

**Summary of the US Patent titled Structure-Preserving Subgraph Queries (US Patent No. 62170122) by Dr. Byron Choi and Mr. Zhe Fan**

Graphs are powerful tools for a wide range of real applications, from biological and chemical databases, social networks, citation networks to information networks. Large graph data repositories have been consistently found in recent applications.

Subgraph query (via subgraph isomorphism), which is a fundamental and powerful query in various real graph applications, has actively been investigated for performance enhancements recently. However, due to the high complexity of subgraph query, hosting efficient subgraph query services has been a technically challenging task, because the owners of graph data may not always possess the information technology (IT) expertise to offer such services and hence may outsource to query service providers (SP).

Unfortunately, as SPs may not always be trusted, security (such as the confidentiality of messages exchanged) has been recognized as one of the critical attributes of Quality of Services (QoS). This directly influences the willingness of both data owners and query clients to use SP's services.

Therefore, it is an objective of the present invention is to provide solution to structure-preserving subgraph queries that is both efficient and private. The present invention solves structure preservations at two levels. The first level is termed structure-preserving subgraph query processing (SPQP) which preserves the structures of both subgraph queries and data graphs. The second level is termed asymmetric structure-preserving subgraph query processing (ASPQP) which preserves only the structure of subgraph queries. The present invention relates to solving the issues related to subgraph query services with tunable preservation of privacy of structural information. More particularly, it relates to a novel cyclic group based encryption (CGBE) method for private matrix operations.