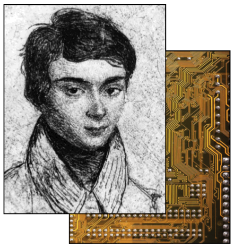
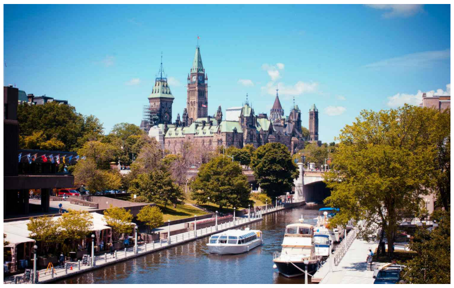


Workshop on the Arithmetic of Finite Fields
WAIFI 2024

`www.waifi.org`

Ottawa, Canada
June 10-12, 2024

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, especially in cryptography and coding theory.
The topics of WAIFI 2024 include but are not limited to:

Theory of finite field arithmetic:
- *Bases (canonical; normal; dual; etc.)*
- *Polynomials (irreducible; primitive; permutation)*
- *Boolean functions and special functions over finite fields*
- *Algebraic curves over finite fields*
- *Dynamical systems over finite fields*

Hardware & software implementations:
- *Design & implementation of finite field processors*
- *Design & implementation of arithmetic algorithms*
- *Pseudorandom number generators*
- *Hardware/software co-design*

Applications of finite fields in:
- *Cryptography (ciphers; PQC; etc)*
- *Coding theory (AG codes; LDPC codes; etc)*
- *Combinatorics (designs; arrays; etc)*
- *Finite geometry*

Authors are invited to submit **original research** papers that has not been previously published or submitted, before WAIFI's notification date, for publication elsewhere. 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: **March 8, 2024**
- Acceptance notification: May 3, 2024
- Post-proceedings version due: July 7, 2024

We expect that 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`

Invited speakers:
- Paulo Barreto, *University of Washington, USA*
- Koray Karabina, *National Research Council, Canada*
- Chloe Martindale, *University of Bristol, England*
- Maria Montanucci, *DTU, Denmark*

Program Committee:
- Claude Carlet, *U. Paris VIII, France and Bergen, Norway*
- Wouter Castryck, *KU Leuven, Belgium*
- Thomas Decru, *KU Leuven and U. Libre Bruxelles, Belgium*
- Sylvain Duquesne, *U. Rennes, France*
- Guang Gong, *U. Waterloo, Canada*
- Anna-Lena Horlemann, *U. St. Gallen, Switzerland*
- Sophie Huczynska, *U. St. Andrews, Scotland*
- Thais Bardini Idalino, *U. Federal Santa Catarina, Brazil*
- Jose Luis Imaña, *U. Complutense Madrid, Spain*
- Jorge Jimenez Urroz, *U. Politécnica Madrid, Spain*
- Angshuman Karmakar, *IIT Kanpur, India*
- Elena Kirshanova, *TII, UAE*
- Sihem Mesnager, *U. Paris VIII, France*
- Lucia Moura, *U. Ottawa, Canada*
- Alessandro Neri, *U. Gent, Belgium*
- Svetla Nikova, *KU Leuven, Belgium* (Program co-Chair)
- Daniel Panario, *Carleton U., Canada* (Program co-Chair)
- Hilder Vitor Lima Pereira, *Unicamp, Brazil*
- Håvard Raddum, *U. Bergen, Norway*
- Francisco Rodriguez Henriquez, *TII, UAE*
- Amin Sakzad, *Monash U., Australia*
- David Thomson, *Carleton U., Canada*
- Alev Topuzoğlu, *Sabanci U., Turkey*
- Geertrui Van de Voorde, *U. Canterbury, New Zealand*
- Qiang (Steven) Wang, *Carleton U., Canada*
- Nusa Zidaric, *U. Leiden, The Netherlands*

General co-Chairs:
- Daniel Panario, *Carleton University, Canada*
- David Thomson, *Carleton University, Canada*
- Qiang (Steven) Wang, *Carleton University, Canada*

Program co-Chairs:
- Svetla Nikova, *KU Leuven, Belgium*
- Daniel Panario, *Carleton University, Canada*