An Efficient Identity based Multi-Proxy Multi-Signcryption Scheme from Bilinear Pairings

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 151
Number 6

Year of Publication: 2016

Authors:
Tej Singh, Rashid Ali, Musharraf Ali

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 signcypers could authorize by a group of original signcypers. Then multi proxy multi signcryption could generate by the cooperation of all signcypers 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