Abstract

Identity based (ID-based) public key cryptosystem gives an efficient alternative for key management as compared to certificate based public key setting. Proxy signature is a signature scheme that an original signer delegates his/her signing capability to a proxy signer, and then the proxy signer creates a signature on behalf of the original signer. Due to various application of the bilinear pairings in cryptography, many identity based signature scheme have been proposed. In this paper, we propose an identity based multi-proxy multi-signature scheme from bilinear pairings. The proposed scheme is more efficient than the multi proxy multi-signature scheme given by Li and Chen [2]. Moreover, The proposed scheme satisfies all the security requirements of a proxy signature given in [10]

References


Index Terms

Computer Science  Security

Keywords

ID-based signature scheme, Bilinear pairing, Multi-proxy multisignature