Southern Federal University

as a manuscript

Kirill Vedenev

Study of Codes from Non-Abelian Group Algebras and Security Analysis of Code-Based Cryptosystems

Dissertation summary
for the purpose of obtaining academic degree
Doctor of Philosophy (PhD) in Applied Mathematics

Academic advisors:
Yury Kosolapov, PhD
Vladimir Deundyak, PhD

Rostov-on-Don – 2024

1 Topic of the dissertation and its relevance

The dissertation is dedicated to exploring various aspects of coding theory and its applications in cryptography. Coding theory, an interdisciplinary field that integrates methods from mathematics, computer science, and engineering, aims to ensure reliable and error-free transmission of information over noisy channels. As coding theory has developed, it has found numerous applications beyond error correction in communication channels. A significant portion of these applications lies within the realm of cryptography and steganography, encompassing code-based public-key encryption schemes, digital signatures, secret sharing, secure multi-party computation, data hiding, protection against unauthorized copying, as well as ensuring information-theoretic privacy using wiretap channels, and so forth.

Each application presents its own specialized requirements for the codes used. For instance, error correction in communication channels focuses on minimizing redundancy and developing efficient encoding and decoding algorithms. In turn, in code-based cryptographic primitives, the emphasis is on resisting attacks. Thus, constructing error-correcting codes that meet diverse requirements and analyzing their applicability in various scenarios is a central objective of coding theory.

Coding theory is deeply interconnected with linear and abstract algebra. For instance, almost all codes employed in practice are linear codes, i.e., linear subspaces of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ denotes the finite field of cardinality q. Transitioning from unstructured codes to linear ones significantly simplifies the encoding process, which can now be performed through multiplication of a message vector by a generator matrix. Moreover, this transition also simplifies the finding of the minimum distance as it is equal to the minimum weight for linear codes. In 1957, E. Prange introduced a subclass of linear codes called *cyclic codes* [117], which are characterized by the property that any codeword $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$ has its cyclic shift $\mathbf{c}' = (c_n, c_1, \ldots, c_{n-1})$ also as a codeword in C. This additional property substantially aids in the application of powerful algebraic techniques for studying codes. Consequently, it allows for deriving estimates of parameters (such as the Bose–Chaudhuri–Hocquenghem (BCH) bound [32]) and developing efficient decoding algorithms (see e.g. [6; 11; 41; 64; 115]).

Group codes (or *G-codes*), which are ideals of group algebras $\mathbb{F}_qG$ where G is a finite group, represent a generalization of cyclic codes. Specifically, cyclic codes of length n can be considered as ideals of the group algebra $\mathbb{F}_qC_n$, with C_n denoting the cyclic group of order n. The concept of group codes was independently proposed by S. Berman in [17; 18] and F. J. MacWilliams [95; 96]. S. Berman discovered that binary Reed-Muller codes, which is another very efficient class of linear codes, can be viewed as ideals of elementary abelian 2-groups [17], and he analyzed the algebraic structure of codes from semisimple abelian group algebras [18]. While in [95; 96], F. J. MacWilliams extended several theorems related to cyclic codes to codes derived from abelian groups.

Group codes exemplify how the rich algebraic structure enables the use of algebraic methods to study code properties and produce codes that inherit the advantages of cyclic codes. Many well-known effective codes are now recognized as group codes, including Generalized Reed-Muller codes and extended Reed-Solomon codes [79; 88]. Additionally, the group structure can be leveraged for decoding, as evidenced by generic decoding techniques of [44], decoders for binary Reed-Muller codes that utilize group structure [88], permutation decoding for codes from semisimple abelian group algebras [40], and automorphism ensemble decoders for Reed-Muller and group-structured LDPC codes [12; 13; 69].

In her seminal work [95], F. J. MacWilliams proposed «*to look for a class of groups, not cyclic,*

which produce codes with some desirable practical properties» as a new promising research direction. Motivated by this and by possible applications of group codes, in this dissertation, we investigate **the problem of constructing and studying group codes derived from finite non-abelian groups**, particularly *dihedral and metacyclic groups*. Below, we provide a brief survey of related works on group codes:

- *Structure of abelian codes.* The algebraic structure of codes from abelian groups have been extensively studied in [5; 17; 18; 89; 95; 96; 119; 121]. In [82], J. Jensen discovered that abelian group codes can be viewed as generalized concatenated codes (see [27; 152]), enabling the derivation of lower bounds on their minimum distance based on the concatenated structure. Another lower bound on minimum distance, derived by P. Camion in [36] (see also [20; 122]), uses the properties of the generalized discrete Fourier Transform and generalizes the BCH bound for cyclic codes. In [19], Bernal et al. generalized Camion's bound and developed a technique to extend any bound for the minimum distance of cyclic codes constructed from its defining sets (ds-bounds) to abelian codes. Note that for certain classes of abelian code, the applicability of locator decoding using the Berlekamp-Massey-Sakata algorithm was shown in [23; 125].

- *Examples of codes from abelian groups* include cyclic codes, Generalized Quadratic Residue codes [94], Generalized Reed-Muller codes [88], Cauchy codes [21; 67], Hyperbolic codes [84], Multiplied cyclic codes [22], and Berman codes [18]. Recently, it was proved that Reed-Muller codes and Berman codes achieve Shannon capacity on the binary erasure channel (BEC) [106; 120]. More recently, a larger class of abelian group codes was shown to achieve capacity on BEC [105], and RM codes were proved to achieve capacity for any binary memoryless channel [4].

- *Majority-logic decoding of group codes.* In [151], K.-H. Zimmerman showed that it is possible to construct L-step majority logic decodable (see [99]) group codes using some methods of modular representation theory. In [56; 58], V. Deundyak et al. further investigated the majority logic decoding of group codes. In [53; 91], C. Tjhai et al. proposed an approach for constructing one-step majority logic decodable cyclic codes via idempotents of the group algebra $\mathbb{F}_q C$. It is important to note that these codes demonstrate excellent performance as Low-Density Parity-Check (LDPC) codes.

- *Relation between abelian and non-abelian codes* In [124], R. Sabin and S. Lomonaco discovered that all central codes (i.e., two-sided ideals) from group algebras of semidirect products of cyclic groups are combinatorially equivalent to abelian codes (i.e., ideals abelian group algebras), with their minimum distances being rather undesirable. However, they also demonstrated the existence of one-sided ideals in those group algebras that produce codes with better parameters than abelian codes, with some examples comparable to the best-known linear codes.

  In [21], Bernal et al. obtained a criterion to decide if a linear code is a group code in terms of its intrinsic properties in the ambient space. They also extended the result of Sabin and Lomonaco by showing that if a group G has two abelian subgroups A and B such that $G = \{ab \mid a \in A, b \in B\}$, then all central codes in $\mathbb{F}_q G$ are combinatorially equivalent to abelian codes. Additionally, they provided a non-constructive proof of the existence of one-sided group codes that are not equivalent to any abelian code.

  Furthermore, in [73], Pillado et al. proved that all central G-codes of length less than 24 are abelian (i.e., can be viewed as ideals of abelian group algebras), and there exist central

non-abelian codes of length 24. The results on the existence of central non-abelian group codes were further refined in [72; 107; 110; 149].

- *Codes from non-abelian group algebras.* In [123], R. Sabin proposed using matrix representations of semisimple group algebras for studying minimal group codes. Specifically, semisimplicity implies that the group algebra can be decomposed into a direct sum of minimal two-sided ideals (central codes), with each summand being isomorphic to an irreducible representation of G over $\mathbb{F}_q$ (in turn, each such representation is isomorphic to a matrix algebra). In [124], R. Sabin and S. Lomonaco studied codes from semisimple group algebras of some split metacyclic groups $G_{n,m,r} = \langle x, y \mid x^n = y^m = e, xy = y^r x \rangle$, where $r^m \equiv 1 \pmod{n}$, using irreducible representations. In particular, they described an algorithm for finding irreducible representations in the case when the ambient field $\mathbb{F}_q$ contains all n-th roots of unity.

  In [68], Dutra et al. considered central codes from semisimple dihedral group algebras $\mathbb{F}_q D_{2n}$, where $D_{2n} = G_{n,2,-1} = \langle x, y \mid x^n = y^2 = e, xy = y^{-1}x \rangle$, defined by idempotents constructed from subgroups, and computed their dimensions and weights. It is worth mentioning that due to the above-mentioned result of Bernal et al., [21], all these codes are equivalent to abelian codes. In [10], S. Assuena and C.P. Miles considered semisimple group algebras $\mathbb{F}_q G$ of non-abelian split metacyclic groups over a finite field and found the primitive central idempotents of $\mathbb{F}_q G$ in the case when the order of G equals $p^m l^n$, where p and l are different prime numbers. In their recent works [8; 9], S. Assuena and C.P. Miles proposed a construction of non-central codes for the same classes of groups using idempotents derived from subgroups and obtained some good non-abelian codes with parameters matching best-known linear codes. Constructions of group codes using idempotents were also explored in [70; 76–78; 116; 128].

  In [34], O. Broche and A. del Rio proposed a computational method for describing the Wedderburn decomposition and the primitive central idempotents of a semisimple finite group algebra of an abelian-by-supersolvable group G from certain pairs of subgroups of G. Building upon this work, in [111], G. Olteanu and V. Gelder proposed algorithms to construct minimal left group codes and showed that their main result can be applied to the metacyclic groups of the form $C_{q^m} \leftthreetimes C_{p^n}$ with C_{p^n} acting faithfully on C_{q^m}, where p and q are different primes and the field size s is coprime to p and q. Additionally, in [111], they presented alternative constructions to some of the best-known linear codes. In [14], Bakshi et al. proposed an algorithm for the computation of a complete set of primitive central idempotents, the automorphism group, and the Wedderburn decomposition of the semisimple group algebra of a finite metabelian group in terms of Shoda pairs. However the Wedderburn isomorphism constructed in [14] is not explicit.

  In [35], F.E. Brochero Martinez obtained an explicit Wedderburn decomposition of the semisimple dihedral group algebra $\mathbb{F}_q D_{2n}$. In 2020, Gao et al. [71] generalized this result by obtaining an explicit Wedderburn decomposition for $\mathbb{F}_q G_{n,2,r}$, where $G_{n,2,r}$ is defined as above and $r^m \equiv 1 \pmod{n}$. In addition, Gao et al. [71] described some linear complementary dual (LCD) codes and central self-orthogonal codes from these group algebras, although a complete description of all codes was not provided in their study [71].

  In 2016, Cao et al. [37] studied the concatenated structure of dihedral codes leveraging only finite field theory and basic theory of cyclic codes and skew cyclic codes. Using similar methods, Cao et al. [112] proved the concatenated structure of codes from a class of

metacyclic groups of the form $G_{n,3,r}$. In 2022, Cao et al. [38] refined the results of [37] and determined all distinct Euclidean LCD codes and Euclidean self-orthogonal dihedral codes in terms of their concatenated structure.

In 2021, M. Borello and A. Jamous [28] derived a BCH-like lower bound on the minimum distance of dihedral codes by viewing dihedral codes as subcodes of expanded cyclic codes over field extensions. Note that a similar technique was leveraged by K. Lally in [87] for deriving the minimum distance bound for quasi-cyclic codes.

- *Asymptotic performance.* In 2006, Bazzi and Mitter [15] proved that binary dihedral codes are asymptotically good. Specifically, for infinitely many block lengths, a random ideal in the binary group algebra of the dihedral group is an asymptotically good rate-half code with a high probability. In 2007, Martínez□Perez and Willems [98] further improved this result. In 2020, assuming the Generalized Riemann Hypothesis is true, Borello et al. [29] proved that metacyclic codes are asymptotically good. In 2020, M. Borello and W. Willems [30] considered metacyclic group algebras of the form $\mathbb{F}_p \langle \alpha, \beta \mid \alpha^p = \beta^q = e, \alpha\beta = \beta^m\alpha \rangle$, where p is a fixed prime and q is a prime such that $p \mid (q-1)$, $m \not\equiv 1 \pmod{q}$, $m^p \equiv 1 \pmod{q}$, and proved that codes from these group algebras are asymptotically good without relying on any additional assumptions.

- *Applications.* Many well-known codes, including cyclic, Reed-Solomon, and Reed-Muller codes, are group codes and thus have numerous practical applications for error and erasure correction. In [56; 57], V. Deundyak and Yu. Kosolapov investigated the applicability of certain majority-logic decodable group codes in code-based encryption schemes and conjectured that *utilizing codes from non-abelian groups could potentially enhance the security of code-based cryptosystems against key-recovery attacks*. In 2023, Borello et al. [63] studied dihedral quantum codes and obtained an example of short dihedral quantum codes that improved upon the parameters of previously known quantum codes.

Overall, these related works evince the relevance and active research interest in studying group codes, highlighting their theoretical importance and practical applications.

In recent years, the applications of coding theory in cryptography for building asymmetric encryption schemes and digital signatures have gained significant research attention and practical relevance. This is primarily due to the fact that integer factorization and discrete logarithm problems used in traditional cryptosystems like RSA and elliptic-curve primitives can be attacked in polynomial time using quantum computers with Shor's algorithm [131], rendering them completely insecure when large-scale quantum computers appear. In contrast, the security of code-based cryptography is mostly based on the hardness of the problem of decoding random linear codes, which is considered to be difficult even for quantum computers [24]. Code-based cryptography is considered the oldest and most studied alternative to traditional number-theoretic and elliptic curve cryptosystems.

In 1978, the same year RSA was published, Robert McEliece, in his seminal work [101], proposed the first public-key encryption scheme based on error-correcting codes. His approach involves using the matrix $\tilde{G} = SGP$ as the public key, where G is a generator matrix of a binary t-error correcting Goppa code C, and S and P are random $k \times k$ invertible and $n \times n$ permutation matrices, respectively. Encryption of a message $m \in \mathbb{F}_2^k$ is performed as $y = m\tilde{G} + \varepsilon$, where ε is a random error of the Hamming weight t. Given the matrices S and P, it is straightforward to recover m using the decoding algorithm of C. An optimized modern version of the Goppa code-based McEliece cryptosystem ClassicMcEliece [45] is still considered secure and was selected

as a finalist in round 3 of the NIST post-quantum standardization competition [135]. Despite its many advantages, the McEliece cryptosystem has a serious drawback of large public keys, which limits its practical applications in many scenarios.

To address this drawback, numerous attempts have been made to replace Goppa codes with more efficient ones in the McEliece protocol, such as Generalized Reed-Solomon codes, Reed-Muller codes, algebraic geometry codes, LDPC codes, concatenated codes, and some group codes [26; 57; 59; 81; 83; 103; 108; 132]. Additionally, to enhance security, there have been propositions to improve the hiding mechanisms of the secret code (see, e.g., [2; 3; 16; 55; 85; 97; 127; 137; 148]). However, many of these modifications have been subjected to successful key-recovery attacks (see, e.g., [31; 43; 46; 47; 49; 50; 60–62; 65; 102; 113; 114; 133; 150]).

These points, combined with the fact that code-based cryptography is one of the leading candidates for quantum-resistant cryptographic primitives, underscore the importance of the **problem of studying the security of code-based cryptosystems in the Hamming metric**, which is considered in the dissertation. To evaluate the security of a code-based cryptosystem, the following steps are generally performed:

1. *Assess the applicability of known attacks* against the cryptosystem. Any new cryptosystem should avoid known attacks.

2. *Assess the possibility of security reduction to known cryptosystems*. The security of any new cryptosystem should not be reducible to that of existing ones.

3. *Analyze the applicability of new cryptanalytic methods*.

There are two possibilities for an adversary to attack an asymmetric code-based encryption scheme: *message-recovery attacks* and *key-recovery attacks*. In message-recovery attacks, the adversary knows the public key and the encrypted message and aims to recover the plaintext *independently of the special properties or structure of the code used*. For code-based cryptosystems, this means the adversary attempts to decode a *random-looking* linear code from t errors. The most effective algorithms for solving this problem are *information-set decoding* [25; 33; 54; 66; 92; 93; 100; 136], which are enhancements of Prange's algorithm [118], and *statistical decoding* [134]. Despite these advanced techniques, the complexity remains exponential in both cases. Therefore, the risk of message-recovery attacks can be mitigated by selecting cryptosystem parameters such that the complexity of the best-known message-recovery attack aligns with the desired security level.

The most dangerous attacks are key-recovery attacks, which, if they exist, cannot be mitigated by choosing parameters. Key-recovery attacks aim to uncover enough of the secret key's structure from the public key by exploiting the special properties of the codes used and the vulnerabilities in their hiding mechanisms. Indeed, many practical codes possess strong algebraic structures (e.g., Reed-Solomon (RS) and Reed-Muller (RM) codes are polynomial evaluation codes) or combinatorial structures (e.g., majority-logic decodable and concatenated codes). If the hiding mechanism is not robust enough, these structures can be exploited to attack the secret key. Thus, key-recovery attacks typically leverage:

- *Algebraic properties of codes*. This includes the structure of Schur-Hadamard products [31; 43; 47; 50; 61; 62; 65; 113; 150] and automorphism groups [114; 129; 133].

- *Combinatorial properties of codes*. For instance, the concatenated structure [46; 130], or the distribution of low-weight codewords [51].

- *Linear algebraic properties of hiding mechanisms and codes*. Examples include [39; 52; 90].

The primary focus of cryptographic part of the dissertation is on key-recovery attacks as it is possible to leverage algebraic and combinatorial proprieties of codes. It should be noted that the degree of key recovery can be classified as follows (in decreasing order):

- *Full key-recovery attacks.* These attacks completely unmask the secret key, allowing an adversary to efficiently decrypt any message (see, e.g., [31; 43; 46; 47; 49; 50; 60–62; 65; 102; 113; 114; 133; 150]).
- *Partial key-recovery attacks.* These attacks allow an adversary to partially recover the secret key, which can then be used to reduce the complexity of message-recovery attacks (see, e.g., [46; 86]).
- *Distinguishers.* In this case, an adversary is able to distinguish a public code from a random one (see, e.g., [1; 65; 104; 148]). The existence of distinguishers does not directly imply the existence of partial and full key-recovery attacks; however, many cryptosystems have been broken by extending distinguishers. Thus, even the lowest degree of key recovery is highly undesirable.

Typically, an adversary conducts key-recovery attacks using only the public key. However, it is also possible to utilize additional information, such as side-channel leaks and collected decryption failures, to aid the attacks. Therefore, key-recovery attacks can be classified into: 1) *Attacks without hints*, and 2) *Attacks with hints*. A notable subclass of key-recovery attacks with hints is *reaction attacks*, which exploit decryption failures (e.g., attacks against HQC and QC-MDPC cryptosystems [74; 75; 109; 147]).

To conclude, the code-based cryptography is a very active research area, with many new cryptographic primitives and attacks appearing. Given the theoretical and practical importance of code-based cryptography, the research community has to carefully assess it for possible vulnerabilities.

2 The Goals and Research Objectives

In addressing the outlined problems, we set the following *goals* this dissertation:

1. Study the structure and properties (including cryptographic) of dihedral and metacyclic group codes;
2. Analyze the security of recently proposed code-based public-key encryption schemes.

To achieve these goals, the following *research objectives* are undertaken:

1. Study the algebraic structure of dihedral codes and their properties, including estimates of their parameters and decoding algorithms.
2. Study the algebraic structure of metacyclic group algebras and metacyclic codes, and obtain estimates of the parameters of metacyclic codes.
3. Study the applicability of dihedral and metacyclic codes in code-based cryptosystems.
4. Assess the security of cryptosystems based on quasi-cyclic and quasi-reproducible MDPC codes against reaction attacks.

5. Theoretically estimate the probability of decoding failure for regular non-binary MDPC codes for the selection of suitable parameters of semantically secure QC-MDPC cryptosystems.

6. Analyze the security of recently proposed asymmetric code-based cryptosystems based on subfield images of codes.

3 Contribution

The main contribution of this dissertation consists of the following:

1. Algebraic description of dihedral codes, including their duals and dihedral codes induced by cyclic codes; upper and lower bounds on the minimum code distance of dihedral codes; a decoding algorithm; and the structure of the Schur-Hadamard squares of dihedral codes.

2. The Wedderburn-like decomposition of finite metacyclic group algebras, algebraic description of metacyclic codes using this decomposition; representation of metacyclic codes as generalized concatenated codes; lower bounds on the minimum distance of metacyclic codes; exploiting the concatenated structure for building partial key-recovery attack on McEliece-type cryptosystems based on metacyclic codes.

3. Proof of the equivalence between permutation-based quasi-reproducible codes and quasi-group codes; reaction attack on cryptosystems based on quasi-group MDPC codes.

4. Theoretical estimates of the probability of decoding failure for non-binary MDPC codes; parameters for semantically secure cryptosystems based on these codes.

5. Two full key-recovery attacks on Ivanov-Krouk-Zyablov (IKZ) cryptosystem [80], and complexity estimates of message-recovery attacks against IKZ cryptosystem.

4 Scientific Novelty

All the aforementioned results are novel and have been independently obtained by the author. The contribution of the advisors consists in formulating the research problems and discussing the obtained results.

5 Research Methodology

In this dissertation, the study of group codes and their properties utilizes methods of linear algebra and classical coding theory, as well as ring theory and group representation theory (in particular, the Wedderburn decomposition of group algebras, and crossed product algebras). The analysis of the security of code-based cryptosystems employs algebraic methods, combinatorics, probability theory, and computer experiments.

6 Practical Significance

The practical significance of the dissertation's findings on dihedral and metacyclic codes, particularly in assessing their parameters and developing decoding algorithms, lies in the potential applications of these codes in communication schemes for error correction. Furthermore, the

dissertation's results concerning the structure of Schur-Hadamard squares of dihedral codes may find application in the construction of linear secret sharing schemes and secure multiparty computation protocols based thereon. The outcomes of constructing attacks on the Ivanov-Kruk-Zyablov cryptosystem and the cryptosystem based on quasi-group MDPC codes expand the spectrum of known cryptanalytic approaches and may prove valuable in developing standards for post-quantum cryptographic primitives. The theoretical estimates of decoding failure rate for regular non-binary MDPC codes directly facilitate the construction of semantically secure post-quantum cryptosystems based on these codes and may also be utilized in selecting codes for highly reliable communication systems.

7 Degree of Reliability

The reliability of the dissertation results is substantiated through rigorous mathematical proofs and, in several cases, validated by computer experiments. Furthermore, the primary findings have been published in peer-reviewed journals and presented at renowned conferences in the fields of algebra, coding theory, and code-based cryptography.

8 Publications

The results of this dissertation have been published in the following works: [138; 140–146]. The papers [138; 139; 141–144; 146] are included in journals and books indexed by Scopus and WoS, and the papers [139; 145] are included in journals recommended by the Higher Attestation Commission (VAK) for the publication of dissertation results.

9 Conferences

The results of this dissertation were presented at the following conferences:

- XVII International Conference «Algebra, Number Theory and Discrete Geometry» (2019, Russia, Tula);
- XVIII International Conference «Algebra, Number Theory and Discrete Geometry» (2020, Russia, Tula);
- XVII International Symposium Problems of Redundancy in Information and Control Systems REDUNDANCY 2021 (2021, Russia, Moscow);
- International Workshop on Code-Based Cryptography CBCrypto 2022 (2022, Norway, Trondheim);
- 8th Huawei Optical Workshop (2022, Russia, Kazan);
- International Workshop on Code-Based Cryptography CBCrypto 2023 (2023, France, Lyon);
- 9th Huawei Optical Workshop (2023, Russia, Saint-Petersburg);
- XVIII International Symposium Problems of Redundancy in Information and Control Systems REDUNDANCY 2023 (2023, Russia, Moscow).

10 Contents

Introduction states the problems considered in the dissertation, substantiates their relevance, provides a survey of related works, formulates goals, and outlines research objectives.

Chapter 1 develops the systematic theory of dihedral codes. Specifically, utilizing the Wedderburn decomposition of $\mathbb{F}_q D_{2n}$ obtained by F. Martinez in [35], we provide a comprehensive algebraic description of D_{2n}-codes, including their idempotent generators and bases. Additionally, an explicit description of dual codes is obtained, as well as a criterion of self-duality. We also study dihedral codes induced by cyclic codes and establish the connections between dihedral codes and cyclic codes. In particular, we obtain lower and upper bounds on the minimum distance of D_{2n}-codes and derive a decoding algorithm by leveraging induced codes. Furthermore, some examples of dihedral codes are provided. Motivated by cryptographic applications of Schur-Hadamard products and Schur-Hadamard squares of codes [42], we study products and squares of dihedral codes. Specifically, we have shown the strong algebraic structure of squares of dihedral codes. The last result implies that using dihedral codes in code-based McEliece-like encryption schemes is not desirable due to possible attacks. However, dihedral codes can have applications in other areas, as demonstrated by M. Borello et al. [29] in building efficient short-length quantum codes.

The results presented in this chapter, including the algebraic structure of dihedral codes, their idempotent generators, and induced codes, have been published in a series of papers [138; 139; 145; 146] in 2018–2020. The results on Schur-Hadamard products and squares of dihedral codes were published in [143] in 2021.

Chapter 2 continues our study of codes from non-abelian group algebras. Split metacyclic groups $G_{n,m,r}$ are defined by the following presentation

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

where $r^m \equiv 1 \pmod{n}$, and represent a natural generalization of dihedral groups. In this context, a natural task arises to generalize the results of the previous chapter to this broader class of groups. As demonstrated in the previous chapter, the Wedderburn decomposition of a group algebra into a direct sum of matrix algebras turns out to be a very powerful and convenient tool for studying group codes. However, the problem of explicitly constructing such a decomposition is non-trivial.

The contribution of this chapter is twofold. Firstly, an explicit Wedderburn-like decomposition of split metacyclic group algebras is provided with the only restriction being $\gcd(q, n) = 1$. Secondly, a systematic theory of split metacyclic codes is developed by leveraging this decomposition. Specifically, the algebraic structure of metacyclic codes is provided. The obtained structure has enabled the discovery of the generalized concatenated (GC) structure of metacyclic codes. It is established that metacyclic codes can be viewed as generalized concatenated codes, with inner codes being cyclic codes and outer codes being skew quasi-cyclic codes. Furthermore, the GC structure enabled the development of a partial key-recovery attack against cryptosystems based on *certain* metacyclic codes. Finally, the class of induced codes is studied, and estimates of the main parameters of metacyclic codes are obtained. *The results of this chapter were partly published in [140], the full version is accepted for the presentation at CBCrypto 2024.*

Chapter 3. Cryptosystems based on quasi–cyclic moderate density parity–check (QC–MDPC) codes are considered among the most perspective post–quantum public–key encryption schemes due to small public–key sizes and excellent performance. However, due to probabilistic decoding of MDPC codes, there is non–zero decryption failure rate. In 2016, Q. Guo, T. Johansson, P. Stankovski [75] showed that decryption failures can be used to construct a key–recovery attack against QC–MDPC cryptosystems. Recently, in order to mitigate GJS attack, P. Santini, E. Persichetti, and M. Baldi [126] proposed generalization of quasi–cyclic codes called quasi–reproducible (QR) codes and QR–MDPC cryptosystems. In this chapter, we consider cryptosystems that are based on quasi-group MDPC codes and propose a generalization of GJS reaction attack against these cryptosystems which exploits the group structure. We show that MDPC cryptosystems based on permutation-based quasi-reproducible codes with single-row signature proposed in [126], are indeed equivalent to quasi-group MDPC cryptosystems, thus implying the applicability of our attack to corresponding cryptosystems of [126] as well. It should be noted that other classes of binary reproducible and quasi-reproducible MDPC code-based cryptosystems are likely to have larger public keys and be less efficient compared to QC-MDPC cryptosystems with theoretically estimated DFR (see e.g. [7]). The results of this chapter were published in [141].

Chapter 4 is devoted to the study the decoding failure rate (DFR) of non-binary MDPC codes using theoretical tools, extending the results of previous binary QC-MDPC code studies. The theoretical estimates of the DFR are particularly significant for cryptographic applications of MDPC codes. Specifically, as mentioned above, exploiting decoding failures makes it possible to recover the secret key of a MDPC cryptosystem. This implies that to attain the desired security level against adversaries in the CCA2 model, the decoding failure rate must be strictly upper-bounded to be negligibly small.

In this chapter, we study the guaranteed error-correction capability of the one-step majority logic (OSML) decoder and provide a plausibility analysis of the single-iteration parallel symbol flipping decoder for non-binary MDPC codes. Through this analysis, we estimate the decoding failure rate of the combined use of these decoders, where parallel symbol flipping is employed to reduce the error weight to a level at which the OSML decoder can successfully correct any remaining errors. Consequently, we obtain worst-case estimates of the DFR, considering some reasonable assumptions. The accuracy and validity of our theoretical model is verified through numerical simulations. Finally, we suggest possible parameters of non-binary QC-MDPC cryptosystems for different NIST security levels, along with their theoretically estimated DFR.

It should be noted that the resulting key sizes are slightly larger than those in the binary case. However, the computational advantages of recent ISD algorithms usually don't scale well with increased field size, therefore it remains possible that non-binary codes may eventually match or surpass binary MDPC codes for cryptographic applications. The results of this chapter were published in [144].

Chapter 5. Recently, F. Ivanov, E. Krouk and V. Zyablov [80] proposed new cryptosystem based of Generalized Reed–Solomon (GRS) codes over field extensions. In their approach, the subfield images of GRS codes are masked by a special transform, so that the resulting public codes are not equivalent to subfield images of GRS codes but burst errors still can be decoded. In this chapter, it is shown that Ivanov-Krouk-Zyablov cryptosystem is insecure and its secret key can be recovered in polynomial time. Specifically, we propose two key-recovery attacks, with the first one being based on twisted squares, which were proposed in [48], and the second one being leveraging only linear algebra.

It should noted that the attack based on linear algebra can be generalized to recover the secret matrix Q even for other classes of codes. So, it appears that the masking transform used by Ivanov, Krouk and Zyablov is intrinsically insecure. It also seems that using hiding transforms that allow decoding error bursts cannot improve key sizes compared to classic approaches due to simplified message-recovery attacks based on information-set decoding. The results of this chapter were published in [142].

Conclusion of the dissertation recalls the main results of the dissertation and provides some concluding remarks.

This dissertation is the first to study the security of non-abelian group codes in code-based cryptosystems. The results of the dissertation indicate that the non-abelian structure (at least for the considered classes of groups) does not seem to increase the resistance of code-based cryptosystems to structural attacks. The results of the dissertation also revealed vulnerabilities in some advanced hiding mechanisms in McEliece encryption protocols.

In particular, *strong algebraic* structure of dihedral codes and their squares turns out to be a serious vulnerability, which allows *distinguishing* low-rate dihedral codes from random ones by leveraging squares. For metacyclic codes, their algebraic structure implies the existence of strong *combinatorial structure* (generalized concatenated decomposition) which allows applicability of known *partial key-recovery attack* of Puchinger et. al [46] to a large class of metacyclic codes. An attack against quasi-reproducible MDPC codes exemplifies the idea of security reduction to known (QG and QC-MDPC) cryptosystems to build a *a reaction attack*. The twisted-squares-based attack against IKZ cryptosystems can be also viewed as an example of security reduction to obtain *full key-recovery attack*. And finally, the second attack of Chapter 5, which is based on linear algebra and matrix distinguishability, exemplifies building new cryptanalitic methods.

Further research directions related to the stated problems may include: studying other classes of non-abelian group algebras and codes derived from them, as well as finding efficient subclasses of codes for various applications, including error correction in noisy channels and cryptography. It may also include developing and assessing the security of code-based cryptosystems and digital signatures.

References

1. A Distinguisher for High-Rate McEliece Cryptosystems / J.-C. Faugere [et al.] // IEEE Transactions on Information Theory. — 2013. — Vol. 59, no. 10. — P. 6830–6844. — ISSN 1557-9654. — DOI: 10.1109/tit.2013.2272036.
2. A new code-based public-key cryptosystem resistant to quantum computer attacks / E. Egorova [et al.] // Journal of Physics: Conference Series. — 2019. — Vol. 1163. — P. 012061. — ISSN 1742-6596. — DOI: 10.1088/1742-6596/1163/1/012061.
3. A variant of the McEliece cryptosystem with increased public key security / M. Baldi [et al.] // WCC 2011-Workshop on coding and cryptography. — 2011. — P. 173–182.
4. *Abbe E., Sandon C.* A proof that Reed-Muller codes achieve Shannon capacity on symmetric channels // 2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS). — IEEE, 2023. — DOI: 10.1109/focs57990.2023.00020.
5. Abelian Codes in Principal Ideal Group Algebras / S. Jitman [et al.] // IEEE Transactions on Information Theory. — 2013. — Vol. 59, no. 5. — P. 3046–3058. — ISSN 1557-9654. — DOI: 10.1109/tit.2012.2236383.

6. Algebraic decoding of cyclic codes: a polynomial ideal point of view / X. Chen [et al.] // Contemporary Mathematics. — 1994. — Vol. 168. — P. 15–15.
7. Analysis of the error correction capability of LDPC and MDPC codes under parallel bit-flipping decoding and application to cryptography / P. Santini [et al.] // IEEE Transactions on Communications. — 2020. — Vol. 68, no. 8. — P. 4648–4660.
8. *Assuena S.* Good codes from metacyclic groups II // Journal of Algebra and Its Applications. — 2020. — Vol. 21, no. 02. — ISSN 1793-6829. — DOI: 10.1142/s0219498822500402.
9. *Assuena S., Milies C. P.* Good codes from metacyclic groups // Contemp. Math. — 2019. — Vol. 727. — P. 39–49.
10. *Assuena S., Milies C. P.* Group algebras of metacyclic groups over finite fields // São Paulo Journal of Mathematical Sciences. — 2016. — Vol. 11, no. 1. — P. 46–52. — ISSN 2316-9028. — DOI: 10.1007/s40863-016-0043-7.
11. *Augot D., Betti E., Orsini E.* An introduction to linear and cyclic codes // Gröbner Bases, Coding, and Cryptography. — 2009. — P. 47–68.
12. Automorphism ensemble decoding of quasi-cyclic LDPC codes by breaking graph symmetries / M. Geiselhart [et al.] // IEEE Communications Letters. — 2022. — Vol. 26, no. 8. — P. 1705–1709.
13. Automorphism ensemble decoding of Reed-Muller codes / M. Geiselhart [et al.] // IEEE Transactions on Communications. — 2021. — Vol. 69, no. 10. — P. 6424–6438.
14. *Bakshi G. K., Gupta S., Passi I. B. S.* The Algebraic Structure of Finite Metabelian Group Algebras // Communications in Algebra. — 2015. — Vol. 43, no. 6. — P. 2240–2257. — ISSN 1532-4125. — DOI: 10.1080/00927872.2014.888566.
15. *Bazzi L., Mitter S.* Some randomized code constructions from group actions // IEEE Transactions on Information Theory. — 2006. — Vol. 52, no. 7. — P. 3210–3219. — ISSN 0018-9448. — DOI: 10.1109/tit.2006.876244.
16. *Berger T. P., Loidreau P.* How to mask the structure of codes for a cryptographic use // Designs, Codes and Cryptography. — 2005. — Vol. 35. — P. 63–79.
17. *Berman S. D.* On the theory of group codes // Cybernetics. — 1969. — Vol. 3, no. 1. — P. 25–31. — ISSN 1573-8337. — DOI: 10.1007/bf01072842.
18. *Berman S. D.* Semisimple cyclic and Abelian codes. II // Cybernetics. — 1970. — Vol. 3, no. 3. — P. 17–23. — ISSN 1573-8337. — DOI: 10.1007/bf01119999.
19. *Bernal J. J., Guerreiro M., Simon J. J.* From ds-Bounds for Cyclic Codes to True Minimum Distance for Abelian Codes // IEEE Transactions on Information Theory. — 2019. — Vol. 65, no. 3. — P. 1752–1763. — ISSN 1557-9654. — DOI: 10.1109/tit.2018.2868446.
20. *Bernal J. J., Bueno-Carreno D. H., Simon J. J.* Computing the Camion's multivariate BCH bound // 2013 IEEE Information Theory Workshop (ITW). — IEEE, 2013. — DOI: 10.1109/itw.2013.6691285.
21. *Bernal J. J., Rio A. del, Simon J. J.* An intrinsical description of group codes // Designs, Codes and Cryptography. — 2009. — Vol. 51, no. 3. — P. 289–300. — ISSN 1573-7586. — DOI: 10.1007/s10623-008-9261-z.
22. *Bernal J. J., Bueno-Carreño D. H., Simón J. J.* Constructions of Abelian Codes Multiplying Dimension of Cyclic Codes // Mathematics in Computer Science. — 2019. — Vol. 14, no. 2. — P. 415–421. — ISSN 1661-8289. — DOI: 10.1007/s11786-019-00416-5.

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

24. *Bernstein D. J.*, *Lange T.* Post-quantum cryptography // Nature. — 2017. — Vol. 549, no. 7671. — P. 188–194.

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

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

27. *Blokh È. L.*, *Zyablov V. V.* Coding of generalized concatenated codes // Problemy Peredachi Informatsii. — 1974. — Vol. 10, no. 3. — P. 45–50.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

45. Classic McEliece: conservative code-based cryptography / D. J. Bernstein [et al.] // NIST submissions. — 2017. — Vol. 1, no. 1. — P. 1–25.

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

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

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

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

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

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

52. Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko Cryptosystems / Y. Lee [et al.] // IEEE Communications Letters. — 2020. — Vol. 24, no. 12. — P. 2678–2681. — ISSN 2373-7891. — DOI: 10.1109/lcomm.2020.3019054.

53. Cyclotomic idempotent-based binary cyclic codes / C. Tjhai [et al.] // Electronics Letters. — 2005. — Vol. 41, no. 6. — P. 341. — ISSN 0013-5194. — DOI: 10.1049/el:20057266.

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

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

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

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

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

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

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

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

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

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

64. *Ding C.*, *Li C.* BCH cyclic codes // Discrete Mathematics. — 2024. — Vol. 347, no. 5. — P. 113918.

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

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

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

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

69. Enhancing Iterative Decoding of Cyclic LDPC Codes Using Their Automorphism Groups / C. Chen [et al.] // IEEE Transactions on Communications. — 2013. — Vol. 61, no. 6. — P. 2128–2137. — ISSN 0090-6778. — DOI: 10.1109/tcomm.2013.032713.120050.

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

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

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

73. GROUP CODES OVER NON-ABELIAN GROUPS / C. G. PILLADO [et al.] // Journal of Algebra and Its Applications. — 2013. — Vol. 12, no. 07. — P. 1350037. — ISSN 1793-6829. — DOI: 10.1142/s0219498813500370.

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

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

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

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

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

79. Ideal representation of Reed–Solomon and Reed–Muller codes / E. Couselo [et al.] // Algebra and Logic. — 2012. — Vol. 51, no. 3. — P. 195–212. — ISSN 1573-8302. — DOI: 10.1007/s10469-012-9183-8.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

108. *Niederreiter H.* Knapsack-type cryptosystems and algebraic coding theory // Prob. Contr. Inform. Theory. — 1986. — Vol. 15, no. 2. — P. 157–166.

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

110. Non-Abelian Group Codes over an Arbitrary Finite Field / C. García Pillado [et al.] // Journal of Mathematical Sciences. — 2017. — Vol. 223, no. 5. — P. 504–507. — ISSN 1573-8795. — DOI: 10.1007/s10958-017-3363-y.

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

112. On a Class of Left Metacyclic Codes / Y. Cao [et al.] // IEEE Transactions on Information Theory. — 2016. — Vol. 62, no. 12. — P. 6786–6799. — ISSN 1557-9654. — DOI: 10.1109/tit.2016.2613115.

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

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

115. *Peterson W. W.*, *Brown D. T.* Cyclic codes for error detection // Proceedings of the IRE. — 1961. — Vol. 49, no. 1. — P. 228–235.

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

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

118. *Prange E.* The use of information sets in decoding cyclic codes // IRE Transactions on Information Theory. — 1962. — Vol. 8, no. 5. — P. 5–9.

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

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

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

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

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

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

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

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

127. Security of generalised Reed-Solomon code-based cryptosystems / M. Baldi [et al.] // IET Information Security. — 2019. — Vol. 13, no. 4. — P. 404–410.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

149. When are all group codes of a noncommutative group Abelian (a computational approach)? / C. G. Pillado [et al.] // Journal of Mathematical Sciences. — 2012. — Vol. 186, no. 4. — P. 578–585. — ISSN 1573-8795. — DOI: 10.1007/s10958-012-1006-x.

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

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

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