Cryptology ePrint Archive: Report 2011/147

The Optimal Linear Secret Sharing Scheme for Any Given Access Structure

Tang Chunming, Gao Shuhong, Zhang Chengli

Abstract: Any linear code can be used to construct a linear secret sharing scheme. In this paper, it is shown how to decide optimal linear codes (i.e., with the biggest information rate) realizing a given access structure over finite fields. It amounts to solving a system of quadratic equations constructed from the given access structure and the corresponding adversary structure. The system becomes a linear system for binary codes. An algorithm is also given for finding the adversary structure for any given access structure.

Category / Keywords: cryptographic protocols /

Date: received 23 Mar 2011

Contact author: ctang at gzhu edu cn