Speaker: Eyal Kushilevitz, Technion

Title: Distributed Obfuscation and Non-Interactive Secure Multiparty Computation

We introduce and study the notion of ``distributed obfuscation'', a natural generalization of obfuscation that is motivated by the goal of obtaining ``best possible'' non-interactive protocols for secure multiparty computation.
A distributed obfuscation scheme for a function f(x_1,...,x_n) is defined by a joint probability distribution R=(R_1,...,R_n) and local encoding functions ENC_i(x_i,r_i). For a set T, the scheme is said to be T-robust if, when sampling r_1,...,r_n from R, revealing the messages ENC_i(x_i,r_i), for i not in T, together with the randomness r_i, for i in T, gives the same information about the x_i's, for i not in T, as an oracle access to the function f restricted to these input values. The scheme is t-robust if it is T-robust for every T of size at most t and is fully robust if it is n-robust.

A t-robust distributed obfuscation naturally gives rise to a non-interactive t-robust protocol for f: given a correlated randomness setup specified by R, each party P_i on input x_i reveals the message m_i=ENC_i(x_i,r_i). The n messages m_i can be used to decode f(x_1,...,x_n). The t-robustness guarantees that each set of at most t corrupted parties can learn no more than the restriction of f fixing the inputs of uncorrupted parties, which, in this non-interactive setting, one cannot hope to hide.

We consider {information-theoretic} distributed obfuscation and obtain unconditional positive results for some special cases of interest:
-- efficient, fully robust distributed obfuscation scheme for group products.
-- fully robust distributed obfuscation whose complexity is polynomial in the size of the input domain (i.e., efficient only for ``small'' functions).
-- a t-robust distributed obfuscation of complexity n^{O(t)} for symmetric functions (i.e., a polynomial-time scheme for any constant t).

On the negative side, we show that natural attempts to realize distributed obfuscation using private simultaneous messages protocols and garbling schemes from the literature fail to achieve even 1-robustness.