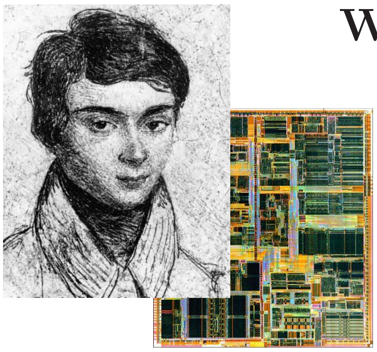

Workshop on the Arithmetic of Finite Fields
WAIFI 2008

www.waifi.org

Siena, Italy
July 6-9, 2008

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 and their hardware/software implementations and technical applications.

This will be the second WAIFI workshop. WAIFI 2007 was held in Madrid (Spain). The topics of WAIFI 2008 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*
○ *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 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.

○ Submission deadline: **February 18th, 2008**
○ Acceptance notification: April 4th, 2008
○ Final version due: April 14th, 2008

The WAIFI 2007 proceedings appeared as a volume of the Springer **Lecture Notes in Computer Science (LNCS)**. We expect the same for WAIFI 2008.

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:
○ Omran Ahmadi, *University of Waterloo, Canada*
○ Daniel Augot, *INRIA-Rocquencourt, France*
○ Jean-Claude Bajard, *University of Montpellier II, France*
○ Luca Breveglieri, *Politecnico di Milano, Italy*
○ Stephen Cohen, *University of Glasgow, UK*
○ Ricardo Dahab, *Universidade Estadual de Campinas, Brasil*
○ Gianluca Dini, *University of Pisa, Italy*
○ Serdar Erdem, *Gebze Institute of Technology, Turkey*
○ Joachim von zur Gathen (Program co-Chair)
○ Elisa Gorla, *University of Zürich, Switzerland*
○ Dirk Hachenberger, *University of Augsburg, Germany*
○ Anwar Hasan, *University of Waterloo, Canada*
○ Marc Joye, *Thomson R&D, France*
○ Çetin Kaya Koç (Program co-Chair)
○ Arjen Lenstra, *EPFL, Switzerland*
○ Peter Montgomery, *Microsoft Research, USA*
○ Ferruh Özbudak, *Middle East Technical University, Turkey*
○ Francesco Pappalardi, *University of Roma 3, Italy*
○ Francisco Rodríguez-Henríquez, *Cinvestav, Mexico*
○ René Schoof, *University of Roma 2, Italy*
○ Eric Schost, *University of Western Ontario, Canada*
○ Jamshid Shokrollahi, *Ruhr-University Bochum, Germany*
○ Berk Sunar, *Worcester Polytechnic Institute, USA*
○ Chris Umans, *California Institute of Technology, USA*
○ Colin Walter, *Comodo Research Lab, UK*

General co-Chairs:
○ José L. Imaña, *Complutense University of Madrid, Spain*
○ Enrico Martinelli, *University of Siena, Italy*

Financial, Local arrangements Chairs:
○ Sandro Bartolini, *University of Siena, Italy*
○ Roberto Giorgi, *University of Siena, Italy*

Program co-Chairs:
○ Joachim von zur Gathen, *B-IT, University of Bonn, Germany*
○ Çetin Kaya Koç, *Oregon State University, USA*

Publicity Chair:
○ Claude Carlet, *University of Paris 8, France*