1026-94-76 **Rainer Steinwandt*** (rsteinwa@fau.edu), Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431. *On Defining and Proving Security in Cryptographic Key Establishment.*

An adequate specification of security goals is a crucial point in the design of cryptographic protocols. The talk discusses the problem of finding definitions that adequately formalize the intuition of a "secure key establishment" and enable meaningful security proofs.

The main focus of the talk is on *group* key establishment where the number of protocol participants can be greater than 2. Here the assumption that all protocol participants are honest is not necessarily justified, therewith raising the question of provable security guarantees in the presence of malicious insiders. It turns out that the establishment of such security guarantees does not necessarily require a significant loss in terms of efficiency. Combining provable security guarantees and acceptable efficiency seems to be possible.

(Based on joint work with Jens-Matthias Bohli and María Isabel González Vasco.) (Received February 13, 2007)