1129-94-180 **Benjamin Fine*** (fine@fairfield.edu), Department of Mathematics, Fairfield University, Fairfield, CT 06824, **Anja Moldenhauer**, Department of Mathematics, Florida Stlantic University, Boca Rtaon, FL , and **Gerhard Rosenberger**, Fachebriech Mathematik, University of Hamburg, Hamburg, Germany. *An Analysis of the Closest Vector Secret Sharing Scheme.*

Abstract:

An (n,t) secret sharing scheme with $t \leq n$ is a crypotgrapic protocol designed to allow a secret to be shared among n participants in such a way that any t can access the secret but not less than t. The gold standard in secret sharing is a beautiful method due to Shamir based on polynomial interpolation. In this talk we discuss a geometric alternative to the Shamir scheme given by Chum, Fine, Rosenberger and Zhang based on the closest vector theorem. We show hos this method can be implemented and show that it has several advantages over the Shamir scheme. (Received March 14, 2017)