abstract

COMPUTER SCIENCE AND DISCRETE MATHEMATICS SEMINAR I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

This paper revisits the construction of Universally One-Way Hash Functions (UOWHFs) from any one-way function due to Rompel (STOC 1990). We give a simpler construction of UOWHFs which also obtains better efficiency and security. The construction exploits a strong connection to the recently introduced notion of *inaccessible entropy* (Haitner et al. STOC 2009). With this perspective, we observe that a small tweak of any one-way function f is already a weak form of a
UOWHF: Consider F(x, i) that outputs the i-bit long prefix of f(x). If F were a UOWHF then given a random x and i it would be hard to come up with x' \neq x such that F(x, i) = F(x', i). While this may not be the case, we show (rather easily) that it is hard to sample x' with almost full entropy among all the possible such values of x'. The rest of our construction simply amplifies and exploits this basic property.

With this and other recent works we have that the constructions of three fundamental cryptographic primitives (Pseudorandom Generators, Statistically Hiding Commitments and UOWHFs) out of one-way functions are to a large extent unified. In particular, all three constructions rely on and manipulate computational notions of entropy in similar ways. Pseudorandom Generators rely on the well-established notion of pseudoentropy, whereas Statistically Hiding Commitments and UOWHFs rely on the newer notion of inaccessible entropy.

Joint work with Iftach Haitner, Thomas Holenstein, Omer Reingold and Salil Vadhan (Eurocrypt 2010)