1046-94-1447 **Rainer Steinwandt*** (rsteinwa@fau.edu), Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431. *Group Theory in Authenticated Key Establishment: What Assumption(s) Do We Make?*

When exploring the potential of group theory for constructing key establishment schemes, cryptographic issues like authentication and key derivation are not always discussed in detail. Conceptually, it seems desirable that addressing these questions does not impose the introduction of additional (possibly idealizing) assumptions.

The talk discusses techniques for (password-based) authentication and for key derivation in key establishment protocols. At this, the focus is on the so-called standard model, i.e., a scenario where no idealizing assumptions, like the availability of a random oracle, can be made. (Received September 15, 2008)