# Notice of Seminar:

Series: *Cryptography Seminar*

Title: "*Securing mobile ad hoc networks using identity-based schemes*"

Speaker: *Katrin Hoeper, University of Waterloo*

Date/Location: *December 1 (Thursday): 2:30 - 3:30 pm, DC 1331*

*Abstract*:

In this presentation, we utilize some special features of identity-based cryptographic (IBC) schemes, such as pre-shared secret keys from pairings, to design identity-based authentication and key exchange (IDAKE) schemes that meet the special constraints and requirements of mobile ad hoc networks (MANETs). We introduce a basic MANET-IDAKE scheme in which a trusted third party (TTP) initializes all devices before they join the network and a fully self-organized MANET-IDAKE scheme that does not require any central TTP. As part of these schemes, we present the first key revocation and key renewing algorithms for IBC schemes. Furthermore, we present an extremely efficient yet secure IDAKE protocol that can be used in the presented schemes. The schemes bootstrap the security in MANETs and enable the implementation of secure routing, authentication, key exchange, and other security protocols in a variety of MANET applications. Finally, we provide a security and performance discussion.