A Secure Proxy Blind Signature Scheme using ECC

Daniyal M. Alghazzawi, Trigui Mohamed Salim and Syed Hamid Hasan

Department of Information Systems,
King Abdul Aziz University, Kingdom of Saudi Arabia
shh786@hotmail.com

Abstract. This paper describes an efficient simple proxy blind signature scheme. The security of the scheme is based on Elliptic Curve Discrete Logarithm Problem(ECDLP). This can be implemented in low power and small processor mobile devices such as smart card, PDA etc. A proxy blind signature scheme is a special form of blind signature which allows a designated person called proxy signer to sign on behalf of two or more original signers without knowing the content of the message or document. It combines the advantages of proxy signature and blind signature scheme and satisfies the security properties of both proxy and blind signature scheme.

Keywords : ECDLP, blind signature, proxy signature.