1011-68-277 **Emanuele Viola*** (viola@eecs.harvard.edu), Maxwell Dworkin 140, 33 Oxford Street, Cambridge, MA 02138. *Pseudorandom bits for low complexity classes: new results and applications.*

A pseudorandom generator (PRG) is an efficient deterministic algorithm that stretches a randomly chosen seed into a much longer sequence, which nevertheless fools any efficient 'observer,' in the sense that the observer cannot distinguish it from truly random. The type of observer varies. PRGs that fool general circuits would have a striking variety of applications, but such PRGs are only known to exist based on unproven assumptions. On the other hand, PRGs that fool more restricted observers are sometimes known to exist unconditionally, and they also have many applications.

In this talk I will present a new PRG that fools any poly(n)-size constant-depth circuit with log(n) 'arbitrary symmetric gates.' Here, an arbitrary symmetric gate is a gate that computes an arbitrary symmetric function, such as Parity or Majority. Our PRG improves on a PRG by Luby, Velickovic and Wigderson (ISTCS '93) that only fools circuits of depth 2 with 1 arbitrary symmetric gate.

Our PRG implies that any function computable by a poly(n)-size *probabilistic* constant-depth circuit with log(n) arbitrary symmetric gates can be computed *deterministically* in subexponential time. This seems to be the richest probabilistic circuit class known to be contained in deterministic subexponential time. (Received August 29, 2005)