WCC 2024 Program

Monday June 17

8:50 - 9:00 **- Welcome speech**

9:00 - 10:00 **- Invited talk** (chair: Pierre Loidreau)

- From Code-Based Cryptography to Packing Bounds
  Thomas Debris

10:00 - 10:30 **- Coffee Break**

10:30 - 12:10 **- Codes (I)** (chair: Fernanda Pambianco)

- Linear programming lower bounds for energy of weighted spherical codes
  Sergiy Borodachov, Peter Boyvalenkov, Peter Dragnev, Douglas Hardin, Edward Saff and Maya Stoyanova
- PIR Codes, Unequal-Data-Demand Codes, and the Griesmer Bound
  Henk D.L. Hollmann, Martin Puskin and Ago-Erik Riet
- Additive twisted codes: new distance bounds and infinite families of quantum codes
  Reza Dastbasteh and Petr Lisonek
- Characterization of Some Non-Canonical Minihypers in $PG(r, 3)$ and the Main Problem of Coding Theory
  Assia Rousseva, Ivan Landjev and Emiliyan Rogachev

12:10 - 14:00 **- Lunch**

14:00 - 15:40 **- Public key cryptography** (chair: Daniel Panario)

- Public-key encryption from LIP
  Léo Ackermann, Adeline Roux-Langlois and Alexandre Wallet
- A Niederreiter public-key cryptosystem using a convolutional approach
  Paulo Almeida, Miguel Beltrá Vidal and Diego Napp
- Extensible Decentralized Secret Sharing and Schnorr Signatures
  Michele Battagliola, Riccardo Longo and Alessio Meneghetti
- Group Factorisation for Smaller Signatures from Cryptographic Group Actions
  Giuseppe D'Alconzo, Alessio Meneghetti and Edoardo Signorini

15:40 - 16:10 **- Coffee break**

16:10 - 17:25 **- Symmetric cryptography** (chair: Léo Perrin)

- Equivalence of Generalised Feistel Networks
  Patrick Derbez and Marie Euler
- New Models for the Cryptanalysis of ASCON
  Mathieu Degré, Patrick Derbez, Lucie Lahaye and André Schrottenloher
- Optimal S-boxes against alternative operations
  Marco Calderini, Roberto Civino and Riccardo Invernizzi

Tuesday June 18

9:00 - 10:00 **- Invited talk** (chair: Alain Couvreur)

- Tensor Codes
  Eimear Byrne

10:00 - 10:30 **- Coffee Break**

10:30 - 12:10 **- Rank-metric codes** (chair: Jean-Pierre Tillich)

- On the maximum weight codewords of linear rank-metric codes
  Olga Polverino, Paolo Santonastaso and Ferdinando Zullo
- Stabilizers of graphs of linear functions and rank-metric codes
  Valentino Smaldore, Corrado Zanella and Ferdinando Zullo
- The geometry of covering codes in the sum-rank metric
  Matteo Bonini, Martino Borello and Eimear Byrne
- Bounds on Sphere Sizes in the Sum-rank Metric and Coordinate-additive Metrics
  Hugo Sauerbier Couvée, Thomas Jerkovits and Jessica Bariffi

12:10 - 14:00 **- Lunch**

14:00 - 15:40 **- Boolean functions** (chair: Alev Topuzoğlu)

- On the Properties of the Ortho-Derivatives of Quadratic Functions
  Anne Canteaut, Alain Couvreur and Léo Perrin
- On Functions of $\mathbb{F}_{2^{2t}}$ mapping Cosets of $\mathbb{F}_{2^t}^*$ to Cosets of $\mathbb{F}_{2^t}^*$
  Jules Baudrin, Anne Canteaut and Léo Perrin
- On the algebraic degree stability of Boolean functions when restricted to affine spaces
  Claude Carlet, Serge Christian Feukoua Jonzo and Ana Salagean
- On rotation-symmetric Boolean bent functions outside the $\mathcal{M}^\#$ class
  Alexandr Polujan, Sadmir Kudin and Enes Pasalic

15:40 - 16:10 **- Coffee break**

16:10 - 17:25 **- Boolean functions and decoding** (chair: Patrick Felke)

- Further Investigation on Differential Properties of the Generalized Ness-Helleseth Mapping
  Yongbo Xia, Furong Bao, Shaoping Chen, Chunlei Li and Tor Helleseth
- Iterative decoding of skew constacyclic codes
  Kayodé Epiphane Nouetowa and Ivan Pogildiakov
- How to Lose Some Weight - A Practical Template Syndrome Decoding Attack
  Sebastian Bitzer, Jeroen Delvaux, Elena Kirshanova, Sebastian Maaßen, Alexander May and Antonia Wachter-Zeh

Wednesday June 19

9:00 - 10:00 **- Invited talk** (chair: Daniele Bartoli)

- Two Applications of Number Theory to Information Theory
  Giacomo Micheli

10:00 - 10:30 **- Coffee Break**

10:30 - 11:45 **- Codes (II)** (chair: Daniel Augot)

- Distance Distribution of Cyclic Orbit Flag Codes
  Clementa Alonso-González and Miguel Ángel Navarro-Pérez
- Weight Distribution of the Binary Reed-Muller Code $R(4, 9)$
  Miroslav Markov and Yuri Borissov
- Understanding the new distinguisher of alternant codes at degree 2
  Axel Lemoine, Rocco Mora and Jean-Pierre Tillich

12:10 - 14:00 **- Lunch**

14:00 - 17:00 **- Guided visit of Perugia**

Thursday June 20

9:00 - 10:00 **- Invited talk** (chair: María Naya-Plasencia)

- Commutative Cryptanalysis as a Generalization of Differential Cryptanalysis
  Christof Beierle

10:00 - 10:30 **- Coffee Break**

10:30 - 12:10 **- Codes (III)** (chair: Annamaria Iezzi)

- Spread Code Constructions from Abelian non-cyclic groups
  Joan-Josep Climent, Verónica Requena and Xaro Soler-Escrivà
- On equidistant single-orbit cyclic subspace codes
  Mahak Mahak and Maheshanand Bhaintwal
- A class of locally recoverable codes over finite chain ring
  Giulia Cavicchioni, Eleonora Guerrini and Alessio Meneghetti
- Introducing locality in some generalized AG code
  Bastien Pacifico

12:10 - 14:00 **- Lunch**

14:00 - 15:40 **- Maximum rank-metric (MRD) codes** (chair: Massimo Giulietti)

- On 3-dimensional MRD codes of type $\langle x^{q^t}, x + \delta x^{q^{2t}}, G(x)\rangle$
  Francesco Ghiandoni.
- A geometric construction of a class of non-linear MRD codes
  Nicola Durante, Giovanni Giuseppe Grimaldi and Giovanni Longobardi
- New scattered sequences of order $m \geq 3$
  Alessandro Giannoni and Giuseppe Marino
- Exceptional scattered polynomials in odd degree
  Massimo Giulietti and Giovanni Zini

15:40 - 16:10 **- Coffee break**

16:10 - 17:25 **- Finite geometries and finite fields** (chair: Giuseppe Marino)

- Further Results on Orbits and Incidence matrices for the Class O_6 of Lines External to the Twisted Cubic in $PG(3; q)$
  Alexander A. Davydov, Stefano Marcugini and Fernanda Pambianco
- Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order dp with $d \neq p$ prime
  Arianna Dionigi and Barbara Gatti
- On the Recursive Behaviour of the Number of Irreducible Polynomials with Certain Properties over Finite Fields
  Max Schultz

Friday June 21

9:00 - 10:00 **- Invited talk** (chair: Christina Boura)

- Security of Encryption Modes and an Exposition of Proof Techniques
  Bart Mennink

10:00 - 10:30 **- Coffee Break**

10:30 - 12:10 **- DE CIFRIS Session - Concluding remarks**

12:10 - 14:00 **- Lunch**