Abstract

Proxy signcryption scheme allows an original signer to delegate his signing power to a proxy such that the latter can signcrypt a message on behalf of the former. In this paper, a new proxy signcryption scheme is proposed based on Discrete Logarithm Problem (DLP) and Diffie-Hellman Problem (DHP) with a reduced computational cost compared to other schemes in literature. The proposed scheme achieves public ciphertext authentication as the signcrypted message before being accepted, the receiver first verifies the signature. This property is very useful as the receiver can filter some incorrect ciphertext before decrypting it which achieves more efficient unsigncryption. Also, a variant of the main scheme that works over elliptic curves will be considered, since it has proven to provide better security with shorter keys and hence less storage requirements which makes it more suitable for resource constrained devices such as pagers and mobile phones. Numerical examples have been given with Mathematica to emphasize the ease of its practical use.
7. Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption)