ или более мономов степени 2 из базиса кода $\mathsf{RM}(2, m)$ гарантировано дает нестабильный подкод.*

Теорема дает алгоритм построения нестабильных подкодов порядка 2, а также из нее следует, что подкоды, полученные удалением m или менее мономов заведомо будут порождать нестойкие криптографические схемы.

Раздел 1.2 посвящен анализу величины $w(m, r)$. В этом общем случае диссертационная работа оценивает целевое значение сверху и снизу следующими теоремами.

Теорема 3. *Для любого натурального r и $m \geqslant 2r$ выполнено*

$$w(m, r) \geqslant \frac{1}{2}\left(\sqrt{(\gamma+1)^2 + 8 \cdot \binom{m}{2r}} + \gamma + 1\right), \text{ где } \gamma = \sqrt{\sum_{u=\max\{1, 3r-m\}}^{r-1} \binom{r}{u}}.$$

Теорема 4. *Для любого натурального $r \geqslant 2$, $m \geqslant 2r$ и $h < r/3$*

$$w(m, r) \leqslant \binom{m}{r} - T(r, m, h) \cdot \left(\binom{2r}{r} - 2\right),$$

где

$$T(r, m, h) = \max\big\{t : \exists S_1, \ldots, S_t \left(S_i \subset \{1, \ldots, m\} \;\&\right.$$
$$\left.\& \, |S_i| = 2r \;\&\; (i \neq j \Rightarrow |S_i \cap S_j| \leqslant h),\; i, j \in \{1, \ldots, t\}\right)\big\}.$$

Верхняя оценка в работе также была улучшена эмпирически через сведение задачи на кодах к задаче на графах и построение жадного алгоритма для этого графа. Алгоритм содержится в Приложении диссертационной работы.

Исследование вопроса закрывает Раздел 1.3. В нем рассматриваются подкоды, полученные исключением из стандартного базиса ℓ мономов. Для них доказана следующая теорема.

Теорема 5. *Если $\ell = const$ и $r \geqslant 2\ell+1$, то доля нестабильных подкодов кодов* $\mathsf{RM}(r, m)$ *стремится к нулю при* $m \to \infty$.

Таким образом, результаты диссертации показывают, что при случайной генерации маловероятно попасть в подкод, на основе которого может быть построена стойкая криптографическая схема. Однако, следуя предложенной в работе методике систематического исключения векторов максимальной степени, можно конструктивно формировать гарантировано нестабильные подкоды, что, в свою очередь, обеспечивает потенциальную стойкость соответствующих криптосистем, в частности схемы подписи CFS.

Глава 2 посвящена анализу возможностей построения схемы электронной подписи на основе квазициклических кодов.

С точки зрения хранения открытой информации такой подход является высокоэффективным, поскольку позволяет хранить в памяти не каждый элемент матрицы открытого ключа, а лишь первую строку каждой подматрицы. В результате объем памяти, необходимый для хранения квазициклической матрицы размера $k_0 r \times n_0 r$, снижается с $k_0 n_0 r^2$ бит до $k_0 n_0 r$ бит.

Одним из шагов рассмотренного в диссертационной работе алгоритма генерации ключей на основе квазициклического кода является построение случайной невырожденной двоичной квазициклической матрицы. Для реализации этого алгоритма необходимо эффективно проверять матрицу на невырожденность. Сложность проверки на невырожденность матрицы в поле $\mathbb{F}_2$ стандартным образом определяется по алгоритму гауссова исключения и может быть оценена как $O(n_0^3 r^3)$ при $n = n_0 r, n_0 \to \infty$. Однако такой способ не учитывает квазициклическую структуру и не оптимизирован для матриц такого вида.

Другой подход к решению этой задачи был предложен в работе, посвященной схеме LEDAcrypt[73]. Он основан на представлении квазициклической матрицы как матрицы многочленов $M(Q)$ над факторкольцом кольца многочленов $K_f = \mathbb{F}_2[x]/(x^r - 1)$, полученной заменой каждого циркулянта Q с первым столбцом $\widehat{q}$ степени r на многочлен $\widehat{q}_1 + \widehat{q}_2 x + \cdots + \widehat{q}_r x^{r-1}$. Для колец не работают классические алгоритмы линейной алгебры над полем, включающие алгоритм Гаусса. Поэтому авторы предлагают вместо этого применить к матрице $M(Q)$ экспоненциальный алгоритм вычисления перманента. Такой алгоритм возможно использовать при малых значениях параметра n_0 (например, $n_0 = 4$). Но схема подписи CFS требует значительно бóльших параметров[74], таких как $n_0 = 63$, и для них экспоненциальная сложность построения подходящей матрицы становится запретительной.

В работе для решения этой задачи квазициклическая матрица рассматривается в форме матрицы многочленов $M(Q)$, по аналогии с тем, как это было сделано в LEDAcrypt. Далее, на основе этой матрицы, вводится вспомогательная матрица $\mathrm{wt}_2(M(Q))$, элементы которой представляют собой четность весов

[73] M. Baldi и др. «LEDAcrypt: Low-dEnsity parity-check coDe-bAsed cryptographic systems». В: *NIST proposal* (2019), с. 1—83.

[74] E. D. Fiallo. «A digital signature scheme mCFSQC-LDPC based on QC-LDPC codes». В: *Mat. Vopr. Kriptogr.* 12.4 (2021), с. 99—113.

соответствующих многочленов, то есть четность количества их ненулевых коэффициентов. Раздел 2.1 посвящен строгому заданию этих матриц.

Связь между свойствами обратимости указанных матриц формализована в следующей теореме Раздела 2.2.

Теорема 6. *Квазициклическая матрица Q вырождена тогда и только тогда, когда вырождена соответствующая ей матрица $M(Q)$. Для того, чтобы была вырождена матрица Q, необходимо, чтобы была вырождена матрица $\mathrm{wt}_2(M(Q))$.*

Раздел 2.3 посвящен оценке доли невырожденных матриц в факторкольцах K_f и K_{x^r-1}. Этот результат представлен в следующей теореме.

Теорема 7. *Доля $\varrho(K_f, n)$ невырожденных матриц $A \in K_f^{n\times n}$ удовлетворяет неравенству*

$$\varrho(K_f, n) > e^{-2}\left(1 - \sum_{\alpha\in\overline{\eta}(f)} 2^{-\deg\alpha}\right),$$

где $\overline{\eta}(f(x))$ есть множество неприводимых собственных делителей.

Для любого простого r и натурального n верно неравенство

$$\varrho(K_{x^r-1}, n) > \frac{1}{4e^2}.$$

В Разделе 2.4 предложен эффективный алгоритм приведения матрицы $A \in K_f^{n\times n}$ к верхнетреугольному виду. На его основе в Разделе 2.5 построен алгоритм генерации случайной обратимой матрицы над кольцом K_f. Алгоритм реализуется посредством случайной генерации матрицы многочленов и последующей проверки обратимости ее определителя. В случае отрицательного результата генерация повторяется. Простроенный алгоритм эффективен, что описывает следующая теорема.

Теорема 8. *Пусть $f(x)$ — многочлен степени $r \geqslant 1$. Тогда существует алгоритм, действующий в кольце K_f, который выводит невырожденную матрицу и завершается с вероятностью 1, причем каждую невырожденную матрицу он возвращает с одинаковой вероятностью. В среднем (по внутреннему источнику случайности) он требует генерации $n^2r[\varrho(K_f, n)]^{-1}$ случайных бит и выполнения $O\left(n^3r^2[\varrho(K_f, n)]^{-1}\right)$ битовых операций, где $\varrho(K_f, n)$ есть доля невырожденных матриц над кольцом K_f.*

В качестве альтернативного подхода был предложен другой алгоритм решения той же задачи, но специализированный для колец K_{x^r-1}. На первом этапе осуществляется генерация случайной двоичной матрицы с последующей проверкой ее обратимости. В случае положительного результата данная матрица интерпретируется как матрица весов, на основе которой формируется матрица

многочленов таким образом, чтобы вес каждого многочлена совпадал со значением в соответствующем элементе. На завершающем этапе вновь требуется проверка обратимости построенной матрицы через вычисление ее определителя. Трудоемкость этого алгоритма задается следующей теоремой.

Теорема 9. *Существует алгоритм, действующий в кольце K_{x^r-1}, который выводит невырожденную матрицу и завершается с вероятностью 1, причем каждую невырожденную матрицу он возвращает с одинаковой вероятностью. В среднем (по внутреннему источнику случайности) он требует выработки*

$$\frac{n^2 + n^2 r \varrho(\mathbb{F}_2, n)}{\varrho(K_{x^r-1}, n)}$$

случайных бит и выполнения

$$O\left(n^3 r^2 \frac{\varrho(\mathbb{F}_2, n)}{\varrho(K_{x^r-1}, n)}\right)$$

битовых операций, где $\varrho(\mathbb{F}_2, n)$ и $\varrho(K_{x^r-1}, n)$ есть доля невырожденных матриц над полем $\mathbb{F}_2$ и кольцом K_{x^r-1}, соответственно.

В **Главе 3** рассматривается возможность построения ключей электронной подписи CFS на основе конструкции Сидельникова. Если раньше открытый ключ был произведением $MR\Gamma$ тройки матриц, составляющих секретный ключ, где M была невырожденной матрицей, R — проверочной матрицей некоторого линейного кода, а Γ — перестановочной матрицей, то теперь рассматриваются открытые ключи вида $(M_1R_1\|M_2R_2)\Gamma$, где обе матрицы M_1, M_2 невырождены и входят в секретный ключ, а R_1, R_2 — порождающие матрицы, вообще говоря, не обязательно одинаковых кодов.

В силу того, что один открытый ключ как в оригинальной, так и в модифицированной криптосистеме может быть получен из различных секретных ключей, их множество естественным образом разбивается на классы эквивалентности. Тогда для изучения особенностей структуры каждого класса можно использовать любого его представителя. В частности, можно обращаться к открытым ключам вида $(R_1\|MR_2)\Gamma$, где $M = M_1^{-1}M_2$.

В работе рассматриваются только случаи, когда матрицы R_1 и R_2 совпадают. Код, заданный такой порождающий матрицей, в работе обозначен через $\mathcal{C}[M]$, а также для него введено определение: такой код называется *кодом с разложимым квадратом*, если $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$ и *кодом с неразложимым квадратом*, если $(\mathcal{C}[M])^2 \subsetneq \mathcal{C}^2 \times \mathcal{C}^2$.

Способ задания ключей криптосистемы на основе конструкции Сидельникова неоднократно подвергался изучению. Работа И. Чижова, С. Конюхова и А. Давлетшиной[75] рассматривает случай, когда схема строится полностью на

[75] И. В. Чижов, С. А. Конюхов и А. М. Давлетшина. «Эффективная структурная атака на криптосистему Мак-Элиса–Сидельникова». В: *International Journal of Open Information Technologies* 8.7 (2020), с. 1—10.

кодах Рида–Маллера (авторы рассматривают обобщение, где используется некоторое произвольное число копий кода $u \geqslant 2$). Она предлагает полиномиальную атаку восстановления секретного ключа по открытому ключу криптосистем, использующих код Рида–Маллера с разложимым квадратом.

Полиномиальная атака на вариант, в котором R_1 — порождающая матрица кода Рида–Маллера, а R_2 — порождающая матрица случайного линейного кода И. Чижова и Е. Поповой,[76] также возможна в предположении о разложимости квадрата соответствующего кода. Эти результаты были обобщены в работе В. Деундяка и Ю. Косолапова[77], где для криптографической схемы на основе u порождающих матриц произвольных линейных кодов построено сведение к стойкости схем на каждом коде по-отдельности.

В то же время в работе И. Чижова[78] показано, что с вероятностью близкой к 1 случайный линейный код обладает разложимым квадратом. Это делает введенное понятие кода с неразложимым квадратом актуальным необходимым условием стойкой криптосистемы.

Раздел 3.1 вводит дополнительное определение *укорочения кода* и связанное с ним свойство. В Разделе 3.2 вводится понятие эквивалентных секретных ключей схемы подписи, а также показано взаимно однозначное соответствие между классом эквивалентности и некоторым введенным множеством перестановок $\mathcal{G}_R(M_1, M_2)$. Соответствующая теорема есть обобщение результата из диссертационной работы И. Чижова[79], доказанного для кодов Рида–Маллера.

Теорема 10. *Для произвольной матрицы R полного ранга существует взаимно однозначное соответствие между классом эквивалентности секретных ключей вида $[(M_1, M_2, \Gamma)]_R$ и множеством $\mathcal{G}_R(M_1, M_2)$.*

Еще одним обобщением является полученная в этом разделе оценка снизу на мощность открытых ключей соответствующей схемы подписи CFS.

Теорема 11. *Справедлива оценка снизу на мощность ε множества открытых ключей схемы подписи CFS на основе конструкции Сидельникова:*

$$\frac{(2n)!h_k}{2^n|\mathrm{Aut}(\mathcal{C})|} \leqslant \varepsilon,$$

где $\mathcal{C}$ — произвольный код с порождающей матрицей R, все столбцы которой различны, а h_k — число невырожденных $(k \times k)$-матриц над полем $\mathbb{F}_{q^m}$.

---

[76] И. В. Чижов и Е. А. Попова. «Структурная атака на криптосистемы типа Мак-Элиса–Сидельникова, построенной на основе комбинирования случайных кодов с кодами Рида–Маллера». В: *International Journal of Open Information Technologies* 8.6 (2020), с. 24—33.

[77] V. M. Deundyak и Y. V. Kosolapov. «On the strength of asymmetric code cryptosystems based on the merging of generating matrices of linear codes». В: *16th International Symposium "Problems of Redundancy in Information and Control Systems REDUNDANCY 2019* (2019), с. 143—148.

[78] И. В. Чижов. «Квадрат Адамара последовательно соединенных линейных кодов». В: *Дискретная математика* 3 (2023), с. 100—124.

[79] И. В. Чижов. «Ключевое пространство криптосистемы Мак-Элиса–Сидельникова». В: *Дискрет. матем.* 21 (2009), с. 132—159.

Введено понятие кода с разложимым и неразложимым квадратом и доказано, что любой линейный код обязан удовлетворять одному из этих определений.

Теорема 12. $(\mathcal{C}[M])^2 \subseteq \mathcal{C}^2 \times \mathcal{C}^2$ *для всех невырожденных матриц* M.

Получено описание класса эквивалентности секретных ключей схемы подписи CFS на основе конструкции Сидельникова, построенной на произвольном линейном коде, если код $\mathcal{C}[M]$ имеет разложимый квадрат.

Теорема 13. *Если* $(\mathcal{C}[M])^2 = \mathcal{C}^2 \times \mathcal{C}^2$, *то* $\mathcal{A}(\mathcal{C}) \subseteq \mathcal{G}_R(I, M) \subseteq \mathrm{Aut}(\mathcal{C}^2 \times \mathcal{C}^2)$, *где*

$$\mathcal{A}(\mathcal{C}) = \bigcup_{\Gamma \in \mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{C})} \{\Gamma, \Gamma\Gamma_b, \Gamma_b\Gamma\},$$
$$\Gamma_b : \Gamma_b(k) = ((k - 1 + n) \bmod 2n) + 1, 1 \leqslant k \leqslant 2n.$$

Раздел 3.3 уточняет результат, полученный для произвольных линейных кодов, за счет сужения области исследования до обобщенных кодов Рида–Соломона. Теперь, когда R является порождающей матрицей кода Рида–Соломона, описание класса эквивалентности секретных ключей принимает следующий вид.

Теорема 14. *Если* $(\mathsf{GRS}_k(\alpha, v)[M])^2 = \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2)$, *то*

$$\mathcal{A}(\mathsf{GRS}_k(\alpha, v)) \subseteq \mathcal{G}_R(I, M) \subseteq \mathcal{A}(\mathsf{GRS}_{2k-1}(\alpha, v^2)).$$

Раздел 3.4 содержит примеры невырожденных матриц M, задающих коды с неразложимым квадратом. Такие коды не могут быть найдены случайно в силу их малой вероятности, при этом они являются потенциальной основой для построения стойких криптографических схем, не подверженных упомянутым выше атакам.

Следующие три теоремы гарантируют неразложимый квадрат у соответствующих кодов.

Теорема 15. *Если* $\{i_1, i_2\} \cap \{1, k\} \neq \varnothing$ *в матрице*

$$T_{a,b}^{i_1,i_2} = \begin{array}{c} \\ \\ \\ {\scriptstyle i_1\rightarrow} \\ \\ {\scriptstyle i_2\rightarrow} \\ \\ \\ \end{array} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots & \dots & \vdots \\ a_1 & a_2 & \dots & a_{i_1} & \dots & a_{i_2} & \dots & a_k \\ \vdots & \vdots & \dots & \vdots & \ddots & \vdots & \dots & \vdots \\ b_1 & b_2 & \dots & b_{i_1} & \dots & b_{i_2} & \dots & b_k \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix}^{\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \\ \\ \\ {\scriptstyle i_1\downarrow} \\ \\ {\scriptstyle i_2\downarrow} \\ \\ \\ \end{array}},$$

и матрица

$$\begin{pmatrix} a_{i_1} & a_{i_2} \\ b_{i_1} & b_{i_2} \end{pmatrix}$$

невырождена, то

$$\left(\mathsf{GRS}_k(\alpha, v)\left[T_{a,b}^{i_1,i_2}\right]\right)^2 \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2),$$

Теорема 16. $(\mathsf{GRS}_k(\alpha, v)[D])^2 \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2)$ *для произвольной диагональной матрицы* D *и* $k \leqslant \frac{n+1}{2}$.

Теорема 17. *Для любой матрицы* H' *над* $\mathbb{F}_{2^m}$ *вида*

$$H' = \left(\begin{array}{c|c} \hat{H} & H_1 \\ \hline 0 & H_2 \end{array}\right),$$

где $\hat{H}$ *— ортогональная подматрица, выполнено*

$$(\mathsf{GRS}_k(\alpha, v)[H'])^2 \subsetneq \mathsf{GRS}_{2k-1}(\alpha, v^2) \times \mathsf{GRS}_{2k-1}(\alpha, v^2).$$

Глава 4 посвящена разработке альтернативного подхода к построению схемы электронной подписи на основе кодов, исправляющих ошибки. Недостатком схемы CFS является то, что использование некоторых классов кодов может привести к снижению ее криптографической стойкости. Это связано с некорректностью предположения о сложности для конкретных классов кодов задачи синдромного декодирования, которая заключается в поиске вектора e веса t такого, что $He^T = s^T$ для заданной матрицы H, вектора s и числа t. На сегодняшний день доказательство NP-трудности известно только для линейного кода общего вида. Его можно найти, например, в работе Э. Берлекэмпа, Р. Мак-Элиса и Х. Ван Тилбурга[80]. Поэтому целесообразным представляется построение схемы электронной подписи на основе оригинальной вычислительно сложной задачи, стойкость которой не зависит от структуры используемого кода. Такой поход исключает возможность использования алгоритмов декодирования, непосредственно опирающихся на внутренние свойства кодов, что обусловливает необходимость поиска принципиально иного подхода по сравнению со схемой CFS.

Вариант решения поставленной задачи предложен в Разделе 4.1, также в нем введены формальные модели нарушителя. В качестве основы для построения новой схемы электронной подписи выбрана схема идентификации, предложенная Я. Штерном[81]. Как показали А. Фиат и А. Шамир[82] в 1987 году, на

[80] E. R. Berlekamp, R. J. McEliece и H. C. A. van Tilborg. «On the inherent intractability of certain coding problems». В: *IEEE Transactions on Information Theory* 24.3 (1978), с. 384—386.

[81] J. Stern. «A new identification scheme based on syndrome decoding». В: *CRYPTO' 93. CRYPTO 1993. Lecture Notes in Computer Science*. Т. 773. 1994, с. 13—21.

[82] A. Fiat и A. Shamir. «How to prove yourself: practical solutions to identification and signature problems».

базе схемы идентификации возможно построение схемы электронной подписи, посредством внедрения дополнительной хэш-функции, имитирующий интерактивный ответ второй стороны. Для построенной схемы в Разделе 4.2 через серию сведений получено обоснование стойкости в модели EUF-CMA, в которой нарушитель, с целью построения подделки, имеет возможность запрашивать подписи на выбранные им сообщения, а также вычислять значения внутренней хэш-функции. Стойкость построенной схемы подписи описывает следующая теорема.

Теорема 18. *Пусть $\mathcal{A}$ — нарушитель, решающий задачу* EUF-CMA *для подписи на основе схемы идентификации Штерна, делая не более q_f запросов к оракулу хэширования* F *и не более q_s запросов к оракулу генерации подписи* Sign. *Тогда*

$$\mathsf{Adv}^{\text{EUF-CMA}}_{\text{Stern}}(\mathcal{A}) \leqslant \max\left\{ 15q_f \cdot \sqrt[3]{\frac{\delta^2(T+\tilde{\tilde{c}}(2q_f+q_sT^{Sig}_{\text{Stern}}))}{\min\{T_{\mathsf{SD}},T_{\mathsf{Coll}}\}}} + \right.$$

$$\left. + \left(\frac{2}{3}\right)^{\delta}\cdot(1+q_f) + q_s\cdot\left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta}, \left(\frac{2}{3}\right)^{\delta}\cdot\left(1+q_f\left(1+2\delta\cdot 1.1^{\delta}\right)\right) + q_s\cdot\left(\frac{14\tilde{c}\delta q_f}{T_{\mathsf{Coll}}}\right)^{\delta} \right\},$$

где T^{Sig}_{Stern} — сложность алгоритма генерации подписи, T есть максимальная возможная сложность нарушителя $\mathcal{A}$, T_{SD} и T_{Coll} — сложности оптимальных алгоритмов, решающих задачи синдромного декодирования и поиска коллизии хэш-функции с вероятностями успеха не менее, чем $1-\frac{1}{e}$, а $\tilde{c}$ и $\tilde{\tilde{c}}$ — константы, зависящие от модели вычислений.

Схема подписи на основе схемы идентификации Штерна разрабатывалась в рамках деятельности рабочей группы Технического комитета 26 по стандартизации.

В **Заключении** представлены основные результаты диссертации.

Приложение включает код одного из приведенных в Главе 1 алгоритмов, написанный на языке `Python`.

Заключение. К основными результатами диссертационной работы можно отнести следующее.

1. Описана структура всех подкодов кодов Рида–Маллера второго порядка, свойства которых являются причиной уязвимости соответствующих вариантов схемы подписи CFS. Такое описание, в частности, помогает построить подкод, дающий схему подписи, стойкую к известным атакам. Для кодов произвольного порядка выписаны оценки, задающие стойкие подкоды, и показано, что число таки кодов стремится к нулю с ростом параметра m, задающего код Рида–Маллера. Таким образом, при случайном

В: *Advances in Cryptology — CRYPTO' 86. CRYPTO 1986. Lecture Notes in Computer Science.* Т. 263. 1987, с. 186—194.

выборе подкода кода Рида–Маллера почти невозможно построить стойкую схему подписи.

2. Для другого варианта схемы подписи CFS, в котором ключи строятся на основе квазициклических кодов, предложены алгоритмы, позволяющие эффективно генерировать ключевую пару. Известные ранее алгоритмы при решении этой задачи либо не использовали структуру кода, что сказывалось на их трудоемкости, либо, несмотря на специализацию, работали за экспоненциальное время.

3. При справедливости дополнительного условия в случае, когда ключи подписи CFS строятся на основе конструкции Сидельникова, получены соотношения, описывающие классы эквивалентности секретных ключей. Это же условие является необходимым для ряда известных атак и выполняется с вероятностью, близкой к единице. В совокупности это говорит о невозможности использования конструкции Сидельникова при случайном выборе экземпляров кодов. Поэтому в работе предложено несколько специальных классов секретных ключей, схемы на которых не подвержены известным атакам.

4. Наконец, предложен вариант построения схемы электронной подписи, которая лишена недостатков, связанных с особенностями базовых кодов. Синтез такой подписи состоит в применении преобразования Фиата–Шамира к протоколу идентификации Штерна. Стойкость построенной схемы обоснована и сведена к NP-трудной задаче декодирования случайного линейного кода.

Полученные в диссертации результаты могут быть применены при разработке новых подходов к проектированию криптографических схем с открытым ключом. Работа позволяет выбирать наиболее стойкие классы кодов для кодовых систем, исключая неперспективные варианты, а также способствует повышению эффективности и безопасности построения электронных подписей.

Благодарности. Автор диссертации выражает благодарность за постановку задачи, внимание к работе и советы своему научному руководителю кандидату физико-математических наук Чижову Ивану Владимировичу. Также автор благодарит мужа и друзей за поддержку, оказанную в процессе написания работы.

СПИСОК ПУБЛИКАЦИЙ АВТОРА ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность и индексируемых в базе ядра Российского индекса научного цитирования «eLibrary Science Index»:

[1] Vysotskaya V. Characteristics of Hadamard Square of Special Reed–Muller Subcodes // Прикладная дискретная математика. – 2021. – №– 53. С. 75–88. – EDN: TEDEFN.
0.88 п.л., Scopus, RSCI, импакт-фактор 0.11 (JCI).

[2] Высоцкая В. В., Высоцкий Л. И. Обратимые матрицы над некоторыми факторкольцами: идентификация, построение и анализ // Дискретная математика. 2021. – Т. 33. – №2. – С. 46–65. – EDN: VASNIG.
1.25 п.л., RSCI, импакт-фактор 0.39 (РИНЦ).
Соавтору принадлежит алгоритм приведения матрицы над факторкольцом кольца многочленов к верхнетреугольному виду (Алгоритм 1 по тексту статьи), остальные результаты статьи получены Высоцкой В. В., 90%, 1.06 п.л.
На англ. языке: Vysotskaya V., Vysotsky L. Invertible matrices over some quotient rings: identification, generation, and analysis // Discrete Mathematics and Applications. – 2022. – 32(4). – pp. 263–278. – EDN: EDHYGI.
1 п.л., вклад автора 90%, 0.94 п.л., Scopus, WoS, импакт-фактор 0.22 (JCI).

[3] Высоцкая В. В. О структурных особенностях пространства ключей криптосистемы Мак-Элиса–Сидельникова на обобщенных кодах Рида–Соломона // Дискретная математика. – 2024. – Т. 36. №4. – С. 28–43. – EDN: IBRMIU.
1 п.л., RSCI, импакт-фактор 0.39 (РИНЦ).

[4] Vysotskaya V., Chizhov I. The security of the code-based signature scheme based on the Stern identification protocol // Прикладная дискретная математика. 2022. – №57. – С. 67–90. – EDN: FFRFUH.
1.56 п.л., Scopus, RSCI, импакт-фактор 0.11 (JCI).
Соавтору принадлежит постановка задачи и верификация результатов, остальные результаты статьи получены Высоцкой В. В., 95%, 1.56 п.л.

В прочих изданиях:

[5] Vysotskaya V. New estimates for dimension of Reed–Muller subcodes with maximum Hadamard square // Прикладная дискретная математика. Приложение. – 2020. – №13. – С. 98–100. – EDN: TCYZCI.
0.19 п.л., ВАК, импакт-фактор 0.06 (РИНЦ).