PROGRAM — SETA 2014 (24–28 NOVEMBER 2014)

Monday 24 November

Invited talk

09:30–10:30 **Kathy Horadam**: *Relationships between CCZ and EA equivalence classes and corresponding code invariants*

10:30–11:00 Coffee break

Boolean functions

11:00–11:30 Claude Carlet, Guangpu Gao, and Wenfen Liu: *Results on constructions of rotation symmetric bent and semi-bent functions*

11:30–12:00 Qichun Wang and Chik How Tan: *Properties of a family of cryptographic Boolean functions*

12:00–14:00 Lunch

14:00–14:30 Andrew Klapper: *A new transform related to distance from a Boolean function (Extended abstract)*

14:30–15:00 Chunming Tang and Yanfeng Qi: *Constructing hyper-bent functions from Boolean functions with the Walsh spectrum taking the same value twice*

15:30–16:00 Sihem Mesnager: *Characterizations of plateaued and bent functions in characteristic p*

16:00–16:30 Coffee break

Tuesday 25 November

Invited talk

09:30–10:30 **Tor Helleseth**: *Two-level autocorrelation sequences and a proof of the Lin conjecture*

10:30–11:00 Coffee break

Perfect sequences

11:00–11:30 Oleg Kuznetsov: *A method of optimisation of the exhaustive computer search for perfect sequences*

11:30–12:00 Vladimir E. Gantmakher and Mikhail V. Zaleshin: *Almost six-phase sequences with perfect periodic autocorrelation function*

12:00–14:00 Lunch

14:00–14:30 Sam Blake and Andrew Tirkel: *A construction for perfect periodic autocorrelation sequences*

14:30–15:00 Guang Gong and Solomon Golomb: *A simple construction of almost perfect quinary ASK and QAM sequences*

15:00–15:30 Coffee break

Correlation of arrays

15:30–16:00   Santiago Barrera Acevedo: *Inflation of perfect arrays over the basic quaternions of size* $m \times n = (q + 1)/2$

16:00–16:30   Samuel Blake, Oscar Moreno, and Andrew Tirkel: *Families of 3D arrays for video watermarking*

Wednesday 26 November

Invited talk

09:30–10:30   **Bernhard Schmidt**: *Circulant Hadamard matrices and twisted cyclotomic integers*

10:30–11:00   Coffee break

Relative difference sets

11:00–11:30   Vladimir Tonchev and David Clark: *The nonexistence of* $(18, 3, 18, 6)$ *relative difference sets*

Aperiodic correlation

11:30–12:00   Anatolii Leukhin and Egor Potekhin: *Exhaustive search for optimal minimum peak sidelobe binary sequences up to length* 80

Afternoon   Excursion

Thursday 27 November

Invited talk

09:30–10:30   **Josef Dick**: *The inverse of the star-discrepancy problem and the generation of pseudorandom numbers*

10:30–11:00   Coffee break

Pseudorandom sequences and stream ciphers

11:00–11:30   Elena Dubrova: *An equivalence-preserving transformation of shift registers*

11:30–12:00   Weihua Liu and Andrew Klapper: *A lattice rational approximation algorithm for AFSRs over quadratic integer rings*

12:00–14:00   Lunch

14:00–14:30   Domingo Gomez and Ana Gomez: *On the lattice structure of inversive PRNG via the additive order*

14:30–15:00   Harry Bartlett, Ali Alhamdan, Leonie Simpson, Ed Dawson, and Kenneth Koon-Ho Wong: *Weaknesses in the initialisation process of the common scrambling algorithm stream cipher*

15:00–15:30   Coffee break

15:30–16:00   Ting Gu and Andrew Klapper: *Distribution properties of half-l-sequence*

Crosscorrelation of sequences

16:00–16:30   Yongbo Xia, Tor Helleseth, and Gaofei Wu: *A note on cross-correlation distribution between a ternary m-sequence and its decimated sequence*

Evening   Banquet

Friday 28 November

Prime numbers in sequences

09:30–10:00   Solomon Golomb: *Conjectures involving sequences and prime numbers*

OFDM and CDMA

10:00–10:30   Yutaka Jitsumatsu, Masahiro Hashiguchi, and Tatsuro Higuchi: *Optimal sign patterns for a generalized Schmidl-Cox method*

10:30–11:00   Longye Wang, Xiaoli Zeng, and Hong Wen: *A novel construction of asymmetric sequence pairs set with zero-correlation zone*

11:00–11:30   Coffee break

Frequency-hopping sequences

11:30–12:00   Hongyu Han, Daiyuan Peng and Xing Liu: *On low-hit-zone frequency-hopping sequence sets with optimal partial Hamming correlation*

12:00–12:30   Xing Liu, Daiyuan Peng and Hongyu Han: *Improved Singleton bound on frequency hopping sequences*