Approximation Theory and Special Functions
ATSF 2026 Conference - 9th Series
September 2-5, 2026, Ankara - Türkiye

Optimizing Graph Path Encoding with Probabilistic Cryptography

Gökçe Çaylak Kayaturan

Ordu University, Department of Mathematics, Ordu, Türkiye
e-mail: gokcekayaturan@odu.edu.tr

Abstract

As network architectures grow in complexity, the need for efficient and private path verification becomes paramount. This paper proposes a novel framework for encoding graph paths using binary arrays integrated with ElGamal encryption to ensure both space efficiency and cryptographic security. By representing a sequence of edges or nodes as elements within a probabilistic filter, we achieve constant-time membership queries while significantly reducing the overhead associated with traditional path logging.

To address privacy concerns and prevent unauthorized path reconstruction, we utilize the homomorphic properties of the ElGamal cryptosystem. In this model, the bit array is constructed within the encrypted domain, or the indices are generated via ElGamal-signed identifiers. This ensures that an intermediate observer cannot determine the specific edges of a path without the corresponding private key, effectively mitigating traffic analysis attacks.

In the literature, to improve privacy protection and secure communications between parties, Diffie-Hellman key exchange protocol has been used [1]. Alternatively, we believe that the ElGamal encryption system also works perfectly with binary set representation methods for the same purpose for large-scale graph topologies. This research contributes a scalable solution for secure source routing and verifiable telemetry in decentralized networks.

Keywords: Network, ElGamal Encryption, Diffie-Hellman key exchange, graph.

References:

[1] N. Ahmed, R. A Michelin, W. Xue, G. D. Putra, S. Ruj, S. S Kanhere and S. Jha, DIMY: Enabling privacy-preserving contact tracing. J. Network Computer Appl. 202 (2022), Article No. 103356, 14 pp.