WCC 2011

Monday April 11

9:00 Welcome

9:05 - 10:45 – RSA and elliptic curve cryptography

- **Reconstruction and Error Correction of RSA Secret Parameters from the MSB Side**
  Santanu Sarkar, Sourav Sen Gupta, Subhamoy Maitra
- **The Equivalence of Strong RSA and Factoring in the Generic Ring Model of Computation**
  Divesh Aggarwal, Ueli Maurer, Igor Shparlinski
- **Cryptanalysis of Dual CRT-RSA**
  Santanu Sarkar, Subhamoy Maitra
- **On the Number of Distinct Legendre, Jacobi, Hessian and Edwards Curves**
  Reza Rezaeian Farashahi

10:45 - 11:15 – Coffee break

11:15 - 12:05 – Invited talk

Knapsacks in cryptography: A survey of old and recent results
Antoine Joux

12:05 - 14:00 – Lunch

14:00 - 15:15 – Combinatorics and discrete geometry

- **Optimality of a 2-identifying code in the hexagonal grid**
  Ville Junnila, Tero Laihonen
- **The Dual Code of Points and t-Spaces in the Projective Space**
  Maarten De Boeck
- **Optimal arcs in three-dimensional Hjelmslev spaces**
  Stoyan Boev, Thomas Honold, Ivan Landjev

15:15 - 15:45 – Coffee break

15:45 - 17:50 – Codes over rings

- **Construction of new completely regular $\mathbb{Z}_2\mathbb{Z}_4$-linear codes from old**
  Josep Rifà, Lorena Ronquillo
- **On the Parameters of Codes With Two Homogeneous Weights**
  Eimear Byrne, Alison Sneyd
- **Characteristics of invariant weights related to code equivalence over rings**
  Cathy Mc Fadden, Marcus Greferath, Jens Zumbrägel
- **Algebraic Decoding of Negacyclic Codes over $\mathbb{Z}_4$**
  Eimear Byrne, Marcus Greferath, Jaume Pernas, and Jens Zumbrägel
- **New ring-linear codes from geometric dualization**
  Michael Kiermaier, Johannes Zwanzger

Tuesday April 12

9:00 - 10:40 – Cryptographic functions I

- **CCZ and EA Equivalence between Mappings over Finite Abelian Groups**
  Alexander Pott, Yue Zhou
- **On CCZ-equivalence of Addition mod 2^n**
  Ernst Schulte-Geers
- **A construction of bent functions from plateaued functions**
  Ayca Cesmelioglu, Wilfried Meidl
- **A new construction of bent functions based on $\mathbb{Z}$-bent functions**
  Sugata Gangopadhyay, Anand Joshi, Gregor Leander, Rajendra Kumar Sharma

10:40 - 11:10 – Coffee break

11:10 - 12:00 – Invited talk

Stream ciphers, filter generators, univariate polynomials and coding theory
Tor Helleseth

12:00 - 14:00 – Lunch

14:00 - 15:40 – Code-based cryptography

- **Improving the efficiency of Generalized Birthday Attacks against certain structured cryptosystems**
  Robert Niebuhr, Pierre-Louis Cayrel, Johannes Buchmann
- **A variant of the McEliece cryptosystem with increased public key security**
  Marco Baldi, Marco Bianchi, Franco Chiaraluce, Joachim Rosenthal, Davide Schipani
- **The non-gap sequence of a subcode of a generalized Reed-Solomon code**
  Irene Márquez-Corbella, Edgar Martínez-Moro and Ruud Pellikaan
- **Permutation decoding: Towards an approach using algebraic properties of the σ-subcode**
  Matthieu Legeay

15:40 - 16:10 – Coffee break

16:10 - 18:15 – Permutation groups

- **A Relation Between Quasi-Cyclic Codes and 2-D Cyclic Codes**
  Cem Guneri, Ferruh Özbudak
- **Factorisation in $M_\ell(\mathbb{F}_q)[X]$. Construction of quasi-cyclic codes**
  Christophe Chabot
- **A Complete Characterization of Irreducible Cyclic Orbit Codes**
  Anna-Lena Trautmann, Joachim Rosenthal
- **The automorphism groups of binary extremal self-dual codes of length $24m$**
  Javier de la Cruz, Wolfgang Willems
- **Class of Binary Generalized Goppa Codes Perfect in Weighted Hamming Metric**
  Sergey Bezzateev, Natalia Shekhunova

Wednesday April 13

9:00 - 10:40 – Geometric codes

- **Evaluation Codes from smooth Quadric Surfaces and Twisted Segre Varieties**
  Alain Couvreur, Iwan Duursma
- **Bounding the number of points on a curve using a generalization of Weierstrass semigroups**
  Peter Beelen, Diego Ruano
- **List decoding of a class of affine variety codes**
  Olav Geil, Casper Thomsen
- **On the weights of affine-variety codes and some Hermitian codes**
  Marco Pellegrini, Chiara Marcolla, Massimiliano Sala

10:40 - 11:10 – Coffee break

11:10 - 12:25 – Symmetric cryptography

- **Non-Binary Feedback with Carry Registers and Algebraic Feedback Registers**
  Mark Goresky, Andrew Klapper
- **Exploiting Linear Hull in Matsui's Algorithm 1**
  Andrea Röck, Kaisa Nyberg
- **Generalized Feistel Networks Revisited**
  Andrey Bogdanov, Kyoji Shibutani

12:25 - 14:30 – Lunch

Thursday April 14

9:00 - 10:40 – Other types of errors

- **On Optimal DNA Codes for Additive and Non-Additive Stem Similarity**
  Arkadii D'yachkov, Anna Voronina, Julia Volkova, Nikita Polyanskii
- **Three-Dimensional Fire Codes**
  Igor Boyarinov
- **Some codes correcting single symmetric errors of limited magnitude**
  Torleiv Kløve, Jinquan Luo, Somaye Yari
- **Generalized Bose-Lin Codes, a Class of Codes Detecting Asymmetric Errors of a Limited Magnitude**
  Irina Naydenova

10:40 - 11:10 – Coffee break

11:10 - 12:00 – Invited talk

Polar coding and some cryptographic applications
Erdal Arikan

12:00 - 14:00 – Lunch

14:00 - 15:40 – Cryptographic functions II

- **Planar products of linearized polynomials**
  Gohar M. Kyureghyan, Ferruh Özbudak
- **The selfnegadual properties of generalised quadratic Boolean functions**
  Lars Eirik Danielsen, Matthew G. Parker
- **Quadratic functions with prescribed spectra**
  Wilfried Meidl, Alev Topuzoglu
- **Counting quadratic forms of codimension 2 in characteristic 2 and relations to maximal curves**
  Ferruh Ozbudak, Zulfukar Saygi

15:40 - 16:10 – Coffee break

16:10 - 17:50 – Discrete algebra and finite fields

- **On divisibility of polynomials of special type over fields of characteristic 2**
  Leonid A. Bassalygo, Victor A. Zinoviev
- **A Lower Bound for the Nonlinearity of Exponential Welch Costas Functions**
  Risto M. Hakala
- **Some Results on Kloosterman Sums and their Minimal Polynomials**
  Faruk Gologlu, Gary McGuire, Richard Moloney
- **An Action of PGL(2,q) on Irreducible Polynomials over $\mathbb{F}_q$**
  Henning Stichtenoth, Alev Topuzoğlu

Friday April 15

9:00 - 10:40 – Decoding algorithms and LDPC

- **LDPC codes arising from partial and semipartial geometries**
  Peter Vandendriessche
- **Scheduled-PEG construction of LDPC codes for Upper-Layer FEC**
  Lam Pham Sy, Valentin Savin, David Declercq, Nghia Pham
- **Fast Decoding of Gabidulin Codes**
  Antonia Wachter, Valentin Afanassiev, Vladimir Sidorenko
- **Multicomponent Network Coding**
  Ernst M. Gabidulin, Nina I. Pilipchuk

10:40 - 11:10 – Coffee break

11:10 - 12:00 – Spherical codes

- **Constructive spherical codes near the Shannon bound**
  Patrick Solé, Jean-Claude Belfiore
- **On the number of lattice points in a small sphere**
  Annika Meyer

12:00 - 12:55 – Cryptography

- **Statistical Asynchronous Weak Commitment Scheme: A New Primitive to Design Statistical Asynchronous Verifiable Secret Sharing Scheme**
  Ashish Choudhury, Arpita Patra
- **An Analysis of the Naor-Naor-Lotspeich Subset Difference Algorithm**
  Sanjay Bhattacherjee, Palash Sarkar

12:50 - 14:50 – Lunch