



Workshop on the Arithmetic of Finite Fields

WAIFI 2012

In Cooperation with the IACR



www.waifi.org

Bochum, Germany, July 16-19, 2012

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

- 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. 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

Confirmed Invited Speakers:

- Prof. Florian Heß, *Universität Oldenburg, Germany*
- Prof. Alexander Pott, *Universität Magdeburg, Germany*
- Prof. Emmanuel Thomé, *INRIA, France*

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, *LIP6 CNRS/U. Pierre et Marie Curie, France*
- Stephane Ballet, *Institut de Mathématiques de Luminy, France*
- Jean-Luc Beuchat, *University of Tsukuba, Japan*
- Luca Breveglieri, *Politecnico di Milano, Italy*
- Debrup Chakraborty, *CINVESTAV-IPN, Mexico*
- Ricardo Dahab, *University of Campinas, Brasil*
- Jérémie Detrey, *INRIA, France*
- Haining Fan, *Tsinghua University, China*
- Olav Geil, *Aalborg University, Denmark*
- Guang Gong, *University of Waterloo, Canada*
- Jorge Guajardo, *Robert Bosch LLC, USA*
- Anwar Hasan, *University of Waterloo, Canada*
- Tor Helleseth, *University of Bergen, Norway*
- José L. Imaña, *Complutense University of Madrid, Spain*
- Koray Karabina, *University of Waterloo, Canada*
- Alexander Kholosha, *University of Bergen, Norway*
- Tanja Lange, *Tech. Univ. of Eindhoven, The Netherlands*
- Ivan Langjev, *Bulgarian Academy of Sciences, Bulgaria*
- Julio López, *University of Campinas, Brasil*
- Edgar Martínez-Moro, *University of Valladolid, Spain*
- Gary Mullen, *Pennsylvania State University, USA*
- Harald Niederreiter, *Austrian Academy of Sciences, Austria*
- Arash Reyhani-Masoleh, *Univ. of Western Ontario, Canada*
- Erkay Savas, *Sabanci University, Turkey*
- Peter Schwabe, *Academia Sinica, Taiwan*
- Igor Semaev, *University of Bergen, Norway*
- Patrick Solé, *Télécom ParisTech, France & AbdelAziz University, Saudi Arabia*
- Arne Winterhof, *Austrian Academy of Sciences, Austria*

General Chair:

- Christopher Wolf, *Ruhr Universität Bochum, Germany*

Publicity Chair:

- Jean-Jacques Quisquater, *UCL Crypto Group, Belgium*

Program co-Chairs:

- Ferruh Özbudak, *Middle East Technical University, Turkey*
- Francisco Rodríguez-Henríquez, *CINVESTAV-IPN, Mexico*