1046-68-1973 **Antonio R. Nicolosi*** (nicolosi@cs.stevens.edu), Computer Science Department, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030. *Average-Case vs. Generic-Case Complexity of Lattice Problems.* Preliminary report.

Lattice problems whose average-case complexity is connected to worst-case assumptions are appealing foundations for provably secure cryptosystems. A sharper understanding of their inherent hardness would enable more precise security analyses, thus resulting in more efficient cryptographic primitives.

In this talk, we review the landscape of the average-case complexity of lattice problems, sketch some of the technical tools employed in their analysis, and discuss our on-going efforts to assess their generic-case complexity. (Received September 16, 2008)