International Journal of Innovative Computing, Information and Control
Volume **4**, Number **2**, February **2008**

ICIC International ©2008 ISSN 1349-4198
pp. **425–431**

ROBUST *T*-OUT-OF-*N* PROXY SIGNATURE BASED ON RSA CRYPTOSYSTEMS

Ya-Fen Chang

Department of Computer Science and Information Engineering
National Taichung Institute of Technology
Taichung 404, Taiwan
cyf@cs.ccu.edu.tw

Chin-Chen Chang

Department of Information Engineering and Computer Science
Feng Chia University, Taichung 40724, Taiwan
Department of Computer Science and Information Engineering
National Chung Cheng University, Chiayi 621, Taiwan
ccc@cs.ccu.edu.tw

Received January 2007; revised July 2007

Abstract. *Proxy signature allows one user to delegate his signing capacity to other people. No proxy signature scheme based on the widespread RSA cryptosystem was proposed until 2003. However, the first RSA-based (t, n) threshold proxy signature scheme suffers from some drawbacks: (1) the original signer's private key can be derived and (2) the delegates' identities need to be chosen carefully. In this paper, we will propose an improved RSA-based (t, n) threshold proxy signature scheme with free-will identities and without the help of the trusted combiner. Moreover, the proposed scheme ensures the proxy signers' partial anonymity to provide the real proxy signers' privacy for safety, and no proxy signing key will be retrieved by the cooperation of the proxy signers.*

Keywords: Cryptography, (t, n) Threshold, RSA, Proxy signature

1. **Introduction.** With the rapid growth of network technologies, plenty of applications have been proposed, and security becomes an important issue [23,24]. Proxy signature was first proposed in 1996 [3]. With the proxy function, the original signer is allowed to delegate his signing capacity to another user, the proxy signer. That is, the proxy signer can sign the messages on behalf of the original signer.

Taking secret sharing into consideration [4-6], the threshold proxy signature schemes were proposed [7,8]. In a (t, n) threshold proxy signature scheme, the original signer delegates his signing capacity to n proxy signers. The original signer can set t freely such that $1 \leq t \leq n$, and t or more proxy signers can cooperate to generate valid proxy signatures on behalf of the original signer. Consequently, threshold proxy signature schemes are more practical, flexible, and secure than other conventional proxy signature schemes.

The requirements of a practical and secure (t, n) threshold proxy signature scheme are listed as follows [1,18]:

(1) Secrecy: The system must ensure that the original signer's private key cannot be derived from any information. Furthermore, no proxy signers can cooperate to derive the original signer's private key.

(2) Proxy Protection: No one can generate the valid partial proxy signature except the authorized proxy signer, and neither can the original signer.