Cryptology ePrint Archive: Report 2012/719

An ideal multi-secret sharing scheme based on minimal privileged coalitions

Yun Song , Zhihui Li

Abstract: How to construct an ideal multi-secret sharing scheme for general access structures is difficult. In this paper, we solve an open problem proposed by Spiez et al.recently [Finite Fields and Their Application, 2011(17) 329-342], namely to design an algorithm of privileged coalitions of any length if such coalitions exist. Furthermore, in terms of privileged coalitions, we show that most of the existing multi-secret sharing schemes based on Shamir threshold secret sharing are not perfect by analyzing Yang et al.'s scheme and Pang et al.'s scheme. Finally, based on the algorithm mentioned above, we devise an ideal multi-secret sharing scheme for families of access structures, which possesses more vivid authorized sets than that of the threshold scheme.

Category / Keywords: applications / secret sharing

Date: received 24 Dec 2012

Contact author: snnulzh at 25yahoo com cn

Available formats: PDF | BibTeX Citation

Version: 20121227:173626 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]