abstract

COMPUTER SCIENCE AND DISCRETE MATHEMATICS SEMINAR I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We prove completeness results for certain class of functions which have implications for automatic proving of universally-composable security theorems for ideal and real functionalities composed of if-then-else programs with (uniform) random number generation and data objects from additive group of GF(2^m) . The theorems imply that, within this language framework, there is a decision procedure to find out if a real functionality realizes an ideal functionality, and this procedure is in computational time independent of m (which is essentially the security parameter).

Since most cryptographic functionalities have such simple if-then-else probabilistic form, this approach has widespread practical theorem proving appeal. The completeness theorems are of the following form. Let f_1, f_2,...,f_k be k pseudo-linear functions in n variables, and let f be another pseudo-linear function in the n variables. We show that if f is a function of the given k functions, then it must be a pseudo-linear function of the given k functions. This generalizes the straightforward claim for just linear functions. We also prove a more general theorem where the k functions can in addition take further arguments, and prove that if f can be represented as an iterated composition of these k functions, then it can be represented as a probabilistic pseudo-linear iterated composition of these functions. Proceeding further, we generalize the theorem to randomized pseudo-linear functions. (Joint work with Arnab Roy, IBM Research)