ABSTRACT

CFEM & CTIC workshop:
Theory and Practice of Secure Multiparty Computation
May 30 to June 3, 2016
Aarhus University, Denmark

Title: Function Secret Sharing, Part I: Constructions from One-Way Functions and Applications

Yuval Ishai, Technion, Israel

Function secret sharing (FSS) is a secret sharing scheme for functions. More concretely, the goal of FSS is to split a function f from a function class F into succinctly described f_1,…,f_m, such that f(x)=f_1(x)+…+f_m(x) for every input x, and every strict subset of the f_i computationally hides f. This additive secret sharing of functions can be generalized to other linear secret sharing schemes.

We will describe constructions of FSS schemes based on one-way functions for simple function classes F, including the class of point functions. We will also present applications of FSS as well as barriers to obtaining stronger results.

Joint work with Elette Boyle and Niv Gilboa This is joint work with Sean Kennedy and Gordon Wilfong (Bell Labs).