Abstract

This paper presents public verifiable identity based multi-proxy multi-signcryption scheme from pairings. In this scheme a proxy signcrypter group could authorized as a proxy agent by the cooperation of all members in the original signcrypter group. Then the proxy signcryption can be generated by the cooperation of all the signcrypters in the authorized proxy signcrypter group on the behalf of the original signcrypter group. As compared to the scheme Liu and Xiao, the proposed scheme provides public verifiability of the signature along with simplified key management.

References


9. Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption)


Index Terms

Computer Science Pattern Recognition

Keywords

Bilinear pairings, Identity-based cryptography, ID based Signcryption, multi signature, proxy signature.