Designing a Public-Key Cryptosystem Using Graph Partitioning into Perfect Matching

Jane Shonon Cutinha[1,*], Sabitha D'Souza[1], and Swati Nayak[1]

[1]Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India-576104

janecutinha21@gmail.com, sabitha.dsouza@manipal.edu, swati.nayak@manipal.edu

Abstract

Cryptography serves as the backbone of modern digital security, protecting sensitive information across electronic communication and transactions. The rapid advancement of computational capabilities poses a threat to classical cryptographic systems, necessitating the development of more secure alternatives. We propose a novel graph-based public key encryption scheme that leverages the hardness of partitioning a 4-regular graph into four disjoint subsets, such that each induced subgraph is a perfect matching. The scheme encodes plaintexts as multivariate polynomials over edge variables using a recursive encoding structure. We provide a comprehensive security analysis demonstrating that the scheme is resilient against key recovery, ciphertext search, and plaintext search attacks.

Keywords— Graph-based encryption, graph partitioning, perfect matching, public key encryption

*presenting author