abstract

COMPUTER SCIENCE/DISCRETE MATH SEMINAR, I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We study the parallel time-complexity of basic cryptographic primitives such as one-way functions (OWFs) and pseudorandom generators (PRGs). Specifically, we consider the possibility of computing instances of these primitives by NC0 circuits, in which each output bit depends on a constant number of input bits. Despite previous efforts in this direction, there has been no significant theoretical evidence supporting this possibility, which was posed as an open question in several previous works.

We essentially settle this question by providing overwhelming evidence for the possibility of cryptography in NC0. Our main result is that every "moderately easy" OWF (resp., PRG), say computable in NC1, can be compiled into a corresponding OWF (resp., low-stretch PRG) in which each output bit depends on only four input bits. The existence of OWF and PRG in NC1 is a relatively mild assumption, implied by most number-theoretic or algebraic intractability assumptions commonly used in cryptography. A similar compiler can also be obtained for other cryptographic primitives such as one-way permutations, encryption, commitment, and collision-resistant hashing.

Our techniques can also be applied to obtain unconditionally provable constructions of non-cryptographic PRGs. In particular, we obtain epsilon-biased generators where each output bit depends on 3 input bits, resolving an open question of Mossel et al.

Our results make use of the machinery of randomizing polynomials, which was originally motivated by questions in the domain of information-theoretic secure multiparty computation.

Joint work with Benny Applebaum and Eyal Kushilevitz