CORR 99-10

Determining the maximum consistent set of shares in a threshold scheme

D.R. Stinson and R. Wei

Abstract The shares in a (k, n) Shamir threshold scheme consist of n points on some polynomial of degree at most $k-1$. If one or more of the shares are faulty, then the secret may not be reconstructed correctly. Supposing that at most t of the n shares are faulty, we show how a suitably chosen covering design can be used to compute the correct secret. We review known results on coverings of the desired type, and give two new construction. We also consider a randomized algorithm for the same problem, and compare it to the deterministic algorithm obtained by using a particular class of coverings.