International Journal of Innovative Computing, Information and Control
Volume **6**, Number **7**, July **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 3205–3218

AN IMPROVED (t, n) THRESHOLD PROXY SIGNATURE SCHEME WITH FAULT TOLERANCE BASED ON RSA

Ying Zhang[1,2,3], Dian-Wu Yue[1,2] and Huisheng Zhang[3]

[1]School of Information Science and Technology
[3]Department of Mathematics
Dalian Maritime University
Dalian 116026, P. R. China
zhgyg77@sina.com

[2]National Mobile Communications Research Laboratory
Southeast University
Nanjing 210096, P. R. China

Received January 2009; revised May 2009

Abstract. *Threshold proxy signature is an important security technology for distributed applications such as ad hoc network, in which any t or more proxy signers can cooperatively generate a proxy signature, but less t signers cannot. Recently, Hwang et al. proposed a practical (t, n) threshold proxy signature scheme based on the RSA cryptosystem. However, the scheme has several security weaknesses pointed out by Wang et al. In order to overcome the security issues of the existing threshold proxy signature schemes, we propose an improved (t, n) threshold proxy signature scheme, and demonstrate that our scheme is more secure and effective when compared to Hwang's scheme and others. Moreover, the proposed scheme has an optional capability of fault tolerance to balance the scalability under different situations.*

Keywords: Secret sharing, Proxy signature, Threshold scheme, Fault tolerance, RSA

1. Introduction.

Proxy signature was first introduced by Mambo et al. in 1996 [12, 13], and is becoming more and more attractive in real applications, such as electronics transaction, mobile agent environment, grid computing, global distribution network, and distributed shared object systems [8, 15, 18]. In a proxy signature scheme, an original signer authorizes the proxy signers to sign a message. Any receiver can verify the signature to see whether or not it is signed by the authorized proxy signers.

Subsequently, threshold proxy signature schemes were proposed in order to apply the proxy signature scheme to a situation in which the original signer wants to delegate the signing power to a group of proxy signers for sharing signing responsibility [5, 20]. To date, many threshold proxy signature schemes have been proposed such as [2, 3, 9]. In a (t, n) threshold proxy signature scheme, the original signer delegates the signing right to a group of n proxy signers, in which t or more signers can generate a proxy signature cooperatively, but less t members cannot do it. As Hwang et al. mentioned in their innovative work on threshold proxy signature scheme based on RSA (HLL scheme) [4], a practical and secure (t, n) threshold proxy signature scheme should satisfy the following six requirements:

- Secrecy. The original signer's private key cannot be derived from any information, such as the sharing of the proxy signing key or the original signer's public key, and so on. Particularly, even if all proxy signers collude together, they cannot derive the original signer's private key.
- Proxy protection. Only a delegated proxy signer can generate his partial proxy signature.