International Journal of Innovative Computing, Information and Control
Volume **4**, Number **6**, June **2008**

ICIC International ©2008 ISSN 1349-4198
pp. **1347–1356**

A MULTI-POLICY THRESHOLD SIGNATURE SCHEME WITH TRACEABLE PARTICIPANT COSIGNERS

Chia-Ho Chu[1], Hsiu-Feng Lin[1], Chin-Chen Chang[1] and Chih-Ying Chen[2]

[1]Department of Information Engineering and Computer Science
[2]Department of Communications Engineering
Feng Chia University
Taichung 40724, Taiwan
chiaho@hclab.iecs.fcu.edu.tw; hflin@fcu.edu.tw; ccc@cs.ccu.edu.tw
chihchen@fcu.edu.tw

Received February 2007; revised June 2007

Abstract. *In a (t, n) threshold scheme, the secret can be reconstructed by the cooperation of t or more users. With this basic concept, Lee devised a threshold signature scheme with multiple signing policies in 2001. His approach still keeps the main benefit, that is, each member only needs to hold one secret shadow. In Lee's paper, any verifier can authenticate the legality of a group signature with the threshold value t. If a dispute arises, however, no one can trace the cosigners from the group signature. Therefore, we present a multi-policy threshold signature with the ability to recover participant cosigners. In the proposed scheme, different documents can be signed by a suitable threshold value t, and the cosigners are anonymous when they participate in the (t, n) threshold signature. If it is necessary to find out the participant cosigners, one can open the group signature with the help of the system center. Moreover, we also solve the linkage problem, meaning that an opened group signature will not disclose the participant cosigners of other group signatures. In our scheme, each user needs to keep one secret key, one secret shadow and two secret values.*

Keywords: Cryptography, Group signature, Threshold signature, Traceable threshold signature, Multi-policy threshold signature, Linkage problem

1. **Introduction.** (t, n)-threshold signature is a group-oriented digital signature technology. In a (t, n)-threshold signature, the group secret key is shared by n authorized members of the group, and any t (the threshold value) or more members can collaborate to produce a valid signature on behalf of the group. But members fewer than t, no matter how they cooperate, can never generate the valid group signature. In addition, the verifier can verify the validity of the group signature according to the corresponding public key of the group, without identifying the identities of the cosigners. Therefore, threshold signature is the major technique for many groups such as governments, schools, business, and army—those which need group decision—to realize electronization and to participate in internet activities. Accordingly, it has become one important research issue of applied cryptography since in 1991 Desmedt and Frankel [2] initiate the first (t, n) threshold system.

Further, in real applications, many documents with different significance have to be signed up by a group. And the corresponding signing thresholds and group secret keys should be different. If the group deals with those cases by applying a basic threshold signature scheme repeatedly, each authorized group member has to keep too many secret shadows. In this way it would not only cause inefficiencies but also security problems.