abstract

COMPUTER SCIENCE/DISCRETE MATH SEMINAR, I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We prove a number of general theorems about CZK, the class of problems possessing computational zero-knowledge proofs. Our results are *unconditional*, in contrast to most previous works on CZK which rely on the assumption that one-way functions exist.

We establish several new characterizations of CZK, and use these characterizations to prove results such as:

-- Honest-verifier CZK equals general CZK.

-- Public-coin CZK equals private-coin CZK.

-- CZK is closed under union (and more generally, "monotone formula closure").

-- CZK with imperfect completeness equals CZK with perfect completeness.

-- Any problem in [CZK intersect NP] can be proven in computational zero knowledge by a BPP^NP prover.

-- CZK with black-box simulators equals CZK with general, non-black-box simulators.

The above equalities refer to the resulting *class* of problems (and do not necessarily preserve other efficiency measures such as round complexity).

Our approach is to combine the conditional techniques previously used in the study of CZK

with the unconditional techniques developed in the study of SZK, the class of problems possessing statistical zero-knowledge proofs. To enable this combination, we prove that every problem in CZK can be decomposed into a a problem in SZK together with a set of instances from which a one-way function can be constructed.