CFEM workshop: Theory and Practice of Multiparty Computation
4 to 8 June, 2012
Aarhus University, Denmark

Speaker: Ueli Maurer, ETH Zürich

Title: Abstract cryptography and secure multi-party computation

I will present abstract cryptography, a new framework for defining and proving security of cryptographic protocols, with an emphasis on applications to secure multi-party computation. Abstract cryptography differs from previous approaches (like UC) both in terms of the types of statements made as well as in terms of the abstraction level at which they are proved. An important aspect of abstract cryptography is that concepts are abstracted top-down, in the spirit of abstract algebra, rather defined bottom-up as in traditional cryptography and theoretical computer science. This leads to new insights.

Joint work with Renato Renner.