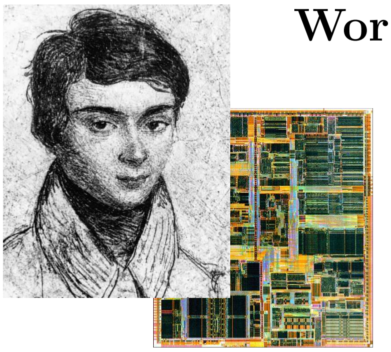

Workshop on the Arithmetic of Finite Fields
WAIFI 2007

www.waifi.org

Madrid, Spain
June 21-22, 2007

Call for Papers

The focus of this workshop is to have a forum bringing together mathematicians, engineers and physicists researching on finite field arithmetic, to communicate and advance in the theory, applications and implementations of such fields. The workshop will help to bridge the gap between the mathematical theory of finite fields and their hardware/software implementations and technical applications.

The topics of WAIFI 2007 include but are not limited to:

Theory of finite field arithmetic:
- ○ *Optimal bases (canonical, normal, dual, etc.)*
- ○ *Optimal 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*
- ○ *Pseudorandom number generators*
- ○ *Hardware/Software Co-design*
- ○ *IP (Intellectual Property) components*
- ○ *Field programmable and reconfigurable systems*

Applications of finite fields:
- ○ *Cryptography*
- ○ *Communication systems*
- ○ *Error correcting codes*
- ○ *Quantum computing*

Authors are invited to submit **original research** papers. Electronic submission will be strongly encouraged. A detailed description of the electronic submission procedure will apear 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 12 pages (excluding the bibliography and clearly marked appendices), and at most 15 pages in total, using at least 11-point font and reasonable margins.

- ○ Submission deadline: **February 14th, 2007**
- ○ Acceptance notification: March 23th, 2007
- ○ Final version due: April 4th, 2007

The proceedings will be published in the Springer **Lecture Notes in Computer Science (LNCS)** series in time for distribution at the workshop.

Notice that 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, accomodation, travel and registration will be posted on the Workshop web site: http://www.waifi.org

Program Committee:
- ○ Jean-Claude Bajard, *CNRS-LIRMM in Montpellier, France*
- ○ Ian F. Blake, *University of Toronto, Canada*
- ○ Marc Daumas, *CNRS-LIRMM in Perpignan, France*
- ○ Jean-Pierre Deschamps, *University Rovira i Virgili, Spain*
- ○ Josep Domingo, *University Rovira i Virgili, Spain*
- ○ Philippe Gaborit, *University of Limoges, France*
- ○ Joachim von zur Gathen, *B-IT, University of Bonn, Germany*
- ○ Pierrick Gaudry, *LORIA-INRIA, France*
- ○ Guang Gong, *University of Waterloo, Canada*
- ○ Jorge Guajardo, *Philips Research, Netherlands*
- ○ Anwar Hasan, *University of Waterloo, Canada*
- ○ Çetin K. Koç, *Oregon State University, USA*
- ○ Tanja Lange, *Technical University of Denmark, Denmark*
- ○ Julio López, *UNICAMP, Brasil*
- ○ Gary Mullen, *Pennsylvania State University, USA*
- ○ Harald Niederreiter, *National University of Singapore, Singapore*
- ○ Ferruh Ozbudak, *Middle East Technical University, Turkey*
- ○ Erkay Savas, *Sabanci University, Turkey*
- ○ Igor Shparlinski, *Macquarie University, Australia*
- ○ Horacio Tapia-Recillas, *UAM-Iztapalapa, D.F., Mexico*
- ○ Apostol Vourdas, *University of Bradford, UK*

General co-Chairs:
- ○ José L. Imaña, *Complutense University of Madrid, Spain*
- ○ Çetin K. Koç, *Oregon State University, USA*

Financial, Local arrangements Chairs:
- ○ Luis Piñuel, *Complutense University of Madrid, Spain*
- ○ Manuel Prieto, *Complutense University of Madrid, Spain*

Program co-Chairs:
- ○ Claude Carlet, *University of Paris 8, France*
- ○ Berk Sunar, *Worcester Polytechnic Institute, USA*

Publicity Chair:
- ○ Gustavo Sutter, *Autonomous University of Madrid, Spain*