Bilinear Pairings-based Threshold Proxy Signature Schemes with Known Signers

Xue Qingshui Cao Zhenfu Qian Haifeng
Dept. of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, 200030, China
Email: {xue-qsh, zfcao}@cs.sjtu.edu.cn, ares@sjtu.edu.cn **Tel.:** 86-021-62932951

ABSTRACT

So far, all threshold proxy signature schemes are based on discrete logarithm problems in the modular multiplicative group of a large prime. The kind of threshold proxy signature scheme becomes more and more complex and cost more and more computation. In the paper, we propose a bilinear pairings-based threshold proxy signature scheme with known signers and its security is analyzed and discussed. The scheme can provide the properties of nonrepudiation, unforgeability, identifiability, distinguishability, verifiability, prevention of misuse of proxy signing right, etc. Furthermore, we show that the proposed scheme is more efficient than Sun's and Hsu et al's scheme in terms of computational complexities and communication costs in some cases.

Keywords: Cryptography, Digital Signatures, Proxy Signature, Threshold Proxy Signature, Bilinear Pairings