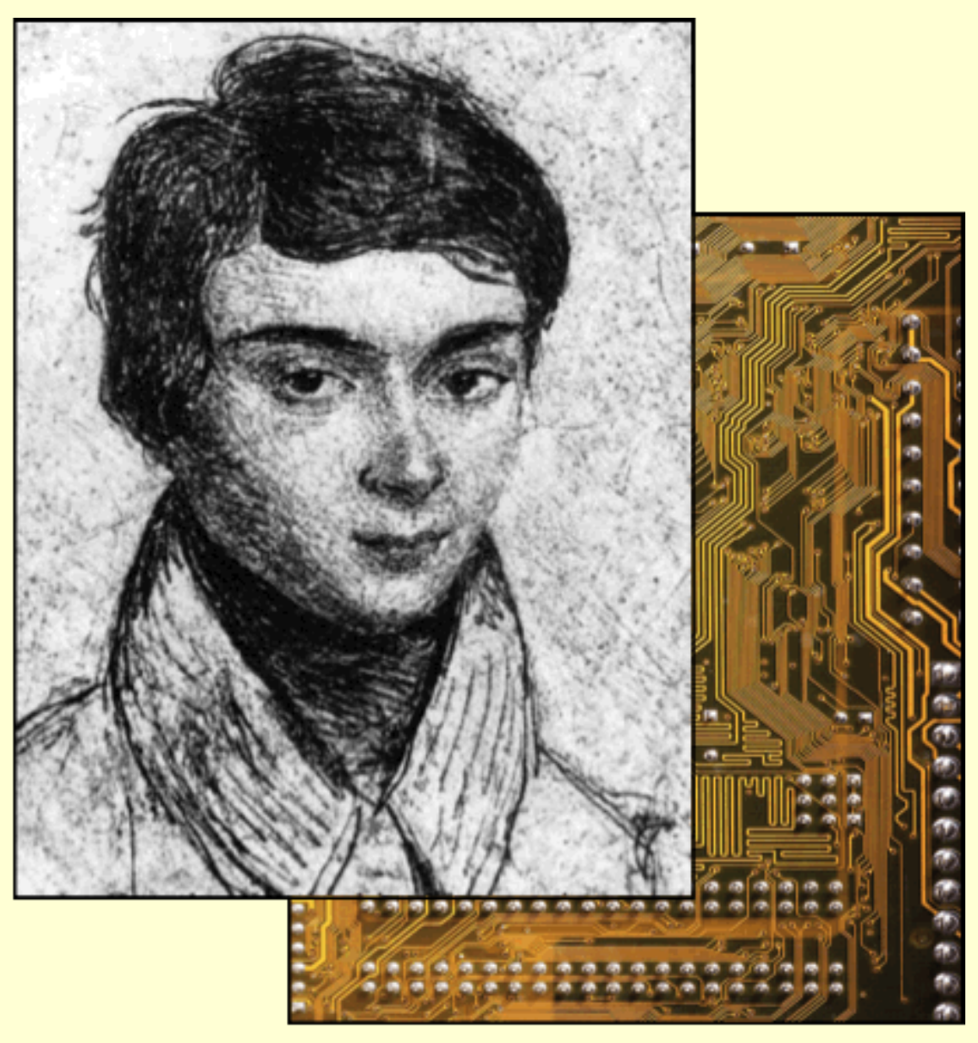

WAIFI 2020

International Workshop on the Arithmetic of Finite Fields

Rennes, France. July 6-8, 2020

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.

The topics of WAIFI 2020 include but are not limited to:

Theory of finite field arithmetic:

- Bases (normal bases, duality, complexity…)
- Polynomial factorization, irreducible polynomials
- Primitive polynomials, permutation polynomials
- Special functions over finite fields (Boolean functions, APN functions, …)
- Curves over finite fields
- Algebraic dynamical systems over finite fields

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 of finite fields:

- Cryptography
- Communication systems
- Error correcting codes
- Finite geometry
- Quantum computing

Important Dates

- ~~Submission deadline: March 8, 2020 (GMT time)~~
- ~~Acceptance notification: April 29, 2020~~
- ~~Final pre-proceedings version due: June 1, 2020~~
- Final post-proceedings version due: August 5, 2020
- Submission deadline: March 22, 2020 (GMT time)
- NEW Acceptance notification: June 1, 2020
- NEW Final pre-proceedings version due: June 25, 2020
- NEW Registration deadline: June 30, 2020

Workshop Proceedings

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

Authors are invited to submit original research papers. A detailed description of the electronic submission procedure will appear on the **WAIFI** webpage: `http://www.waifi.org`. The paper should be at most 16 pages, using at least 11-point font and reasonable margins.

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, accommodation, travel and registraion will be posted on the Workshop website: `http://www.waifi.org`.

Plenary Speakers

- André Chailloux (Inria Paris, France)
- Elisa Gorla (University of Neuchatel, Switzerland)
- Gary McGuire (University College Dublin, Ireland)
- Emmanuela Orsini (KU Leuven, Belgium)
- Erich Schost (University of Waterloo, Canada)

Committees

General Chairs:

- Sylvain Duquesne, Rennes 1 University, France
- Arnaud Tisserand, CNRS, Lab-STICC, Lorient, France

Organizing Committee:

- Elisa Lorenzo Garcia, Rennes 1 University, France
- Felix Ulmer, Rennes 1 University, France
- Pierre Alain Fouque, Rennes 1 University, France
- Adeline Langlois-Roux, CNRS IRISA, Rennes, France
- Karim Bigou, Brest University, France

Program co-Chairs:

- Jean Claude Bajard, Sorbonne University, France
- Alev Topuzoglu, Sabancı University, Turkey