International Journal of Innovative
Computing, Information and Control
Volume **5**, Number **5**, May **2009**

ICIC International ©2009 ISSN 1349-4198
pp. 1395–1406

A (t, n)-FAIR DYNAMIC THRESHOLD SECRET SHARING SCHEME

Tzuoh-Yi Lin, Tzong-Chen Wu, Chin-I Lee

Department of Information Management
National Taiwan University of Science and Technology
Taipei 106, Taiwan
linjoe@gmail.com; tcwu@cs.ntust.edu.tw; D9109108@ntust.edu.tw

Tzong-Sun Wu

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

Received November 2007; revised May 2008

Abstract. *A (t, n) threshold secret sharing scheme enables the secret dealer to decompose the secret into n shares which are separately distributed to participants of the same size. Any t or more participants can reconstruct the shared secret, where the threshold value t is predefined according to the sharing policy. However, if there is a cheater releasing a false share in the secret reconstruction, he can obtain the secret alone. This paper presents a novel (t, n)-fair dynamic threshold secret sharing scheme in which the dealer can distribute multiple shared secrets associated with different threshold values. Meanwhile, the secret share held by each participant remains unchanged. Furthermore, the proposed scheme has the following features: (1) cheater identification – all participants can identify the cheaters during the secret reconstruction; (2) fair reconstruction of the shared secret – each participant has an equal ability to recover the shared secret, even if there are v cheaters among these participants, where $v < t/2$; (3) fixed length of public information – the public information is independent of the threshold value and the number of participants.*

Keywords: Secret sharing, Dynamic threshold, Cheater identification, Fair secret reconstruction

1. **Introduction.** In 1979, Shamir [1] and Blakley [2] independently proposed (t, n) threshold schemes to protect the shared secret such that the secret can be reconstructed with high flexibility. In their schemes, the dealer first divides the shared secret into n distinct shares, and then separately delivers these shares to n participants. After that, any t out of n participants can cooperatively reconstruct the shared secret, where t is the pre-specified threshold value and $1 \leq t \leq n$. Since then, many solutions and variants have been proposed [3-15].

Consider a scenario that a dishonest participant (the cheater) releases a fake share and the other participants honestly release their shares during the secret reconstruction. Hence, only the cheater can obtain the secret while the other participants have nothing about the secret. This brings out the "so-called" cheating problem. To resolve the problem, many protocols have been developed to detect the false shares [16-22]. However, they cannot prohibit the cheater from solely obtaining the shared secret if he is the last one to release his share [23,24]. To protect the honest participants against cheating in secret reconstruction is refered to as the fair secret sharing. In 1995, Lin and Harn [23] proposed a protocol to reconstruct a secret in a fair way. The probability of the cheater