Dynamic Coprime Labeling: A Novel Framework for Cryptographic Safe Prime Generation on k-Uniform Hypergraphs

Tonapi, Anushka (School: Alpine Public School)

Classical graph coprime labelings given by Gallian (2009) are static and unchanging, thus inadaptable to real-world systems. We introduce dynamic coprime labeling (DCL), a novel extension of coprime labeling for time-sensitive networks, that maintains relative coprimality among adjacent vertices as the graph evolves over time. The definition of coprime labeling is extended to an injective labeling function, a time variable, and a transformation function. We characterize families of coprime-preserving transformations and provide proofs for paths, wheels, cycles, and the n-hypercube. We introduce two classes of coprime-preserving transformations and present an interesting application of DCL to Carmichael's theorem. Further, we analyze DCL from a computational perspective and improve upon existing algorithms for minimal coprime labeling. We offer a creative application to cryptographic safe prime generation wherein we implement a DCL on a k-uniform hypergraph and perform entropy extraction from CSPRNG, apply SHA-256 on the seed values, use a division sieve and run Miller-Rabin to measure the success rate of generating Sophie Germain primes. Berlekamp-Massey is implemented to measure the resistance of the framework to LFSR-based prediction, and we use the security definition of a formal indistinguishability game to check the DCL framework's resistance to five attack vectors: brute force, preimage resistance, collision resistance, timing side-channel analysis and statistical quality assessment via the NIST SP 800-22. We find that the framework passes fourteen NIST tests, and cryptanalysis results show that our framework has a High overall security level. These results establish DCL as a rigorous framework for further algorithmic and applied investigations.

Awards Won: