1077-68-2091 **Daniele Micciancio*** (daniele@cs.ucsd.edu), UCSD, 9500 Gilman Dr., Mail Code 0404, La Jolla, CA 92093. *Lattice Cryptography and Pseudorandomness.*

Most lattice cryptography is based on the evaluation of simple linear functions like $f_a(x_1, \ldots, x_n) = \sum_i a_i \cdot x_i$, where the x_i are small integers and the a_i are randomly chosen elements from an abelian group G which describe the function f_a. The versatility of lattice cryptography in the solution of a wide range of security problems comes from the fact that, not only the function f is typically one-way (i.e., computationally hard to invert), but it also produces a pseudorandom output: it is computationally hard to distinguish $(a_1, \ldots, a_n, f_a(x_1, \ldots, x_n))$ from a randomly chosen sequence of $n + 1$ group elements. A fundamental question in lattice cryptography is: for what choices of the group G and input distribution $(x_1, \ldots, x_n)$, it is possible to prove that if f is a one-way function, then its output is pseudorandom? In this talk I will survey the current state of the art regarding this question, present an overview of the known techniques used in the study of this problem, and describe the main open problems in the area. (Received September 21, 2011)