International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **11**, November **2011**

 ISSN 1349-4198
pp. 6177–6185

AN ENHANCED THRESHOLD AUTHENTICATED ENCRYPTION SCHEME WITH CONVERTIBILITY

Tzung-Her Chen and Ci-Lin Li

Department of Computer Science and Information Engineering
National Chiayi University
No. 300, Syuefu Rd., Chiayi City 60004, Taiwan
thchen@mail.ncyu.edu.tw

Received June 2010; revised October 2010

Abstract. *Recently, Chung et al. (2009) proposed a novel and valuable threshold authenticated encryption scheme. Unfortunately, it has a potential weakness: if the secret message involves criminal evidence or illegal content, the designated receiver cannot authenticate the secret message in the later dispute. The authors of this paper aim at enhancing Chung et al.'s scheme by adding the convertibility capability so that the designated receiver can demonstrate that the signature with respect to the message has been signed. And then, the enforcement agency can trace the source of secret messages. In addition to inheriting the advantages of Chung et al.'s scheme, the improved scheme achieves the goal that the designated recipient can convert an authenticated signature into an ordinary signature. It is worthwhile to note that the main advantages are that, with the ordinary signature along with the signed message, the third party can verify if the authenticated signature was generated by a specific signer group. In this way, public verifiability to the authenticated encryption scheme is satisfied.*
Keywords: Digital signature, Authenticated encryption, Convertible, Labor-division

1. **Introduction.** Horster et al. (1994) [1] proposed the first authenticated encryption (AE for short) scheme which encrypts the message in the signature, and only the designated recipient can recover message and verify the signature. Hence, the AE scheme has become a security requirement including privacy, integrity and authenticity simultaneously.

Considering the situation that the message to sign is large, a large message should be divided into a sequence of message blocks, and the message blocks with some redundancy have to be added to ensure that the message blocks are consecutive. Hence, Hwang et al. (1996) [4] modified Horster et al.'s AE scheme to form an authenticated encryption scheme with message linkage. In Hwang et al.'s scheme, a large message is divided into n blocks, and the signer encrypts them to form $(n-1)$ encryption blocks and generates the signature. It is notable that the encryption blocks' relative order is sequential so that it can avoid an outsider modifying, deleting, replicating and reordering encryption blocks.

Later, Lee and Chang (1999) [5] proposed another AE scheme with linkage between message blocks to lower the computational cost. However, Lee and Chang's has a drawback; i.e., the designated recipient can recover the message blocks only after collecting the entire encryption blocks. In order to correct the above-mentioned drawback, Tseng et al. (2003) [6] proposed another AE.

With the development of business requirements, the concept of multi-signature schemes [11,12] and (t, n) threshold signature schemes [7-9] has been presented to satisfy the requirement in real word. Especially, the (t, n) threshold signature schemes allow t out of n signers in the group join and agree to generate a valid signature. Recently, Chung