International Journal of Innovative Computing, Information and Control
Volume **6**, Number **9**, September **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 3843–3852

EFFICIENT CONVERTIBLE MULTI-AUTHENTICATED ENCRYPTION SCHEME WITHOUT MESSAGE REDUNDANCY OR ONE-WAY HASH FUNCTION

Jia-Lun Tsai[1], Tzong-Sun Wu[2,*], Han-Yu Lin[3] and Jong-Eao Lee[4]

[1]Department of Information Management
National Taiwan University of Science and Technology
Taipei 106, Taiwan
crousekimo@yahoo.com.tw

[2]Department of Computer Science and Engineering
National Taiwan Ocean University
Keelung 202, Taiwan
*Corresponding author: ibox456@gmail.com

[3]Department of Computer Science
[4]Department of Applied Mathematics
National Chiao Tung University
Hsinchu 300, Taiwan
hanyu.cs94g@nctu.edu.tw; jlee@math.nctu.edu.tw

Received February 2009; revised December 2009

Abstract. *A convertible multi-authenticated encryption (CMAE) scheme providing confidentiality, authenticity and non-repudiation properties allows a designated recipient to recover and verify an authenticated message which is signed by multiple signers. The recipient has the ability to further prove the dishonesty of signers to any third party if they repudiate their signature latter. In 2008, Wu* et al. *first proposed a CMAE scheme based on discrete logarithms, but the computational complexity of their scheme is rather high and the message redundancy is required. To improve the performance and remove the message redundancy, Tsai adopted one-way hash functions (such as MD5) to propose a new scheme. In 2005, however, MD5 was cracked by Wang and Yu, which indicates that the schemes using one-way hash functions might turn out to be vulnerable to such an attack. This paper proposes a new efficient CMAE scheme. Neither the one-way hash function nor the message redundancy is employed in the proposed scheme. The scheme not only preserves the advantages of Wu* et al.*'s, but also outperforms their scheme. With low computational cost, our proposed scheme can be practically implemented.*

Keywords: Authenticated encryption, Multisignature, Message recovery, Discrete logarithms

1. **Introduction.** With the rapid development of the network, more and more companies are building business systems on the Internet to increase the work efficiency. Moreover, some companies establish a system to exchange the important data between the company and the other companies. To build such a system, the security requirements should be considered first as follows: (1) How the sender securely sends a message to a specified recipient via an insecure network; (2) How the recipient verifies whether the message is sent from the sender. Authenticated encryption scheme is such a secure message transmission mechanism which achieves the security requirements of confidentiality, authenticity and non-repudiation [1-7]. The confidentiality property ensures that the sensitive information can only be obtained by the designed recipient. With the authenticity property, we can prohibit any adversary from masquerading some one else. The non-repudiation property