Program WCC 2013

Monday, April 15

Invited Talk 1
Chairman: Tor Helleseth
9:00 – 9:50 Kai-Uwe Schmidt, *Low autocorrelation sequences*

Sequences
9:50 – 10:15 Elena Dubrova, *A method for generating full cycles by a composition of NLFSRs*
10:15 – 10:40 Gottlieb Pirsic and Arne Winterhof, *On discrete Fourier transform, ambiguity, and Hamming-autocorrelation of pseudorandom sequences*

10:40 – 11:10 *Coffee Break*

APN Functions
Chairman: Claude Carlet
11:10 – 11:35 Florian Caullery, *APN functions of degree 4e with e≡3 (mod 4)*
11:35 – 12.00 Yuyin Yu, Mingsheng Wang and Yongqiang Li, *A matrix approach for constructing quadratic APN functions*
12:00 – 12:25 Guobiao Weng, Yin Tan and Guang Gong, *On quadratic almost perfect nonlinear functions and their related algebraic object*

12:30 – 14:00 *Lunch*

Coding Theory
Chairman: Daniel Augot
14:00 – 14:25 Torleiv Kløve and Moshe Schwartz, *Covering sets for limited-magnitude errors*
14:25 – 14:50 Nicolas Sendrier and Dimitris E. Simos, *How easy is code equivalence over F_q?*
14:50 – 15:15 Sarah E. Anderson and Gretchen L. Matthews, *Exponents of polar codes using algebraic geometric code kernels*
15.15 – 15:40 Hyun Kwang Kim and Phan Thanh Toan, *New inequalities for q-ary constant-weight codes*

15:40 – 16.10 *Coffee Break*

Feistel Ciphers
Chairman: Anne Canteaut
16:10 – 16:35 Kyoji Shibutani and Andrey Bogdanov, *Towards the optimality of Feistel ciphers with substitution-permutation functions*
16:35 – 17:00 Shingo Yanagihara and Tetsu Iwata, *Type 1.x generalized Feistel structures*
17:00 – 17:25 Mahabir Prasad Jhanwar, Ayineedi Venkateswarlu and Reihaneh Safavi-Naini, *Paillier-based publicly verifiable (non-interactive) secret sharing*

Quantum Algoritms
Chairman: Matthew Parker
17:25 – 17:50 Kaushik Chakraborty and Subhamoy Maitra, *Quantum algorithm to check resiliency of a Boolean function (Extended Abstract)*
17:50 – 18:15 Petr Lisoněk and Vijaykumar Singh, *Construction X for quantum error-correcting codes*

Tuesday, April 16

Invited Talk 2
Chairman: Vincent Rijmen
9:00 – 9:50 Gregor Leander, *Design and analysis of block ciphers - Links to Boolean functions and coding theory*

Coding and Cryptography
9:50 – 10:15 Philippe Gaborit, Gaétan Murat, Olivier Ruatta and Gilles Zémor, *Low rank parity check codes and their application to cryptography*
10:15 – 10:40 Alain Couvreur, Philippe Gaborit, Valérie Gauthier, Ayoub Otmani and Jean-Pierre Tillich, *Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes*

10:40 – 11:10 *Coffee break*

Cryptanalysis
Chairman: Andrey Bogdanov
11:10 – 11:35 Maria Eichlseder, Florian Mendel, Tomislav Nad, Vincent Rijmen and Martin Schläffer, *Linear propagation in efficient guess-and-determine attacks*
11:35 – 12:00 Thomas Johansson and Carl Löndahl, *A new algorithm for finding low-weight polynomial multiples and its applications to TCHo*
12:00 – 12:25 Santanu Sarkar, *Small secret exponent attack on RSA variant with modulus $N=p^2q$*

12:30 – 14:00 *Lunch*

Finite Fields
Chairman: Alexander Pott
14:00 – 14:25 Céline Blondeau and Léo Perrin, *More differentially 6-uniform power functions*
14:25 – 14:50 Kai-Uwe Schmidt and Yue Zhou, *Planar functions over fields of characteristic two (Extended Abstract)*
14:50 – 15:15 Gohar Kyureghyan and Qi Wang, *An upper bound on the size of Kakeya sets in finite vector spaces*
15:15 – 15:40 Grasiele C. Jorge, Antonio Campello and Sueli R. Costa, *q-ary lattices in the lp norm and a generalization of the Lee metric*

15.40 – 16:10 *Coffee Break*

Algebraic Coding Theory
Chairman: Nicolas Sendrier
16:10 – 16:35 Stéphane Ballet and Robert Rolland, *On low weight codewords of generalized affine and projective Reed-Muller codes (Extended Abstract)*
16:35 – 17:00 Morgan Barbier, Clément Pernet and Guillaume Quintin, *On the decoding of quasi-BCH codes*
17:00 – 17:25 Irene Platoni, *Quasi-perfect linear codes from plane cubics*

Optical Orthogonal Codes
Chairman: Alexander Kholosha
17:25 – 17:50 Jin-Ho Chung and Kyeongcheol Yang, *A new class of optimal variable-weight optical orthogonal codes*
17:50 – 18:15 Kenneth Shum, *Optimal three-dimensional optical orthogonal codes and related combinatorial designs*

Wednesday, April 17

Cryptography

Chairman: Thomas Johansson

9:00 – 9:25 Santanu Sarkar, *Further non-randomness in RC4, RC4A and VMPC*

9:25 – 9:50 Vincent Rijmen, Deniz Toz and Kerem Varıcı, *On the four round AES characteristics*

9:50 – 10:15 Hadi Soleimany and Kaisa Nyberg, *Zero-correlation linear cryptanalysis of reduced-round Lblock*

10:15 – 10:40 Felix Fontein, Michael Schneider and Urs Wagner, *A polynomial time version of LLL with deep insertions*

10:40 – 11:10 *Coffee Break*

Boolean Functions

Chairman: Sihem Mesnager

11:10 – 11:35 Ayça Çesmelioğlu, Wilfried Meidl and Alexander Pott, *On the normality of p-ary bent functions*

11:35 – 12:00 Claude Carlet and Andrew Klapper, *On the arithmetic Walsh coefficients of Boolean functions*

12.00 – 12:25 Subhabrata Samajder and Palash Sarkar, *Fast multiplication of the algebraic normal forms of two Boolean functions*

12:30 – 14:00 *Lunch*

15:00 – 18:00 *Excursion*

Thursday, April 18

Finite Fields and Rings
Chairman: Pascale Charpin
9:00 – 9:25 Thomas Feulner, *On canonical forms of ring-linear codes*
9:25 – 9:50 Faruk Göloğlu and Gary McGuire, *When is $x^{-1} + L(x)$ a permutation in odd characteristic?*
9:50 – 10:15 Ferruh Özbudak and Zülfükar Saygı, *On the exact number of solutions of certain linearized equations*
10:15 – 10:40 Arpita Maitra and Goutam Paul, *Symmetric incoherent eavesdropping against MDI QKD*

10.40 – 11.10 *Coffee break*

Lattices and Codes
Chairman: Patric R. J. Östergård
11:10 – 11:35 Wittawat Kositwattanarerk and Frédérique Oggier, *On construction D and related constructions of lattices from linear codes*
11:35 – 12:00 Soon Sheng Ong and Frédérique Oggier, *Lattices from totally real number fields with large regulator*
12:00 – 12:25 David A. Karpuk, Camilla Hollanti and Emanuele Viterbo, *Probability bounds for two-dimensional algebraic lattice codes*

12.30 – 14:00 *Lunch*

Invited Talk 3
Invited talk by Frank Kschischang, CANCELLED

Network Coding and Geometry
Chairman: Marcus Greferath
14:00 – 14:25 Ivan Landjev and Peter Vandendriesche, *On the rank of incidence matrices in projective Hjelmslev spaces*
14:25 – 14:50 Linda Beukemann, Klaus Metsch and Leo Storme, *On weighted $(\delta v_{\mu+1}, \delta v_{\mu}; k-1, q)$-minihypers, q square*

Network Coding and Related Topics 1
Chairman: Camilla Hollanti
14:50 – 15:15 Eimear Byrne, *On bounds for network codes*
15:15 – 15:40 Heide Gluesing-Luerssen, *Tail-biting trellis realizations and local reductions*

15.40 – 16:10 *Coffee break*

16:10 – 16:35 Iván Blanco Chacón, Dionis Remón and Camilla Hollanti, *Fuchsian codes for AWGN channels*
16:35 – 17:00 Jinquan Luo, *Weight distribution of cyclic codes with several non-zeroes*

18:10 Departure from the lobby for the banquet

19:00 Banquet

Friday, April 19

Gabidulin Codes
Chairman: Tuvi Etzion
9:00 – 9:25 Wenhui Li, Vladimir Sidorenko and Di Chen, *On transform-domain decoding of Gabidulin codes*
9:25 – 9:50 Antonia Wachter-Zeh and Alexander Zeh, *Interpolation-based decoding of interleaved Gabidulin codes*
9:50 –10:15 Anna-Lena Trautmann, Natalia Silberstein and Joachim Rosenthal, *List decoding of Lifted Gabidulin codes via the Plücker embedding*

10.15 – 10:45 *Coffee break*

Network Coding and Related Topics 2
Chairman: Simon Blackburn
10:45 – 11:10 Michael Braun, Tuvi Etzion, Patric R. J. Östergård, Alexander Vardy and Alfred Wassermann, *On the existence of q-analogs of Steiner systems*
11:10 – 11:35 Johan S. R. Nielsen and Alexander Zeh, *Multi-trial Guruswami-Sudan decoding for generalised Reed-Solomon codes*
11:35 – 12:00 Emanuele Bellini, Eleonora Guerrini and Massimiliano Sala, *Some bounds on the size of codes*

12:00 – 13:00 *Lunch*

END of WORKSHOP

13:00 – 17:00 COST - Management Committee (MC) – meeting