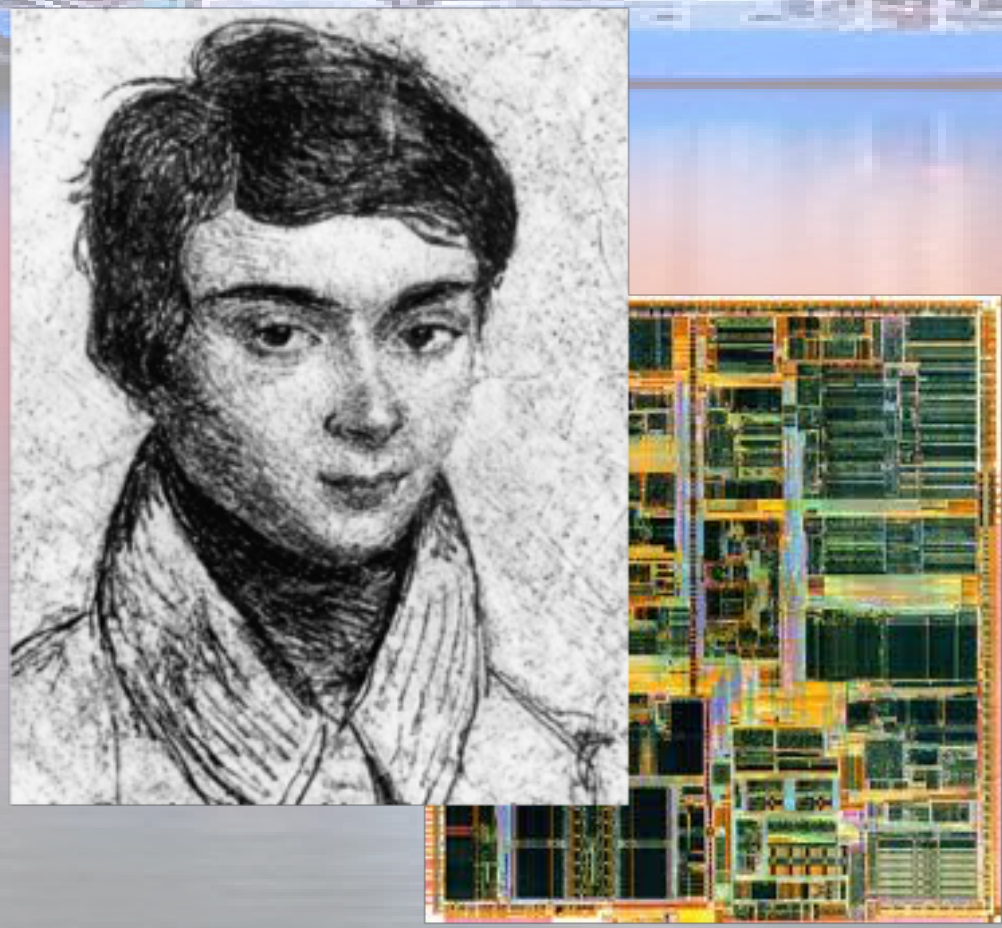
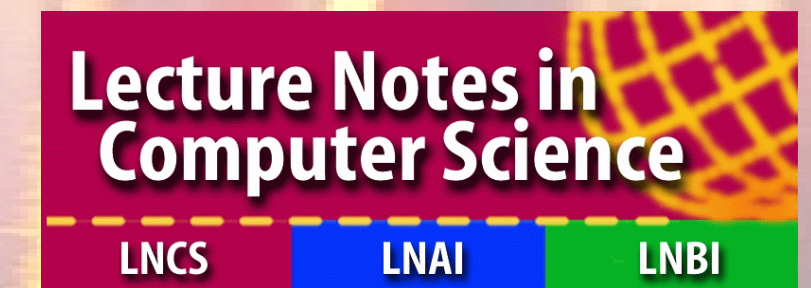


International Workshop on the Arithmetic of Finite Fields

WAIFI 2018

Bergen, Norway,
June 14-16, 2018

www.waifi.org



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 2018 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 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 (**EXTENDED**): **April 8, 2018**
- Acceptance notification: **May 11, 2018**
- Final pre-proceedings version due: **May 20, 2018**
- Final post-proceedings version due: **July 12, 2018**
- Workshop presentations: **June 14-16, 2018**
- Early registration deadline: **May 20, 2018**
- Late registration deadline: **June 7, 2018**

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. 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.

Notice that in order to be included in the proceedings, the authors of an accepted paper must guarantee to present their contribution at the workshop.

NEW: Students presenting their papers at the workshop will be released from registration fee.

NEW: There will be also a best paper award for the best paper presented at the workshop.

More detailed information on instructions for authors, paper submission, technical program, accommodation, travel and registration will be posted on the Workshop web site: <http://www.waifi.org>.

Participants of WAIFI 2018 may be interested to attend the International Workshop on Boolean Functions and Their Applications BFA 2018 which will take place right after WAIFI in Loen, a location close to Bergen:

<http://people.uib.no/chunlei.li/workshops/BFA2018/>