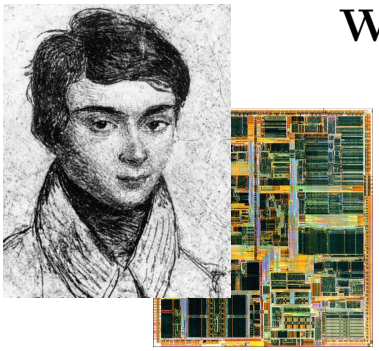

Workshop on the Arithmetic of Finite Fields
WAIFI 2014

www.waifi.org

Tübitak Bilgem, Gebze, Turkey
September 26-28, 2014

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 5th WAIFI workshop. WAIFI 2007, WAIFI 2008, WAIFI 2010, and WAIFI 2012 were held in Madrid (Spain), Siena (Italy), Istanbul (Turkey), and Bochum (Germany), respectively. The topics of WAIFI 2014 include but are not limited to:

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

Hardware & software implementations:
- *Optimal arithmetic modules*
- *Design & implementation of finite field arithmetic processors*
- *Design & implementation of arithmetic algorithms*
- *Pseudorandom number generators*
- *Hardware/software co-design*
- *IP (Intellectual Property) components*
- *Field programmable and reconfigurable systems*

Applications:
- *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: **July 11th, 2014**
- Acceptance notification: August 11th, 2014
- Final version due: September 1st, 2014

The proceedings will be published in the Springer **Lecture Notes in Computer Science (LNCS)** series after the workshop as post-proceedings.

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 and LIX, France*
- Lejla Batina, *Radboud University Nijmegen, The Netherlands*
- Luca Breveglieri, *Politecnico di Milano, Italy*
- Claude Carlet, *University of Paris 8, France*
- Murat Cenk, *Middle East Technical University, Turkey*
- Gérard Cohen, *Telecom ParisTech, France*
- Philippe Gaborit, *University of Limoges, France*
- Pierrick Gaudry, *CNRS, Nancy, France*
- Tor Helleseth, *University of Bergen, Norway*
- Hüseyin Hışıl, *Yaşar University, Turkey*
- Mehran Mozaffari Kermani, *Rochester Institute of Technology, USA*
- Alexander Kholosha, *University of Bergen, Norway*
- Gregor Leander, *Ruhr University Bochum, Germany*
- Julio López, *University of Campinas, Brazil*
- Arash Reyhani-Masoleh, *Western University, Canada*
- Wilfried Meidl, *Sabancı University, Turkey*
- Sihem Mesnager, *University of Paris VIII, France*
- Christophe Negre, *Universit de Perpignan, France*
- Harald Niederreiter, *RICAM, Austrian Academy of Sciences, Austria*
- Erdinç Öztürk, *Istanbul Commerce University, Turkey*
- Alexander Pott, *Otto-von-Guericke University , Germany*
- Francisco Rodríguez-Henríquez, *CINVESTAV-IPN, Mexico*
- Erkay Savaş, *Sabancı University, Turkey*
- Zülfükar Saygı, *TOBB ETU, Turkey*
- Kai-Uwe Schmidt, *Otto-von-Guericke University, Germany*
- Leo Storme, *Ghent University, Belgium*
- Jean-Pierre Tillich, *INRIA-Rocquencourt, France*

General Chair:
- Çetin K. Koç, *University of California Santa Barbara, USA*

Financial, Local Arrangements Chairs:
- Şükran Külekçi, *Mathematical & Computational Sciences Labs, Tübitak Bilgem, Turkey*
- Mehmet Sabır Kiraz, *Mathematical & Computational Sciences Labs, Tübitak Bilgem, Turkey*

Program co-Chairs:
- Sihem Mesnager, *University of Paris VIII, France*
- Erkay Savaş, *Sabancı University, Turkey*

Publicity Chair:
- Jean-Jacques Quisquater, *Université catholique de Louvain, Belgium*