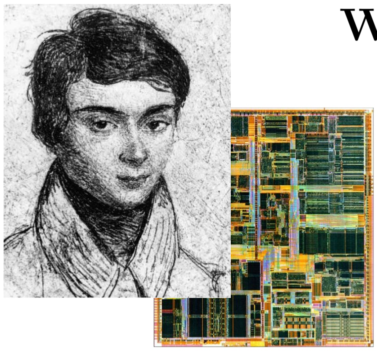

Workshop on the Arithmetic of Finite Fields
WAIFI 2016

www.waifi.org

Ghent, Belgium
July 13-15, 2016

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 6th WAIFI workshop after Madrid (Spain, 2007), Siena (Italy, 2008), Istanbul (Turkey, 2010), Bochum (Germany, 2012) and Gebze (Turkey, 2014). The topics of WAIFI 2016 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, tower fields ...*
○ *Elliptic and hyperelliptic curves*

Hardware & software implementations:
○ *Optimal arithmetic modules*
○ *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*
○ *Finite geometry*
○ *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: **May 1st, 2016, 12.00 CET.**
○ Acceptance notification: **June 11th**, 2016
○ Final pre-proceedings version due: June 20th, 2016
○ Final post-proceedings version due: August 8th, 2016

The proceedings will be published in the Springer **Lecture Notes in Computer Science (LNCS)** series after the workshop as post-proceedings.
A draft will be available during 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:
○ Tsonka Baicheva, *Bulgarian Academy of Sciences, Bulgaria*
○ Jean-Claude Bajard, *University Pierre et Marie Curie, France*
○ Josep Balasch, *KU Leuven, Belgium*
○ Anne Canteaut, *INRIA Rocquencourt, France*
○ Claude Carlet, *University of Paris 8, France*
○ Luca De Feo, *University of Versailles-Saint Quentin, France*
○ Sylvain Duquesne (Program co-Chair), *University Rennes 1, France*
○ Tor Helleseth, *University of Bergen, Norway*
○ Sophie Huczynska, *University of St Andrews, Scotland*
○ Alexander Kholosha, *University of Bergen, Norway*
○ Miroslav Knezevic, *KU Leuven and NXP Semiconductors, Belgium*
○ Gohar Kyureghyan, *University of Magdeburg, Germany*
○ Ivan Landzhev,*New Bulgarian University, Bulgaria*
○ Gregor Leander, *Ruhr University Bochum, Germany*
○ Sihem Mesnager, *University of Paris 8, France*
○ Amir Moradi, *Ruhr University Bochum, Germany*
○ Gary Mullen, *Penn State University, USA*
○ Svetla Nikova (Program co-Chair), *KU Leuven, Belgium*
○ Daniel Panario, *Carleton University, Canada*
○ Ruud Pellikaan, *Technical University Eindhoven, Netherlands*
○ Alexander Pott, *Otto-von-Guericke University, Germany*
○ Christophe Ritzenthaler, *University of Rennes 1, France*
○ Leo Storme, *Ghent University, Belgium*
○ Arnaud Tisserand, *CNRS, University of Rennes 1, France*
○ Frederik Vercauteren, *KU Leuven, Belgium*
○ Paul Zimmermann, *INRIA Nancy - Grand Est, France*

General co-Chairs:
○ Vincent Rijmen, *KU Leuven, Belgium*
○ Leo Storme, *Ghent University, Belgium*

Program co-Chairs:
○ Sylvain Duquesne, *University of Rennes 1, France*
○ Svetla Nikova, *KU Leuven, Belgium*

Publicity Chair:
○ Jean-Jacques Quisquater, *KU Leuven, Belgium*