International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 4 No. IV (October, 2010), pp. 33-46

AN ID-BASED THRESHOLD DIRECTED PROXY SIGNATURE SCHEME FROM BILINEAR PAIRINGS

P. VASUDEVA REDDY, B. UMAPRASADA RAO AND T. GOWRI

Abstract

Proxy signature schemes have been invented to delegate signing rights. In a (t; n) threshold proxy signature scheme, the original signer delegates the power of signing to a designated proxy group of n members. Any t or more proxy signers of the group can cooperatively issue a proxy signature on behalf of the original signer, but (t-1) or less proxy signers cannot. A directed signature scheme is a digital signature scheme in which any signature is generated for a designated veri_er, who can directly verify the signature while others know nothing on its validity. In this paper we propose an ID-based threshold directed proxy signature scheme which combine the concepts of threshold proxy signatures and directed signatures. In this scheme, the original signer delegates the signing power to a group of n proxy signers to cooperatively issue a proxy signature on behalf of him to a designated verifier. The designated verifier can directly verify the validity of proxy signature. In case of necessary, the designated verifier can convenience any other party about the validity of the signature issued to him. We show that the scheme satisfies all security requirements in the random oracle model. The proposed scheme is useful in practical applications where the signed messages are sensitive to the signature receiver and are concern to others.

Key Words: Proxy signatures, ID-based signatures, Directed signatures, Threshold proxy signatures, Bilinear pairings.