International Journal of Innovative
Computing, Information and Control
Volume 4, Number 11, November 2008
 ISSN 1349-4198
pp. 3037–3045

A GROUP-ORIENTED PROXY CMAE SCHEME WITH COMPUTATIONAL SECRECY

Tzong-Sun Wu[1] and Han-Yu Lin[2]

[1]Department of Computer Science and Engineering
National Taiwan Ocean University
Keelung 202, Taiwan
ilan543@gmail.com

[2]Department of Computer Science
National Chiao Tung University
Hsinchu, 300, Taiwan
hanyu.cs94g@nctu.edu.tw

Received August 2007; revised December 2007

Abstract. *This paper presents a group-oriented proxy convertible multi-authenticated encryption (CMAE) scheme for strengthening the gradually wide applications which have to simultaneously fulfill the security requirements of integrity, authentication, confidentiality and non-repudiation. The proposed scheme allows a group of original signers to delegate their signing power to an authorized person called proxy signer, such that the proxy signer can generate an authenticated ciphertext on behalf of the original group. Instead of anyone else, only a designated recipient can decrypt the ciphertext and verify its corresponding signature for the purpose of confidentiality. In case of a later dispute over repudiation, the designated recipient also has the ability to convert the multi-signature into an ordinary one for convincing anyone of the signer's dishonesty. Moreover, the computational secrecy ensures that the produced ciphertext is computationally indistinguishable with respect to two candidate messages.*
Keywords: Group-oriented, Proxy multi-signature, Authenticated encryption, Convertible, Computational secrecy

1. **Introduction.** With the development of Internet, kinds of techniques [1-4] have been proposed to ensure the security of digital world. In 1994, Horster *et al.* [5] proposed an authenticated encryption scheme which further provides digital signatures with confidentiality. Such schemes enable a signer to generate an authenticated ciphertext, such that only the designated recipient can decrypt the ciphertext and verify its corresponding signature. However, a later dispute that the signer disclaims having generated the signature might occur, since only the designated recipient can verify the signature. To deal with the problem, Araki *et al.* [6] proposed a convertible limited verifier signature scheme equipped with a mending mechanism. Yet, their approach was impracticable and incurred extra computation efforts. In addition, Zhang and Kim [7] also pointed out that Araki *et al.*'s scheme couldn't withstand a universal forgery attack on an arbitrary chosen message. In 2002, Wu and Hsu [8] proposed a convertible authenticated encryption (CAE) scheme with better efficiency. The Wu-Hsu scheme allowed the designated recipient to solely convert the signature into an ordinary one for convincing anyone of the signer's dishonesty without any computation efforts or communication overheads.

In 1996, Mambo *et al.* [9,10] proposed proxy signature schemes enabling an original signer to delegate his signing power to an authorized person called proxy signer, such that the proxy signer could generate a valid proxy signature on behalf of the original