Final Program for SETA 2008

Lexington, Kentucky, September 14–18, 2008

Contributed talks are 25 minutes, including time for questions and for changing speakers.

Sunday, September 14

Registration: 6 – 8PM
Reception: 7 – 9PM

Monday, September 15

8 AM – ??? Registration

8:45 AM Opening remarks

Session 1: Probabilistic Methods and Randomness Properties of Sequences

9–10 AM Plenary talk: Point Sets and Sequences for Quasi-Monte Carlo: Construction Methods and Quality Criteria, by Pierre L'Ecuyer

10–10:30 AM Coffee break

10:30–12:35 AM

New Distinguishers Based on Random Mappings Against Stream Ciphers, by Meltem Sönmez Turan, Çağdaş Çalık, Nurdan Buz Saran, and Ali Doğanaksoy

On Independence and Sensitivity of Statistical Randomness Tests, by Meltem Sönmez Turan, Ali Doğanaksoy, and Serdar Boztaş

A Probabilistic Approach on Estimating the Number of Modular Sonar Sequences, by Ki Hyeon Park and Hong-Yeop Song

A Study on the Pseudorandom Properties of Sequences Generated via the Additive Order, by Honggang Hu and Guang Gong

On the Average Distribution of Power Residues and Primitive Elements in Inversive and Nonlinear Recurring Sequences, by Ayça Çeşmelioğlu and Arne Winterhof

12:35–2 PM Lunch

Session 2: Correlation

2–3:15 PM

Some Results on the Arithmetic Correlation of Sequences, by Mark Goresky and Andrew Klapper

A Class of Nonbinary Codes and Sequence Families, by Xiangyong Zeng, Nian Li, and Lei Hu

Results on Crosscorrelation and Autocorrelation of Sequences, by Faruk Göloğlu and Alexander Pott

3:15–3:45 PM Coffee break

3:45–5 PM

m-Sequences of Lengths $2^{2k}-1$ and 2^k-1 with at most Four-Valued Cross Correlation, by Tor Helleseth and Alexander Kholosha

On the Correlation Distribution of Kerdock Sequences, by Xiaohu Tang, Tor Helleseth, and Aina Johansen

Two New Families of Low Correlation Interleaved QAM Sequences, by Gagan Garg, P. Vijay Kumar, and C.E. Veni Madhavan

You are on your own for dinner

Tuesday, September 16

Session 3: Combinatorial and Algebraic Foundations

9–10 AM Plenary talk: Algebraic Causes with Combinatorial Effects, by Robert J. McEliece, with Anna S. Bertiger and Sarah Sweatlock

10–10:30 AM Coffee break

10:30–12:35 AM

The Finite Harmonic Oscillator Sequences, by Shamgar Gurevich, Ronny Hadani, and Nir Sochen

Projective de Bruijn Sequences, by Yuki Ohtsuka, Makoto Matsumoto and Mariko Hagita

Multiplicative Character Sums of Recurring Sequences with Rédei Functions, by Domingo Gomez and Arne Winterhof

On the Connection between Kloosterman Sums and Elliptic Curves, by Petr Lisoněk

12:10–2 PM Lunch

2:15 PM–??? Excursion and Dinner: Kentucky Horse Park

Wednesday, September 17

Session 4: Security Aspects of Sequences

9–10 AM Plenary talk: Sequences, DFT and Resistance Against Fast Algebraic Attacks, by Guang Gong

10–10:30 AM Coffee break

10:30–12:35 AM

Expected π-Adic Security Measures of Sequences, by Andrew Klapper

Distance-Avoiding Sequences for Extremely Low Bandwidth Authentication, by Michael J. Collins and Scott Mitchell

On the Number of Linearly Independent Equations Generated by XL, by Sondre Rønjom and Håvard Raddum

2^n-Periodic Binary Sequences with Fixed k-error Linear Complexity for $k = 2$ or 3, by Ramakanth Kavuluru

Generalized Joint Linear Complexity of Linear Recurring Multisequences, by Wilfried Meidl and Ferruh Özbudak

12:35–2 PM Lunch

Session 5: Algorithms

2–3:15 PM

A Lattice-Based Minimal Partial Realization Algorithm in the Multivariable Case, by Li-Ping Wang

A Fast Jump Ahead Algorithm for Linear Recurrences in a Polynomial Space, by Hiroshi Haramoto, Makoto Matsumoto, and Pierre L'Ecuyer

Parallel Generation of l-Sequences, by Cedric Lauradoux and Andrea Röck

Session 6: Correlation of Sequences over Rings

3:15–3:45 PM Coffee break

3:45–5 PM

Design of M-ary Low Correlation Zone Sequence Sets by Interleaving, by Jin-Ho Chung and Kyeongcheol Yang

The Peak to Sidelobe Level of the Most Significant Bit of Trace Codes over Galois Rings, by Patrick Solé and Dimitrii Zinoviev

On Partial Correlations of Various $\mathbb{Z}_4$ Sequence Families, by Parampally Udaya and Serdar Boztaş

6:00 – 9:00 pm: Banquet

Thursday, September 18

Session 7: Nonlinear Functions over Finite Fields

9–10 AM Plenary talk: On the Higher Order Nonlinearities of Boolean Functions and S-Boxes, and their Generalizations, by Claude Carlet

10–10:30 AM Coffee break

10:30–12:35 AM

On a Class of Permutation Polynomials over $\mathbb{F}_{2^n}$, by Pascale Charpin and Gohar Kyureghyan

On 3-to-1 and Power APN S-Boxes, by Deepak Kumar Dalai

Negabent Functions in the Maiorana-McFarland Class, by Kai-Uwe Schmidt, Matthew G. Parker and Alexander Pott

New Perfect Nonlinear Multinomials over $\mathbb{F}_{p^{2k}}$ for any Odd Prime p, by Lilya Budaghyan and Tor Helleseth

A New Tool for Assurance of Perfect Nonlinearity, by Nuray At and Stephen D. Cohen

You are on your own for lunch