Cryptology ePrint Archive: Report 2013/047

Lower Bounds on the Information Ratio of Linear Secret Sharing Schemes

Carles Padro

Abstract: Superpolynomial lower bounds on the average information ratio of linear secret sharing scheme are presented in this note for the first time. The previously known superpolynomial lower bounds applied only to the average information ratio of linear schemes in which the secret is a single field element. The new bounds are obtained by a simple adaptation of the techniques in those previous works.

Category / Keywords: cryptographic protocols / secet sharing, linear secret sharing schemes, lower bounds on the information ratio.

Date: received 29 Jan 2013

Contact author: cpadro at ma4 upc edu

Available formats: PDF | BibTeX Citation

Version: 20130130:175100 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]