International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **3**, March **2011**

 ISSN 1349-4198
pp. **1039–1054**

GENERALIZATION OF PROXY SIGNATURE BASED ON FACTORIZATION

Cheng-Chi Lee[1], Tzu-Chun Lin[2], Shiang-Feng Tzeng[3] and Min-Shiang Hwang[4,*]

[1]Department of Photonics and Communication Engineering
Asia University
No. 500, Lioufeng Raod, Wufeng, Taichung 41354, Taiwan
cclee@asia.edu.tw

[2]Department of Applied Mathematics
Feng Chia University
No. 100, Wenhwa Road, Seatwen, Taichung 40724, Taiwan

[3]Department of Library and Information Science
Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang City, Taipei County 24205, Taiwan
cclee@mail.fju.edu.tw

[4]Department of Management Information Systems
National Chung Hsing University
No. 250, Kuo Kuang Road, Taichung 402, Taiwan
*Corresponding authors: mshwang@nchu.edu.tw

Received October 2009; revised March 2010

Abstract. *A rich set of proxy signature schemes have been widely researched and discussed so far. However, they have been mainly focusing on dealing with one or two separate proxy situations each. In this article, the authors proposed the generalization of the* $(t_1/n_1 - t_2/n_2)$ *proxy signature scheme based on the factorization of the square root modulo of a composite number. This scheme can be applied to every proxy situation. The* $(t_1/n_1 - t_2/n_2)$ *proxy signature scheme allows the original group of original signers to delegate their signing capability to a designated proxy group of proxy signers. Any verifier can verify the proxy signatures on the messages with the knowledge of the identities of the actual original signers and the actual proxy signers. Furthermore, all possible attacks that have been analyzed so far have failed to break the proposed scheme.*
Keywords: Digital signature, Proxy signature, Multi-proxy multi-signature scheme, Proxy multi-signature scheme, Threshold proxy signature

1. **Introduction.** Digital signatures [3, 19, 37] are widely used to replace hand-written signatures in the digital world. However, simple digital signature schemes are not enough to satisfy today's practical conditions. For example, suppose a chairman in a department needs to go on a business trip. She/He has to find a proxy person to deal with her/his work at the office. Traditional digital signature schemes [1, 21, 33, 48] do not meet this requirement. To remedy this weakness, the proxy function has been added to digital signature schemes, and this new type of digital signature is called proxy signature [4, 28, 40, 44].

In 1996, Mambo et al. [30, 31] proposed the first proxy signature schemes. Their schemes allow the original signer to delegate her/his signing capability to a designated proxy signer so that the designated proxy signer can generate a signature on behalf of the original signer.