1088-94-141 **Benjamin Fine** and **Anja Moldenhauer***, Fachbereich Mathematik, Universität Hamburg, Bundesstrasse 55, 20146 Hamburg, Germany, and **Gerhard Rosenberger**. *A secret sharing scheme based on the closest vector theorem and a modification to a private key cryptosystem.*

An (n, t) secret sharing protocol, with $n, t \in \mathbb{N}$ and $t \leq n$, is a method to distribute a secret among a group of n participants in such a way that it can be recovered only if at least t of them combine their shares. We explain the steps for an (n, t) secret sharing scheme based on the closest vector theorem [first published by C. S. Chum, B. Fine, G. Rosenberger and X. Zhang: *A proposed alternative to the shamir secret sharing scheme.* Contemporary Mathematics, 582, page 47-50, 2012]. We take a look at the security and the complexity and compare it to Shamirs secret sharing scheme. Finally we modify the (n, t) secret sharing scheme based on the closest vector theorem to a private key cryptosystem. (Received February 07, 2013)