Abstract

In a proxy signature scheme, a user delegates his/her signing capability to another user in such a way that the latter can sign messages on behalf of the former. Proxy signature helps the proxy signer to sign messages on behalf of the original signer. It is very useful when the original signer is not available to sign a specific document. In this paper, we propose a secure an identity based proxy signature scheme from bilinear pairings. The proposed scheme satisfy all the security property of proxy signature scheme.

References

A Secure ID-based Proxy Signature Scheme from Bilinear Pairings

CRYPTO01, volume 2139 of LNCS, pages 213229. Springer-Verlag, 2001


Index Terms

Computer Science  Networks
Keywords

Proxy Signature, Bilinear Pairings, ID-Based Cryptography