ID-based directed proxy signature scheme from bilinear pairings

P. Vasudeva Reddy *
B. Umaprasada Rao †
Department of Engineering Mathematics
Andhra University
Visakhapatnam, A.P., India

T. Gowri ‡
Department of Electronics and Communication Engineering
GIT, GITAM University
Visakhapatnam, A.P., India

Abstract

A proxy signature scheme allows an entity to designate his/her signing capability to another entity in such a way that the latter can sign messages on behalf of the former.Such schemes have been suggested for use in a number of applications, particularly in distributed computing where delegation of rights is quite common. In 2006, Sunder Lal *et al.* [25] proposed *designated verifier proxy signatures* (DVPS) by combining the concept of proxy signatures with designated verifier signatures. In which the proxy signature can only be verified by the designated verifier and the designated verifier cannot convince any other party about the validity of the signatures. But in some situations/applications, it is necessary to convince the other parties about the validity of the signature because the signed messages may also be concern to others. In this paper, an ID-based directed proxy signatures from bilinear pairings is proposed by combining the concept of proxy signatures with directed signatures in the ID-based setting. In the proposed scheme, only the designated verifier can directly verify the proxy signature generated by the proxy signer on behalf of the original signer and any other party can verify the validity of the proxy signature with the help of the proxy signer or the designated verifier. Finally, we discussed the security requirements of the proposed scheme.

Keywords and phrases : *ID-based signatures, proxy signatures, directed signatures, bilinear pairings.*

* *E-mail*: vasucrypto@yahoo.com
† *E-mail*: buprasad@yahoo.co.in
‡ *E-mail*: gowri3478@yahoo.com

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 5, pp. 487–500