Cryptology ePrint Archive: Report 2013/189

Ideal and Perfect Hierarchical Secret Sharing Schemes based on MDS codes

Appala Naidu Tentu and Prabal Paul and V Ch Venkaiah

Abstract: An ideal conjunctive hierarchical secret sharing scheme, constructed based on the Maximum Distance Separable (MDS) codes, is proposed in this paper. The scheme, what we call, is computationally perfect. By computationally perfect, we mean, an authorized set can always reconstruct the secret in polynomial time whereas for an unauthorized set this is computationally hard. Also, in our scheme, the size of the ground field is independent of the parameters of the access structure. Further, it is efficient and requires $O(n^3)$, where n is the number of participants.

Keywords: Computationally perfect, Ideal, Secret sharing scheme, Conjunctive hierarchical access structure, Disjunctive hierarchical access structure, MDS code.

Category / Keywords: cryptographic protocols / secret sharing

Date: received 2 Apr 2013

Contact author: naidunit at gmail com

Available formats: PDF | BibTeX Citation

Version: 20130402:145228 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]