Security Analysis and Improvement of Some Threshold Proxy Signature Schemes

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

ABSTRACT

We review Hsu et al's threshold proxy signature scheme with known signers, describe the Tsai et al's attack to Hsu et al's scheme and point out that their attack can't work. We also review Hsu et al's another scheme with unknown signers, analyze its security and point out that it can not resist the public key substitution attack. Based on Hsu et al's second scheme, an improved version which can resist the weakness is proposed.

Keywords: Cryptography, Digital signatures, Proxy signature, Threshold proxy signature