CORR 99-14

Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures

D.R. Stinson & R. Wei

Abstract Verifiable secret sharing schemes (VSS) are secret sharing schemes dealing with possible cheating by the participants. In this paper, we propose a new unconditionally secure VSS. Then we construct a new proactive secret sharing scheme based on that VSS. In a proactive scheme, the shares are periodically renewed so that an adversary cannot get any information about the secret unless he is able to access a specified number of shares in a short time period. Furthermore, we introduce some combinatorial structure into the proactive scheme to make the scheme more efficient. The combinatorial method might also be used to improve some of the previously constructed proactive schemes.