

# WAIFI 2026 Program

**Wednesday, 3 June -- Place: Sala de Grados. Facultad de Derecho**

**9:00 - 9:30 Registration at Facultad de Derecho. Opening**

**Invited Talk 1** (Chair: Domingo Gómez Pérez)

**9:30 - 10:30 Delaram Kahrobaei.**  
**Recent Trends and Future Directions in Post-Quantum Group-based Cryptography in the AI Era.**

**Session 1** (Chair: Domingo Gómez Pérez)

**10:30 - 10:55** Claude Carlet.  
A notion on S-boxes for a partial resistance to some integral attacks.  
**10:55 - 11:20** Noemí DeCastro-García, Lucía Mallo-Fernández and Miguel V. Carriegos.  
Output feedback transformations for preserving observability and structural decodability in convolutional codes.  
**11:20 - 11:50 Break (Cafetería Derecho - 2nd Floor)**

**Session 2** (Chair: Domingo Gómez Pérez)

**11:50 - 12:15** Virginio Fratianni and Sihem Mesnager.  
Self-Orthogonal Codes from  $p$ -ary Quadratic Forms via Character Sums with Applications to LCD and Arbitrary Hull Dimensional Codes.  
**12:15 - 12:40** Satoru Fukasawa.  
Algebraic geometry codes with many automorphisms arising from Galois points.  
**12:40 - 13:05** Beatriz García García, Consuelo Martínez López and Ignacio F. Rúa.  
The Non-Asymptotic Landscape of Abelian Codes: A Framework for (F,G)-Goodness.  
**13:05 - 14:30 Lunch (Cafetería Derecho - 2nd Floor)**

**Invited Talk 2** (Chair: Lejla Batina)

**14:30 - 15:30 Violetta Weger.**  
**How hard is code equivalence?.**

**Session 3** (Chair: Lejla Batina)

**15:30 - 16:00 Break (Cafetería Derecho - 2nd Floor)**  
**16:00 - 16:25** Marc Joye.  
Boolean Arithmetic over  $F_2$  from Group Commutators.  
**16:25 - 16:50** Christian Kaspers and Alexander Pott.  
A new construction of locally-APN functions on  $F_2^{2m}$  using spreads and Sidon sets.  
**16:50 - 17:15** Michiya Iwata, Ryomei Sugai, Kosuke Sakata and Tsuyoshi Takagi.  
Explicit Bounds on the Existence Probability of Random Multivariate Quadratic Systems over Finite Fields.

**19:00 - 20:00 Welcome Cocktail at Palacio de la Magdalena (First Floor)**

**Thursday, 4 June -- Place: Salón de Actos. Escuela Técnica Superior de Náutica**

**Invited Talk 3** (Chair: Ferruh Özbudak)

**9:30 - 10:30** John Sheekey.  
**Arithmetic of Finite Semifields.**

**Session 4** (Chair: Ferruh Özbudak)

**10:30 - 10:55** Vincent Macri, Michael Jacobson and Renate Scheidler.  
**Improvements to Jacobian Arithmetic in Global Function Fields.**

**10:55 - 11:20** Nicolas Méloni, François Palma and Pascal Véron.  
**Equality Tests in the Polynomial Modular Number System.**

**11:20 - 11:50** **Break (E.T.S. Náutica - Main Hall)**

**Session 5** (Chair: Ferruh Özbudak)

**11:50 - 12:15** Ryo Negishi, Kazuki Komine, Akira Katayama and Masaya Yasuda.

**On the (Non-)Existence of Efficient Class Group Orbits for Collision Search in CSIDH.**

**12:15 - 12:40** Francisco Javier Soto Sánchez.

**Codegrees and an Exact Triangle Formula for the Norm-One Cayley Graph over  $F_q^3$  in Characteristic 2.**

**12:40 - 13:05** Hugo Rodrigues Teixeira, Claude Gravel and Daniel Panario.

**Constructing a parameterized polynomial map through functional graphs and applications.**

**13:05** **Conference Group Photo**

**13:05 - 14:30** **Lunch (Cafetería E.T.S. Náutica - Ground Floor)**

**Session 6** (Chair: Vishnupriya Anupindi)

**14:30 - 14:55** Kohtaro Yamaguchi and Shushi Harashita.

**Automorphism groups of hyperelliptic curves of 2-rank zero.**

**14:55 - 15:20** Seon Jeong Kim and Masaaki Homma.

**Classification of Hermitian-relative curves up to projective equivalence.**

**15:20 - 16:15** **Break + Poster Session (E.T.S. Náutica - Main Hall)**

**Short Talks Session**

**16:15 - 16:35** Gary McGuire.

**A Conjecture on Primitive Polynomials.**

**16:35 - 16:45** James A. Davis.

**Generalized Denniston Partial Difference Sets.**

**16:45 - 16:55** Ryutaroh Matsumoto.

**Impure codes exceeding the pure bounds for quantum local recovery.**

**16:55 - 17:05** Nikolay Kaleyski and Joakim Hauger Sunde.

**Testing and reconstructing CCZ- and EA-equivalence of vectorial Boolean functions.**

**17:05 - 17:15** Anamari Nakić.

**Additive Steiner 2-designs.**

**17:15 - 17:20** **Short break**

**17:20 - 17:30** I.F. Rúa, E.F. Combarro, and J. Ranilla.

**Knuth orbits of semifields of order 128 with a nontrivial automorphism.**

**17:30 - 17:40** Francisco Javier Soto.

**On BLR linearity testing for trace monomials over binary fields.**

**17:40 - 17:50** David González González.

**Differential Goppa codes.**

**17:50 - 17:55** **Short break**

**17:55 - 18:05** Fernando Neranga.

**Reversed Dickson Polynomials Over Finite Fields.**

**18:05 - 18:15** Fernando Neranga.

**Quandle Rings and Their Applications in Coding Theory.**

**18:15 - 18:25** Verónica Requena Arévalo.

**Construction of Generalized Weighing Hadamard Matrices over  $(F_p)$ .**

**20:00 - 21:30** **Conference Dinner at La Caseta de Bombas**

**Friday, 5 June -- Place: Sala de Grados. Facultad de Derecho**

**Session 7** (Chair: José Luis Imaña)

**10:00 - 10:25** Miguel Alcocer-Pérez, Nathalie Bochard, Viktor Fischer, Ana Isabel Gómez and Domingo Gómez-Pérez.

Period Counting versus Direct Sampling in Oscillator-based TRNGs: Architectures and Characteristics.

**10:25 - 10:50** Daichi Aoki and Tsuyoshi Takagi.

Designing PMNS for 8-bit Architectures.

**10:50 - 11:15** Doaa Ashmawy and Arash Reyhani-Masoleh.

From Compact to Fast: Exploring 32- and 64-Bit AES Datapaths for IoT Systems.

**11:20 - 11:50 Break (Cafetería Derecho - 2nd Floor)**

**Session 8** (Chair: Daniel Panario)

**11:50 - 12:15** Erkay Savaş, Ali Sah Ozcan and Cihangir Tezcan.

Fast and Energy-Efficient Polynomial Multiplication using FFT, FFNT, and NTT on GPUs for Fully Homomorphic Encryption

**12:15 - 12:40** Olav Geil.

On secret sharing from extended norm-trace curves.

**12:40 - 13:05** Martin Grenouilloux, Chunlei Li and Pierrick Méaux.

On the Resilience Order of Weightwise Almost Perfectly Balanced Functions.

**13:05 - 13:15 Closing Remarks**

**14:30 - Informal Social Activity in Santander**