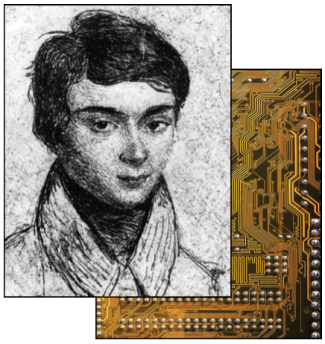

Workshop on the Arithmetic of Finite Fields
WAIFI 2026

www.waifi.org

Santander, Spain
June 3-5, 2026

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, specially in cryptography and coding theory.

The topics of WAIFI 2026 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:
- *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. The paper should be at most 16 pages using the Springer LNCS format. In order to be included in the proceedings, one of the authors of an accepted paper is expected to present their contribution at the workshop.

- Abstract submission deadline: **March 8th, 2026**
- Submission deadline: **March 15th (23:59h AoE), 2026**
- Acceptance notification: April 7th, 2026
- Final version due: April 16th, 2026

- Poster submission deadline: **April 30th, 2026**

The proceedings will be published in the Springer **Lecture Notes in Computer Science (LNCS)**

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:
- Herivelto Martins Borges Filho, *U. São Paulo, Brazil*
- Claude Carlet, *U. Paris VIII (France) and Bergen (Norway)*
- Maria Corte-Real Santos, *ENS Lyon, France*
- Thomas Decru, *KU Leuven, Belgium*
- Sylvain Duquesne, *U. Rennes, France*
- Ana Isabel Gómez Pérez, *U. Rey Juan Carlos, Spain*
- Sophie Huczynska, *U. St. Andrews, Scotland*
- José Luis Imaña, *U. Complutense Madrid, Spain*
- Jorge Jiménez Urroz, *U. Politécnica Madrid, Spain*
- Angshuman Karmakar, *IIT Kanpur, India*
- Gohar Kyureghyan, *U. Rostock, Germany*
- Edgar Martínez Moro, *U. Valladolid, Spain*
- Sihem Mesnager, *U. Paris VIII, France*
- Alessandro Neri, *U. Naples Federico II, Italy*
- Svetla Nikova, *KU Leuven, Belgium*
- Daniel Panario, *Carleton U., Canada*
- Hilder Vitor Lima Pereira, *Unicamp, Brazil*
- Håvard Raddum, *Simula UiB, Norway*
- Francisco Rodríguez Henríquez, *TII, UAE*
- Ana Salagean, *U. Loughborough, UK*
- Amin Sakzad, Monash, *U., Australia*
- David Thomson, *Carleton U., Canada*
- Alev Topuzoğlu, *Sabancı U., Türkiye*
- Monika Trimoska, *TU/e, The Netherlands*
- Qiang (Steven) Wang, *Carleton U., Canada*
- Violetta Weger, *Technical U. Munich, Germany*
- Nusa Zidaric, *U. Leiden, The Netherlands*

General Chair:
- Domingo Gómez Pérez, *University of Cantabria, Spain*

Organizing Committee:
- Ana Isabel Gómez Pérez, *Rey Juan Carlos University, Spain*
- Edgar Martínez Moro, *University of Valladolid, Spain*
- Daniel Sadornil Renedo, *University of Cantabria, Spain*

Program co-Chairs:
- Lejla Batina, *Radboud University, The Netherlands*
- Ferruh Özbudak, *Sabancı U., Türkiye*

Publicity Chair:
- José Luis Imaña, *Complutense University of Madrid, Spain*