NTL: a Library for Doing Number Theory

Victor Shoup

Courant Institute, USA
shoup@cs.nyu.edu

NTL is a high-performance C++ library for doing arithmetic on polynomial over various rings (integers and finite fields), as well as a number of other algebraic structures. I will discuss the history of NTL, as well as some of the basic elements of its design and the algorithms it employs. I will also discuss recent work on making NTL exploit multicore and SIMD computer architectures, as well as NTL's use in implementing fully homomorphic encryption schemes.