Call for Papers

This workshop is a forum of mathematicians, computer scientists, engineers and physicists performing research on finite field arithmetic, interested in communicating the advances in the theory, applications, and implementations of finite fields. The workshop will help to bridge the gap between the mathematical theory of finite fields, their hardware/software implementations and technical applications. The topics of WAIFI 2012 include but are not limited to:

**Theory of finite field arithmetic:**
- Bases (canonical, normal, dual, etc.)
- Polynomial factorization, irreducible polynomials
- Primitive elements
- Prime fields, binary fields, extension fields, etc.
- Elliptic and hyperelliptic curves

**Hardware & software implementations:**
- Design & implementation of finite field processors
- Design & implementation of arithmetic algorithms

**Applications of finite fields:**
- Pseudorandom number generators
- Hardware/software co-design
- IP (Intellectual Property) components
- Field programmable and reconfigurable systems

Authors are invited to submit original research papers. A detailed description of the electronic submission procedure will appear on the WAIFI webpage. The submission should begin with a title, author list, a short abstract, and a list of keywords. The paper should be at most 16 pages, using at least 11-point font and reasonable margins. The proceedings will be published in the Springer Lecture Notes in Computer Science (LNCS) series.

- Submission deadline: **February 27th, 2012**
- Acceptance notification: **April 9th, 2012**
- Final version due: **April 23th, 2012**
- Workshop presentations: **July 16-19, 2012**

In order to be included in the proceedings, the authors of an accepted paper must guarantee to present their contribution at the workshop. More detailed information on instructions for authors, paper submission, technical program, accommodation, travel and registration will be posted on the Workshop web site: [http://www.waifi.org](http://www.waifi.org)