Abstract

This paper presents an improved proxy blind signature scheme with forward security mechanism. The proposed digital signature scheme combines the two special-purpose signature schemes, blind signature and proxy signature. In this signature scheme, the original signer gives authority to another entity which is known as a proxy signer, but without having any idea about the content of the document. This paper proposes an enhanced proxy blind signature, in which the forward security is incorporated and the security of the signature scheme relies on the discrete logarithm problem (DLP). Forward security mechanism will provide protection to the system from the key leakage or key exposure, because in this mechanism, the private key of proxy signer is updated periodically. In case if the signature key at some stage is compromised, the adversary cannot be able to forge signatures as if they had been generated before the exposure or leakage of key.

References

An Improved Proxy Blind Signature Scheme with Forward Security


Index Terms

Computer Science
Security
Keywords
Discrete Logarithm Problem   Forward Security   Proxy Blind Signature