Abstract

Anonymity is one of the important services that must be available to users in the digital world as long as they behave honestly. Users’ communication must be kept authenticated and anonymous unless malicious behaviors are detected. In this case the accused user’s clear identity must be traced and revealed by the system to solve accusations. Enterprise Digital Rights Management (E-DRM) protects business digital applications by allowing an author in an organization to securely upload his confidential package/file(s) and store the contents in a private way on secure servers. This is done in a way that – later – allows an authorized user who is able to prove his authorization for the package to an authorization authority to download and use these contents in a private way. In this paper, we extend our previously proposed E-DRM protocols and propose an E-DRM protocol that allows authorized users to upload, store and download packages in an efficiently secure, anonymous and authenticated way. On the other hand, in case of an accusation or a dispute, our system is able to trace the user to his clear identity to solve accusations.
References


Index Terms

Computer Science

Information Sciences

Keywords
Enterprise security, Digital rights management, Anonymity, Traceability, Threshold cryptography, Authentication, Group signatures