Title: "Group Signatures and Anonymous Reputation Systems"
Speaker: Christina Kolb

Abstract
Reputation systems are used to compute and publish reputation scores for certain services or products. We are interested in reputation systems, where users should only be allowed to rate products that they purchased previously. A reputation system has to achieve different security properties: unforgeability, anonymity, traceability, and linkability, to name the most important ones. The most fundamental requirement of reputation systems is the unforgeability of reputation scores. Anonymity requieres that nobody should be able to find out the user's identity after a user rated a service. Traceability means that it must be impossible for any set of colluding users to create ratings that can not be traced back to a registered user. Linkability requieres that anyone can decide whether or not two ratings for the same service are created by the same user.
Based on short group signatures, we show how to design a reputation system. We prove that, based on widely accepted complexity and number theoretical assumptions, our construction achieves the security requirements above. In addition, our reputation system allows to define different types of users without sacrificing anonymity. Thus one can distinguish between these types of users, for example average users and experts, where scores by experts should be more significant than scores by average users.
In this talk, we present our reputation system and outline the main ideas of the security proofs. We also give a brief overview of future research work.