Journal of The Chinese Institute of Engineers
24(1): 113-116

An Efficient Group-oriented (t,n) Threshold Signature Scheme with Message Linkage

Perng, Chi-Yow; Jan, Jinn-Ke; Tseng, Yuh-Min

Abstract

In 1999, Chen (1999) proposed several signature schemes in his graduate thesis. One is a group-oriented (t,n) threshold signature scheme in which the (t,n) threshold signature is based on an RSA scheme. Although it has advantages, including message recovery, lower cost for transmission, and message linkage, it requires a great amount of time for the modulo exponentiation computation. In this article, we propose an improved scheme, which is more efficient than the one proposed by Chen both in the signature generation and the verification.

Key words：Group-oriented; Message linkage; (t;n); Threshold signature

中文摘要

在 1999 年，陳國倫在他的碩士論文中提出幾個簽章法，其中一個是基於 RSA 之(t;n)門檻群體導向簽章法，此方法雖然具有訊息還原、較小傳輸量及訊息串連等優點，但是他的方法中需要大量的模指數運算，在這篇文章中，吾等提出一個在簽章產生和驗證過程中比陳的方法較有效率的改進方法。

關鍵字：群體導向; 訊息串聯; (t;n)門檻簽章