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

Secure Anonymously Authenticated and Traceable Enterprise DRM System


33. Mark Manulis, Ahmad-Reza Sadeghi, and Jrg Schwenk. Linkable democratic group
signatures. In Kefei Chen, Robert Deng, Xuejia Lai, and Jianying Zhou, editors, Information
Security Practice and Experience, volume 3903 of Lecture Notes in Computer Science, pages
34. Deirdre K Mulligan, John Han, and Aaron J Burstein. How drm-based content delivery
systems disrupt expectations of personal use. In Proceedings of the 3rd ACM workshop on
35. Jaehong Park, Ravi Sandhu, and James Schifalacqua. Security architectures for
36. Torben P. Pedersen. Non-interactive and informationtheoretic secure verifiable secret
sharing. In Proceedings of the 11th Annual International Cryptology Conference on Advances in
37. Michael O. Rabin. Efficient dispersal of information for security, load balancing, and fault
38. Jason K. Resch and James S. Plank. Aont-rs: Blending security and performance in
dispersed storage systems. In Proceedings of the 9th USENIX Conference on File and Storage
7th international conference on the theory and application of cryptology and information
42. Ahmed H. Soliman, Maged H. Ibrahim, and Adel E. El- Hennawy. Improving security and
efficiency of enterprise digital rights management. In proceedings of the 6th IEEE International
IEEE, 2015.
Annual ACM Symposium on Theory of Computing, STOC ’03, pages 116–125, New York, NY,
USA, 2003. ACM.
44. L.R. Welch and E.R. Berlekamp. Error correction for algebraic block codes, dec 30
45. Yang Yu and Tzi-cker Chiueh. Enterprise digital rights management: Solutions against

Index Terms

Computer Science

Information Sciences

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