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

Efficient Pseudorandom Functions via On-the-Fly Adaptation

By
Prof. Dominique Schröder
Saarland University

December 7, 2015, Monday
2:00 pm – 3:00 pm
Room 833, 8/F, Ho Sin Hang Engineering Building, CUHK

Abstract:
Pseudorandom functions (PRFs) are one of the most fundamental building blocks in cryptography with numerous applications such as message authentication codes and private key encryption. In this work, we propose a new framework to construct PRFs with the overall goal to build efficient PRFs from standard assumptions with an almost tight proof of security. The main idea of our framework is to start from a PRF for any small domain (i.e. poly-sized domain) and turn it into an l-bounded pseudorandom function, i.e., into a PRF whose outputs are pseudorandom for the first l distinct queries to F. In the second step, we apply a novel technique which we call on-the-fly adaptation that turns any bounded PRF into a fully-fledged (large domain) PRF. Both steps of our framework have a tight security reduction, meaning that any successful attacker can be turned into an efficient algorithm for the underlying hard computational problem without any significant increase in the running time or loss of success probability.

Instantiating our framework with specific number theoretic assumptions, we construct a PRF based on k-LIN (and thus DDH) that is faster than all known constructions, which reduces almost tightly to the underlying problem, and which has shorter keys. Instantiating our framework with general assumptions, we construct a PRF with very flat circuits whose security tightly reduces to the security of some small domain PRF.

Biography:
Dominique Schröder is an Associate Professor (with tenure) of Computer Science at Saarland University in Germany and he is also a PI of the Center for IT-Security, Accountability, and Privacy (CISPA). Before joining Saarland University as an Assistant Professor in 2012, he was a postdoctoral fellow of the German Academic Exchange Service (DAAD) under Jonathan Katz at the University of Maryland, USA. In November 2010, Dominique completed his Ph.D. with grade “summa cum laude” at Darmstadt University of Technology, Germany, under Marc Fischlin.

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

Hosted & Enquiries : Institute of Theoretical Computer Science and Communications Tel: 3943 1257