IEICE Transactions on Fundamentals of Electronics,
Communications of Computer Sciences, E83-A(12): 2762-2765

A Practical (t,n) Multi-secret Sharing Scheme

Chien, H. Y. ; Jan, J. K. ; Tseng, Yuh-Min

Abstract

Based on the systematic block codes, we propose a (t,n) multi-secret sharing scheme. Compared with the previous works, our schemc has the advantages of smaller communication overhead, easy generator matrix construction and nondisclosure of users secrct shares after multiple secret reconstruction operations. These advantages make the practical implementation of our scheme verv attractive.

Key words：Cryptography; Secret sharing