Cryptology ePrint Archive: Report 2013/082

Secret Sharing, Rank Inequalities and Information Inequalities

Sebastia Martin and Carles Padro and An Yang

Abstract: Beimel and Orlov proved that all information inequalities on four or five variables, together with all information inequalities on more than five variables that are known to date, provide lower bounds on the size of the shares in secret sharing schemes that are at most linear on the number of participants. We present here another negative result about the power of information inequalities in the search for lower bounds in secret sharing. Namely, we prove that all information inequalities on a bounded number of variables only can provide lower bounds that are polynomial on the number of participants.

Category / Keywords: cryptographic protocols / Secret sharing, Information inequalities, Rank inequalities, Polymatroid.

Date: received 17 Feb 2013

Contact author: cpadro at ma4 upc edu