عنوان مقاله:

Multi-User Searchable Encryption Scheme with General Access Structure

محل انتشار:

دومین کنفرانس بین المللی مهندسی دانش بنیان و نوآوری (سال: 1394)

تعداد صفحات اصل مقاله: 7

نویسندگان:

KOBRA AMIRI ZIRTOL - *Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran*

MAHNAZ NOROOZI - *Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran*

ZIBA ESLAMI - *Department of Computer Science, Shahid Beheshti University, G.C., Tehran, Iran Cyberspace Research Center, Shahid Beheshti University, Tehran, Iran*

خلاصه مقاله:

Searchable encryption is a cryptographic primitive that enables searching over encrypted data. Think over an organization that has outsourced its encrypted database. Consider the scenario in which each member of this organization can add encrypted data to the database but accessing the data is limited to certain predefined access structure. That is, only the members of authorized subsets of members can collaborate to search for a desired data and then decrypt the received ciphertexts. In this paper, we construct a scheme that enables such a scenario and supports general access structure

کلمات کلیدی:

searchable encryption; multi-user; general access structure

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/553271