Abstract

Signcryption is a cryptography primitive that fulfills both the functions of digital signature and encryption and guarantees non-repudiation, confidentiality and integrity in a more efficient way. In this paper, we propose an efficient and secure identity based multi-proxy multi signcryption scheme from bilinear pairings. In this scheme a group of proxy signcoters could authorize by a group of original signcoters. Then multi proxy multi signcryption could generate by the cooperation of all signcoters in the proxy group.

References


8. Y. Zheng: Digital signcryption or how to achieve cost (signature & encryption)


Index Terms

Computer Science Information Sciences

Keywords

Bilinear Pairings, Identity-based Cryptography, Signcryption, Proxy Signature, Multi Proxy Multi Signcryption