Cryptology ePrint Archive: Report 2013/054

Joint Compartmented Threshold Access Structures

Ali Aydın Selçuk and Ramazan Yılmaz

Abstract: In this paper, we introduce the notion of a joint compartmented threshold access structure (JCTAS). We study the necessary conditions for the existence of an ideal and perfect secret sharing scheme and give a characterization of almost all ideal JCTASes. Then we give an ideal and almost surely perfect construction that realizes such access structures. We prove the asymptotic perfectness of this construction by the Schwartz-Zippel Lemma.

Category / Keywords: secret sharing, threshold cryptography

Publication Info: Submitted to JCAM, but not accepted yet.

Date: received 3 Feb 2013, last revised 4 Feb 2013

Contact author: ramazan cs at gmail com