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

Speaker: Martin Hirt, ETH Zürich

Title: Hyper-Invertible Matrices and Applications

We introduce the notion of hyper-invertible matrices (HIM): A HIM is a matrix whose every non-trivial square sub-matrix is invertible. HIMs are useful in multi-party settings to efficiently generate random values (field elements, polynomials, etc), possibly with additional constraints. Given n objects, all but t of them being "good", a HIM allows to concentrate the good property on *any* subset of n-t objects, as well as to blur the errors on *any* subset of t objects.

In this talk, we present a construction and several applications of HIMs.