Journal of The Chinese Institute of Engineers
25(6): 723-733

A Unified Approach to Secret Sharing Schemes with Low Distribution Cost

Chien, Hung-Yu; Jan, Jinn-Ke; Tseng, Yuh-Min

Abstract

In secret sharing schemes, the secret holder has to distribute secret shares to each participant before distributing the secrets. To distribute or redistribute shares is a very costly process with respect to both time and resources. Unlike previous works, where different approaches are proposed for different scenarios, we propose a unified approach for both threshold-based schemes and generalized group-oriented cryptosystems. This unified implementation has the following merits: (1) With a unified approach, the implementation requires much less overhead than its counterparts when various secret sharing problems are simultaneously involved; (2) The Secret Holder (SD) does not need to redistribute new secret shares after the secret reconstruction; (3) The SD can, dynamically and efficiently. determine the capacities (weight) of each user on recovering the secrets, and the threshold values of the secrets; (4) To dynamically adjust the capacities of users, the SD does not need to refresh the shadow of each user and each user just memorizes one secret shadow.

Key words：Cryptography; Secret sharing

中文摘要

在秘密分享機制中，蜜一擁有者再分享秘密前必須先透過一安全管道將次秘密分送到參與者手上，這步驟是十分耗費資源及費時。不同於過去研究中分別採用不同機制以解決不同的分享問題，本論文採用同一機制解決所有分享問題。這統一的機制有如下數項優點：（１）因對所以分享問題皆採用同一機制，其實作成本可降低很多；（２）在參與者回復部份秘密後，秘密擁有者不須重送次秘密；（３）秘密擁有者可動態且有效率的決定參與者的權值；（４）參與者只需記憶一份次秘密及使擁有高於一的權值。

關鍵字：密碼學; 秘密分享