Secure Search of Encrypted Cloud Data

(No. T4-1840)

Principal investigator

Moni Naor

Faculty of Mathematics and Computer Science
Department of Computer Science and Applied Mathematics

Summary

Searchable symmetric encryption with practical big-data performance and strong security
Highlights
Outsourcing data storage to remote servers offers invaluable benefits while introducing many concerns when dealing with sensitive data. In the presence of potentially-vulnerable servers, strong user-side encryption preserves the confidentiality of the data but renders essential operations (such as keyword search) extremely expensive and sometimes even unfeasible. To overcome this problem, the cryptography and security community has developed various searchable symmetric encryption (SSE) methods that enable searching through encrypted data without revealing any unnecessary information. However, despite the rapidly increasing commercial interest in SSE technology, it has been shown that the performance of the existing methods scales badly to big data, not due to their usage of expressive cryptographic tools, but rather due to their poor data locality. Practical big-data performance and strong security are the two most essential ingredients for unleashing the potential of SSE technology, but have so far emerged as two extremely conflicting goals.
Our Innovation
The first searchable symmetric encryption (SSE) method that offers practical big-data performance while guaranteeing strong security. The method can be based on any off-the- shelf block cipher and enjoys essentially optimal space and communication overheads together with near-optimal data locality.
Key Features
Â·Â Â Â Â Â Â Â Â A breakthrough combination of cryptographic and algorithmic techniques
Â·Â Â Â Â Â Â Â Â Significant improvements over previous SSE systems in both security and performance
Â·Â Â Â Â Â Â Â Â Practical big-data performance
Â·Â Â Â Â Â Â Â Â Strong and precise security guarantees
Â·Â Â Â Â Â Â Â Â Low-cost implementation given any off-the- shelf block cipher
Development Milestones
Â·Â Â Â Â Â Â Â Â Research complete and technology ready for commercialization
The Opportunity
Market research firm â€˜Markets and Marketsâ€™ projects that the global Cloud security market will grow from $4.20 billion in 2014 to $8.71 billion in 2019, representing an estimated compound annual growth rate (CAGR) of 15.7% from 2014 to 2019.

Patent Status

USA Granted: 10,331,913