Preface

The theory of quasigroups, often referred as "non-associative groups", stands as one of the oldest branches of algebra and combinatorics. Dating back to the nineteenth century, it appears in the form of Latin squares, as evidenced by a seminal paper published by Euler [47]. However, throughout the twentieth century, it was overshadowed by its subset, the theory of groups, to such an extent that in *Mathematical Reviews*, loops and quasigroups were merely classified as "other generalizations of groups". This predominance of group theory can primarily be attributed to the fact that abstract groups readily allow representation, either linearly through matrices and modules or as symmetries in the form of permutation representations.

Applications of quasigroups in coding theory and cryptography have evolved rapidly and garnered significant attention from researchers in these fields. Quasigroups are extensively employed in designing codes that can detect and correct errors [12, 13, 59] in noisy channels. It is also utilized in designing special codes like MDS codes [1, 29]. Similarly, quasigroups find wide applications in designing different cryptographic primitives [116], including S-boxes, block ciphers, stream ciphers, hash functions, secret sharing schemes, zero-knowledge protocols, message authentication codes (MAC), identity-based cryptosystems, etc. Several of these applications are discussed in this thesis. This thesis aims to provide a comprehensive understanding of quasigroup applications in coding theory and cryptography. It consists five chapters, including an introduction and conclusion.

The introduction explores the concept of quasigroups and their applications through a comprehensive literature review. It will also articulate the motivation and objective of the thesis.

Chapter 1 serves as an introductory overview, presenting fundamental concepts in quasigroups, coding theory, and cryptography which are essential for comprehending the thesis. It delves into the quasigroup string transformations, representing finite quasigroups as vector valued Boolean functions, classifications of quasigroups applicable to cryptographic primitives and coding theory. The brief introductions of multivariate polynomial equations and multivariate public-key cryptosystem (MPKC) are also included in the chapter.

In Chapter 2, we introduce a novel check block system based on T-quasigroups. For its construction, we utilize a Frobenius field automorphism of $\mathbb{F}_{p^n}/\mathbb{F}_p$, where $n \geq 2$ and p is an odd prime. We analyze its error detecting capabilities, including the conditions under which it can detect k-jump transposition errors, k-jump twin errors and phonetic errors within erroneous codewords in blocks over the base field. On the similar arguments, we use a group automorphism of $(\mathbb{F}_p, +)$ to construct a check character system and analyze its error detection capabilities. Furthermore, we conduct a comparative analysis between the proposed check block system and Reed-Solomon (RS) codes, showing its superior efficiency in terms of the maximum number of operations required to detect single error. Our system can be implemented in various real-life applications, including ISBN, SSN, and bank routing numbers.

The orthogonality of quasigroups and the concept of i-invertibility of k-ary operations find extensive applications in the development of MDS codes, particularly with dimension 2 and 3 [1, 29]. In Chapter 3, our focus will be on the construction of an MDS code that are dependent on the generalization of i-invertibility of quasigroups, known as extended-i-invertibility of k-ary operations over Q, where Q is an arbitrary finite set. Initially, we define the notion of extended-i-invertibility of k-ary operations over Q^2 using k-ary operations over Q. Subsequently, we present several important results concerning the orthogonal system of k-ary operations over Q^2. Finally, we propose a novel construction method for the MDS codes.

In Chapter 4, we introduce a symmetric encryption scheme, namely *SEBQ*, utilizing quasigroups. SEBQ employs an inherent chaining-like mode of operation, where transformed vectors will be used instead of cipher blocks to encrypt subsequent message blocks. We will prove that SEBQ scheme is secure against indistinguishability under chosen plaintext attack (IND-CPA) and after applying the unbalanced Fiestel transformation, it achieves IND-CCA2 security. To evaluate the randomness of the SEBQ scheme, we conduct an experiment by running the NIST-STS test suite on the generated ciphertext. We compare the results with existing encryption schemes like INRU [122], BCWST [21] and AES-128. Additionally, we analyze the avalanche effect of the secret key, plaintext and random initial vector within the SEBQ scheme. Furthermore, we determine the computational complexity of SEBQ in terms of the number of operations required to encrypt and decrypt a given message. Finally, we ascertain the order of Latin squares which is required to achieve 128-bit and 256-bit security in SEBQ against known-ciphertext attack.

In Chapter 5, we introduce a digital signature scheme, called MQQ-Sigv, whose security relies on the complexity of solving the system of multivariate polynomial

equations over the finite field. The MQQ-Sigv signature scheme belongs to the category of multivariate polynomials based public key cryptography, which has been demonstrated to offer "quantum - secure" digital signature capabilities. To construct the central map of the proposed scheme, we employ the vinegar variation of the bilinear MQQ and provide an efficient algorithm for finding an inverse of the central map. We prove that the MQQ-Sigv signature scheme is secure against Direct attack, Min-rank attack, High-rank attack and Existential unforgeability under chosen message attack. Moreover, we show that after applying the transformation proposed by Wang et al. [126], it becomes computationally infeasible to find an equivalent good key in polynomial time. The primary drawback of multivariate polynomials based public key cryptographic primitives is the large size of secret and public keys. To address this issue, we design the secret key using Toeplitz matrices [65] instead of random matrices and employ minus modifier variation to minimize the public key size. Finally, we analyze the operational characteristics of MQQ-Sigv signature scheme in terms of key size and signature size. We compare these aspects of the MQQ-Sigv scheme with MQQ-SIG scheme [61] and Rainbow scheme [126].

At the end, we draw the conclusion of the thesis and summarize the findings. Subsequently, we outline the future research directions in this subject area. We also highlight the implications of our research and suggest potential areas for further exploration and development.

Keywords: quasigroup; loops; string transformation; parastrophe; T-quasigroup; error-detecting codes; ISBN codes; orthogonality of quasigroups; k-recursive codes; MDS codes; symmetric encryption scheme; IND-CPA, IND-CCA2; multivariate quadratic quasigroups (MQQ); MQQ-SIG; MQQ-ENC; signature scheme.