Computer Science
Seminar

Geometric Range Search over Encrypted Spatial Data

Ming Li
University of Arizona

Abstract: Geometric range search is a fundamental primitive for spatial data analysis in SQL and NoSQL databases. It has extensive applications in Location-Based Services, computer-aided design and computational geometry. Due to the dramatic increase of data size, it is necessary for companies and organizations to outsource their spatial datasets to third-party cloud services (e.g. Amazon) in order to reduce storage and query processing costs, but meanwhile with the promise of no privacy leakage to the third party. Searchable encryption is a technique to perform meaningful queries on encrypted data without revealing privacy. However, geometric range search on spatial data has not been fully investigated nor supported by existing searchable encryption schemes. The main challenge, is that compute-and-then-compare operations required by many range search algorithms cannot be supported by any existing crypto primitives. In this talk, I will present our recent research progresses in privacy-preserving geometric range search over encrypted spatial data. The general approach is to adopt new representations of spatial data, and transform the range query algorithm to avoid compute-and-then-compare operations, so that existing efficient crypto primitives can be integrated. I will present two designs, the first one focuses on circular range search, and the second one can handle arbitrary geometric range query and is more efficient. The security of both schemes are formally proven under standard cryptographic assumptions. Finally, I will discuss some future research challenges and directions in this area.

Friday, November 6, 2015, 3:00 pm
Mathematics and Science Center: W303

Mathematics and Computer Science
Emory University