Modular Arithmetic

Paul Zimmermann, INRIA

This talk will describe the state-of-art of modular arithmetic, which is a basic tool for several applications in algorithmic number theory and cryptography. Classical algorithms will be described (Barrett, Montgomery), as well as less known or recent ones (Svoboda, Mihailescu, ...). Material for this talk is largely based on Chapter 2 of the book *Modern Computer Arithmetic* in preparation with Richard Brent (`http://www.loria.fr/~zimmerma/mca/pub226.html`).