Multi-User Searchable Encryption Scheme for Text Document

Chia-Chi Wu\(^1\) --- Iuon-Chang Lin\(^2\) --- Ya-Hui Liu\(^3\)

\(^1\)National Defense University, , Taoyuan, R.O.C.
\(^2\)Department of Management Information Systems, Nation Chung Hsing University Taichung, Taiwan R.O.C; Department of Photonics and Communication Engineering, Asia University, Taichung, Taiwan, R.O.C.
\(^3\)Department of Management Information Systems, Nation Chung Hsing University Taichung, Taiwan R.O.C

Abstract

We improve the previous method to add the function of user revocation in this scheme. When document owner doesn’t want to share someone he had shared, he can revoke the user who can’t retrieve the specific document. More importantly, the revocation process must not affect other authorized users, the scheme has to keep a low maintenance cost.

Keywords: Multi-User, Searchable Encryption.