WCC 2019

Monday April 1

8:55 Welcome

9:00 - 10:15 - **Cryptographic functions I** (chair : Anne Canteaut)

- Counting Boolean functions with Faster Points.
  Ana Salagean and Ferruh Ozbudak
- On some cryptographic properties of Boolean functions.
  Augustine Musukwa, Massimiliano Sala and Marco Zaninelli
- Homogeneous cubic bent functions without affine derivatives outside M class.
  Alexandr Polujan and Alexander Pott

10:15 - 10:45 - **Coffee break**

10:45 - 11:35 - **Codes with locality I** (chair : Daniel Augot)

- Codes with locality from a cyclic extension of the Suzuki curve.
  Gretchen Matthews
- Constructions of optimal locally recoverable codes via Dickson polynomials.
  Jian Liu, Sihem Mesnager and Deng Tang

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

15:05 - 15:55 - **Combinatorics and discrete geometry I** (chair : Ivan Landjev)

- Subspace Packing.
  Tuvi Etzion, Sascha Kurz, Kamil Otal and Ferruh Özbudak
- Graphs and Self-dual additive codes over GF(4).
  Mithilesh Kumar, Srimathi Varadharajan and Håvard Raddum

15:55 - 16:25 - **Coffee break**

16:25 - 17:15 - **Algebraic and geometric codes.** (chair : Martino Borello)

- On codes in group algebras.
  Wolfgang Willems
- Intersections between the norm-trace curve and some low degree curves.
  Matteo Bonini and Massimiliano Sala

18:00 - 19:00 - **Bienvenue cocktail**

19:30 - **Dinner**

Tuesday April 2

9:00 - 10:15 - **Code-based cryptography I** (chair : Nicolas Sendrier)

- Cryptanalysis of a code-based one-time signature.
  Jean-Christophe Deneuville and Philippe Gaborit
- A Code-Based Signature Scheme in the Standard Model.
  Olivier Blazy, Philippe Gaborit, Dang Truong Mac, Ayoub Otmani and Jean-Pierre Tillich
- Improved Decoders for p-ary MDPC.
  Isaac Canales-Martinez, Qian Guo and Thomas Johansson

10:15 - 10:45 - **Coffee break**

10:45 - 12:00 - **Cryptographic functions II** (chair : Gohar Kyureghyan)

- On equivalence between some families of APN functions.
  Lilya Budaghyan, Marco Calderini and Irene Villa
- Permutations on $\mathbb{F}_{q^n}$ with Invariant Cycle Structure on Certain Lines.
  Daniel Gerike and Gohar Kyureghyan
- Generalized Isotopic Shift of Gold Functions.
  Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert Coulter and Irene Villa

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

14:00 - 15:00 - **Invited talk** (chair : Daniel Augot)

Sub-packetization of Minimum Storage Regenerating codes: A lower bound and a work-around.

Venkatesan Guruswami

15:05 - 15:55 - **Symmetric cryptography I** (chair : Anne Canteaut)

- On the groups of alternative operations for differential cryptanalysis.
  Riccardo Aragona, Roberto Civino, Norberto Gavioli and Carlo Maria Scoppola
- Proving the Forward Bias of Salsa.
  Sabyasachi Dey and Santanu Sarkar

15:55 - 16:25 - **Coffee break**

16:25 - 17:15 - **Rank distance codes** (chair : Pierre Loidreau)

- On the Sparsity of MRD Codes.
  Eimear Byrne and Alberto Ravagnani
- $\mathbb{F}_{q^n}$-linear rank distance codes and their distinguishers.
  Luca Giuzzi and Ferdinando Zullo

17:30 - 18:30 - **Invited talk -** (chair : Felix Ulmer)

Cryptanalysis techniques in cryptography based on algebraic codes.

Alain Couvreur.

19:30 - **Dinner**

Wednesday April 3

9:00 - 10:15 - **Decoding** (chair : Eimear Byrne)

- On decoding additive generalised twisted Gabidulin codes.
  Chunlei Li and Wrya Kadir
- An algorithm for decoding skew Reed-Solomon codes with respect to the skew metric.
  Delphine Boucher
- A Turyn-based neural Leech decoder.
  Vincent Corlay, Joseph Boutros, Philippe Ciblat and Loïc Brunel

10:15 - 10:45 - **Coffee break**

10:45 - 11:35 - **Code-based cryptography II** (chair : Nicolas Sendrier)

- On the security of a Loidreau's rank metric code based encryption scheme.
  Daniel Coggia and Alain Couvreur
- A key recovery attack against LRPC using decryption failures.
  Nicolas Aragon and Philippe Gaborit

11:45 - 12:45 - **Lunch**

12:45 - **Walking with "Sensations Littoral"** or **sand yachting with "Club nautique"**

19:30 - **Conference Dinner**

Thursday April 4

9:00 - 10:15 - **Cryptographic functions III** (chair : Alexander Pott)

- Gowers U_2 norm of Boolean functions and their generalizations.
  Sugata Gangopadhyay, Constanza Riera and Pantelimon Stănică
- Boomerang Uniformity of Popular S-box Constructions.
  Christina Boura, Léo Perrin and Shizhu Tian
- Limitation of the BLR testing in estimating nonlinearity.
  Debajyoti Bera, Subhamoy Maitra, Dibyendu Roy and Pantelimon Stănică

10:15 - 10:45 - **Coffee break**

10:45 - 12:00 - **Combinatorics and discrete geometry II** (chair : Ferruh Ozbudak)

- Upper bounds for energies of codes of given cardinality and separation.
  Peter Boyvalenkov, Peter Dragnev, Douglas Hardin, Edward Saff and Maya Stoyanova
- Homogeneous arcs and linear codes over finite chain rings.
  Thomas Honold and Ivan Landjev
- A near-optimal algorithm for adaptive searching of two counterfeit coins.
  Zilin Jiang, Nikita Polyanskii and Ilya Vorobyev

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

14:00 - 15:00 - **Invited talk** (chair : Ferruh Ozbudak)

Irreducible compositions of polynomials.

Gohar Kyureghyan.

15:05 - 15:55 - **Symmetric cryptography II** (chair: Sihem Mesnager)

- Invariant Hoppping Attacks on Block Ciphers.
  Nicolas Courtois
- Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases.
  Igor Semaev and Andrea Tenti

15:55 - 16:25 - **Coffee break**

16:25 - 16:55 - **Codes with locality II** (chair : Sihem Mesnager)

- Constructions of Optimal Locally Repairable Codes with Information (r, t)-Locality.
  Pan Tan, Zhengchun Zhou, Vladimir Sidorenko and Udaya Parampalli

17:00 - 17:30 - **WCC announcements**

19:30 - **Dinner**

Friday April 5

9:00 - 10:15 - **Codes and their applications** (chair : Jean-Pierre Tillich)

- Classical access structures of ramp secret sharing based on quantum stabilizer codes.
  Ryutaroh Matsumoto
- A new class of traceability schemes.
  Elena Egorova, Grigory Kabatyanskiy and Marcel Fernandez
- The geometric approach to the extendability problem for linear codes.
  Ivan Landjev and Assia Rousseva

10:15 - 10:45 - **Coffee break**

10:45 - 11:35 - **Quantum algorithmic** (chair : Jean-Pierre Tillich)

- Entanglement-assisted Quantum Codes from Algebraic Geometry Codes.
  Francisco Revson Fernandes Pereira, Ruud Pellikaan, Giuliano La Guardia and Francisco Marcos de Assis
- Improvements to low-qubit quantum resource estimates for quantum search.
  Benjamin Pring and James H. Davenport

11:45 - 12:45 - **Lunch**