

Cryptology ePrint Archive: Report 2011/375

Complexity of universal access structures

Laszlo Csirmaz

Abstract: An important parameter in a secret sharing scheme is the number of minimal qualified sets. Given this number, the universal access structure is the richest possible structure, namely the one in which there are one or more participants in every possible Boolean combination of the minimal qualified sets. Every access structure is a substructure of the universal structure for the same number of minimal qualified subsets, thus universal access structures have the highest complexity given the number of minimal qualified sets. We show that the complexity of the universal structure with n minimal qualified sets is between $n/\log_2 n$ and $n/2.7182\dots$ asymptotically.

Category / Keywords: foundations / secret sharing; complexity; entropy method;

Date: received 11 Jul 2011

Contact author: csirmaz at degas ceu hu

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20110712:020454 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]