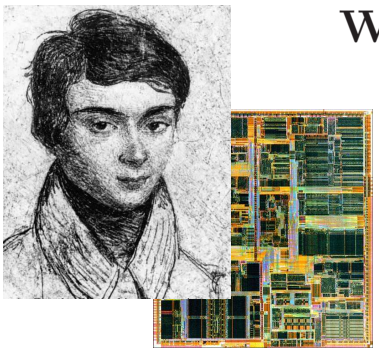
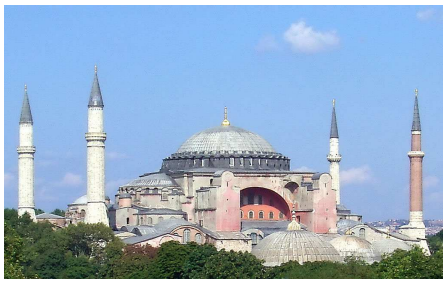


Workshop on the Arithmetic of Finite Fields
WAIFI 2010

www.waifi.org

Istanbul, Turkey
June 27-30, 2010

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 3rd WAIFI workshop. WAIFI 2007 was held in Madrid (Spain), and WAIFI 2008 was held in Siena (Italy). The topics of WAIFI 2010 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 8th, 2010**
- Acceptance notification: March 25th, 2010
- Final version due: April 7th, 2010

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

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:
- Daniel Augot, *INRIA, France*
- Roberto Avanzi, *Ruhr-University Bochum, Germany*
- Jean-Claude Bajard, *LIP6 CNRS/U. Pierre et Marie Curie, France*
- Luca Breveglieri, *Politecnico di Milano, Italy*
- Stephen Cohen, *University of Glasgow, Scotland, UK*
- Cunsheng Ding, *Hong Kong Univ. of Science and Technology, China*
- Serdar Erdem, *Gebze Institute of Technology, Turkey*
- Haining Fan, *Tsinghua University, China*
- Olav Geil, *Aalborg University, Denmark*
- Guang Gong, *University of Waterloo, Canada*
- Jorge Guajardo, *Philips Research, The Netherlands*
- Darrel Hankerson, *Auburn University, USA*
- Anwar Hasan (Program co-Chair)
- Tor Helleseth (Program co-Chair)
- José L. Imaña, *Complutense University of Madrid, Spain*
- Alexander Kholosha, *University of Bergen, Norway*
- P. Vijay Kumar, *Indian Institute of Science, Bangalore, India*
- Tanja Lange, *Technical Univ. of Eindhoven, The Netherlands*
- Julio López, *UNICAMP, Brasil*
- Gary McGuire, *University College Dublin, Ireland*
- Eiji Okamoto, *University of Tsukuba, Japan*
- Alexander Pott, *University of Magdeburg, Germany*
- Francisco Rodríguez-Henríquez, *Cinvestav, Mexico*
- Erkay Savas, *Sabanci University, Turkey*
- Igor Semaev, *University of Bergen, Norway*
- Patrick Solé, *Télécom ParisTech, France*

General co-Chairs:
- Çetin K. Koç, *UCSB, USA, & Istanbul Şehir University, Turkey*
- Ferruh Özbudak, *Middle East Technical University, Turkey*

Program co-Chairs:
- Anwar Hasan, *University of Waterloo, Canada*
- Tor Helleseth, *University of Bergen, Norway*

Financial, Local arrangements Chairs:
- Murat Cenk, *Çankaya University, Turkey*
- Gökay Saldamlı, *Boğaziçi University, Turkey*
- Zülfükar Saygı, *TOBB ETU, Turkey*

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