DESIGN AND ANALYSIS OF SOME NEW CODES AND CRYPTO SCHEMES USING QUASIGROUPS

Thesis submitted in partial fulfillment for the award of degree

DOCTOR OF PHILOSOPHY

IN

MATHEMATICAL SCIENCES

BY

SATISH KUMAR

DEPARTMENT OF MATHEMATICAL SCIENCES
INDIAN INSTITUTE OF TECHNOLOGY
(BANARAS HINDU UNIVERSITY)
VARANASI – 221005
INDIA

Roll No. 18121501 April, 2024

Conclusion and future research directions

This thesis focuses on the design and analysis of specialized codes and cryptographic primitives derived from the structure of quasigroups. The overall conclusion of the thesis can be summarized as follows:

- Firstly, we introduced an innovative check block/character system based on T-quasigroups using the Frobenius field automorphism $\mathbb{F}_{p^n}/\mathbb{F}_p$, where $n \geq 2$ and p is an odd prime. We assessed the error-detecting capabilities of the proposed check block system and analyzed the conditions under which it can detect k-jump transposition errors, k-jump twin errors and phonetic errors in an erroneous codeword. Following the similar approach, we proposed a check character system based on $(p-1)$-T-quasigroups using the group automorphism of $(\mathbb{F}_p, +)$ and analyzed its error-detecting capabilities. We proved that the proposed check block system is efficient than the Reed-Solomon code to detect a single position error. Furthermore, we have shown that the proposed systems can be used at various real world applications similar to ISBN, SSN and bank routing numbers.

- Subsequently, we proposed techniques to utilize orthogonality of quasigroups in novel construction of MDS codes. We defined the notion of extended-i-invertibility of k-ary operation over an arbitrary finite set Q and provided several results concerning the orthogonality of a system of k-ary operations over Q^2. Utilizing the strong orthogonality of a system of k-ary quasigroup operations, we proposed a method for construction of MDS codes. We provided a few examples to support the results of our theory and thereby constructed MDS codes of dimension 2 and 3.

After exploring the applications of quasigroups in coding theory, we further studied the construction of cryptographic algorithms. Towards this, we proposed a symmetric key encryption scheme and a public key digital signature scheme.

- We introduced a symmetric key encryption scheme called *SEBQ*, employing

a chaining-like mode of operation. Unlike traditional chaining mode of operations (CFB, CBC, OFB, etc.), proposed scheme utilizes transformed initial vectors to encrypt subsequent blocks instead of the preceeding ciphertext block. This innovative approach reduces memory usage and computational resources making it suitable for constrained environments [21, 122, 131]. We proved that our scheme is indistinguishable against adaptive chosen ciphertext attack using Feistel transformations. Additionally, we evaluated the randomness of the ciphertext by examining the results obtained by NIST-STS test suite [4] and analysed the avalanche criteria. Furthermore, we compared the computational complexity of our scheme with the existing ones like INRU [122] and BCWST [21]. We also determined the order of Latin square required to achieve 128-bit and 256-bit security against known-ciphertext attack in the proposed scheme.

- Finally, we aimed to design a quantum secure digital signature scheme using multivariate quadratic quasigroup (MQQ). For this, we constructed MQQ using general quasigroup $(Q, *)$ of order 2^d for $d \geq 2$, and explored efficient methods to find their parastrophes. Then, we discussed the construction of public multivariate quadratic polynomials utilizing bilinear MQQ. Thereafter, we proposed a MQQ based digital signature scheme. Furthermore, we proved that the scheme is secure against direct attack, Min-rank attack, High-rank attack and EUF-CMA attack. Utilizing the methodology outlined by Wang et al. [126], we proved that finding an equivalent good key in polynomial time is not feasible for the proposed scheme. We also included the operational characteristics of the proposed signature scheme, highlighting its efficiency and robustness in practical cryptographic applications.

Directions for future research:

- The scope of our study could be broadened by exploring different values of p and n to obtain optimal codes over n-T-quasigroups of order p^n that can detect all types of double errors. Furthermore, the construction of new error correcting systems using quasigroups represents an open and intriguing area of research with wide mathematical applications.

- The work in Chapter 3 can be expanded in the future by considering codes with higher dimensions. We can find the suitable conditions under which proposed codes possess properties like near MDS (NMDS), almost MDS (AMDS) or LCD. Moreover, the construction of error-correcting codes based on quasigroup remains an open research problem and can be envisioned as a future task.

- The $\mathfrak{e}$ and $\mathfrak{d}$ string transformations based on quasigroups as defined in Chapter 4 play a crucial role in designing a secure cryptographic algorithms. The security of the existing quasigroup based encryption schemes can be improved by using more than one quasigroup. Also this can be achieved by applying these string transformations for more than one round of encryption or decryption with different initial vectors [21]. The research community may design S-boxes and block ciphers using different choices of quasigroups and quasigroup string transformations as per their requirements.

- Following the work of Chapter 5, researchers may design a public key encryption scheme based on the proposed algebraic structures or central map. The analysis and optimized implementation of the existing MQQ based cryptographic schemes can be a part of future work.

Mathematicians worldwide are progressively recognizing the potential of quasigroups in designing various mathematical primitives. Significant research efforts are undergoing for the construction of cryptographic primitives and algebraic codes utilizing quasigroups. Quasigroups have indeed proven to be useful tools for enhancing security of cryptographic protocols that are not only easy to implement but also demand minimal silicon area [116]. Beyond the primitives discussed in this thesis, literature presents numerous other primitives such as MACs, quasigroup-based secret sharing schemes, zero-knowledge protocols, the generation of NLPN-sequences, identity-based cryptosystems, etc. [31–35, 75, 116]. An analysis of these primitives may inspire further work toward their efficiency enhancement.