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

Speaker: Hoeteck Wee, George Washington University

Title: Functional Encryption with Bounded Collusions via Multi-Party Computation

We construct functional encryption schemes for polynomial-time computable functions secure against an a-priori bounded polynomial number of collusions. Our constructions require only semantically secure public-key encryption schemes and pseudorandom generators computable by small-depth circuits (known to be implied by most concrete intractability assumptions). For certain special cases such as predicate encryption schemes with public index, the construction requires only semantically secure encryption schemes.

Along the way, we show a "bootstrapping theorem" that builds a q-query functional encryption scheme for arbitrary functions starting from a q-query functional encryption scheme for bounded-degree functions. All our constructions rely heavily on techniques from secure multi-party computation and randomized encodings.

Our constructions are secure under a strong simulation-based definition of functional encryption.

(Joint work with Sergey Gorbunov and Vinod Vaikuntanathan)