In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

ITCSC-CSE Joint Seminar

Random Oracles in the Real World through the Eyes of Obfuscation

By
Mr. Arno Mittelbach
Ph.D. Student, TU Darmstadt

December 1, 2014, Monday

3:00 pm – 4:00 pm

Room 1009, 10/F,
William M.W. Mong Engineering Building, CUHK

Abstract:
Modern Cryptography is said to be based on three principles: 1) Formulation of Exact Definitions 2) Reliance on Precise Assumptions and 3) Rigorous Proofs of Security. Principles are, however, a hard thing to stick to so modern cryptography sometimes relaxes principles 2 and 3 in that proofs are given in an idealized model such as the random oracle model. Here, during the security proof, we assume that all parties get oracle access to a completely random function, i.e., a function where every input is mapped to a completely random output (and that even if each output would be written on one atom would take more than the available atoms in the universe to describe). Then, when instantiating the scheme in the real world we simply replace the idealized random function that we used in the proof by a common fixed hash function, such as SHA3, and "hope" that this results in a secure scheme. The random oracle model (ROM) is a source of great controversy as proofs in the ROM, in theory, do not give any security guarantees in the real world. Yet, from an empirical point of view the random oracle model seems to be at the very least a good heuristic as known failures are usually rather artificial.

In this talk I want to explore the random oracle controversy via the rediscovered tool of indistinguishability obfuscation, a technique to make programs unintelligible. Obfuscation can be used to expose some of the inherent contradictions within the random oracle model. At the same time obfuscation may allow us to overcome random oracles in a broad spectrum of applications by either being used directly in the specification of schemes or in the creation of new primitives such as UCEs (Universal Computational Extractors) which aim at modelling some of the properties possessed by random oracles while bypassing their inconsistencies.

Biography:
Arno Mittelbach is a Ph.D. student at TU Darmstadt, Germany, in Professor Marc Fischlin's group "Cryptography and Complexity Theory". His research interests are the theoretical foundations of hash functions and, lately, indistinguishability obfuscation.

******* ALL ARE WELCOME *******