

Program of SETA 2010

Monday

Morning

8h45-9h **Opening the conference:** *Yves Poilane, Head of Telecom ParisTech*

9h-10h **Invited Talk:** *Jong-Seon No: Low Correlation Zone Sequences*

10h-10h30 Coffee break

10h30-12h **Algorithmic aspects**

- *Srdjan Budisin: Decimation Generator of Zadoff-Chu Sequences*

- *Jean-Michel Chabloz, Shohreh Mansouri, Elena Dubrova: An Algorithm for Constructing a Fastest Galois NLFSR Generating a Given Sequence*

- *Cedomir Stefanovic, Dragana Bajic: Acquisition Times of Contiguous and Distributed Marker Sequences: A Cross-Bifix Analysis]*

Afternoon

14h-15h **Frequency hopping**

- *Xianhua Niu, Daiyuan Peng, Fang Liu: Lower Bounds on the Average Partial Hamming Correlations of Frequency Hopping Sequences with Partial Low Hit Zone*

- *Jin-Ho Chung, Kyeongcheol Yang: New Families of Frequency-Hopping Sequences of Length mN Derived from the k -Fold Cyclotomy*

15h-15h30 Coffee break

15h30-16h30 **Multiple access systems**

- *Kenneth Shum, Yijin Zhang, Wing Shing Wong: User-irrepressible sequences*

- *Wu Dianhua, Cao Jiayun, Fan Pingzhi: New Optimal Variable-Weight Optical Orthogonal Codes*

Tuesday

Morning

9h-10h **Invited Talk:** *Arne Winterhof: Recent Results on Recursive Nonlinear Pseudorandom Number Generators.*

10h-10h30 Coffee break

10h30-12h **Linear complexity**

- *Ayca Cesmelioglu, Wilfried Meidl*: A General Approach to Construction and Determination of the Linear Complexity of Sequences Based on Cosets
- *Fang Liu, Daiyuan Peng, Xiaohu Tang, Xianhua Niu*: On the Autocorrelation and Linear Complexity of q-ary Prime n-square Sequences
- *Ana Salagean, Alexandra Alecu*: An Improved Approximation Algorithm for Computing the k -error Linear Complexity of Sequences Using the Discrete Fourier Transform

Afternoon

14h-15h **Finite fields**

- *Jean-Francois Michon, Philippe Ravache*: Transformations on Irreducible Binary Polynomials
- *Philippe Langevin, Emrah CakCak*: Power Permutations in Dimension 32

15h-15h30 Coffee break

15h30-16h30 **Character sums**

- *Domingo Gomez*: Multiplicative Character Sums with Counter-Dependent Nonlinear Congruential Pseudorandom Number Generators
- *Faruk Göloğlu, Gary McGuire, Richard Moloney*: Ternary Kloosterman Sums Modulo 18 Using Stickelberger's Theorem

16h30-17h **Merit factor**

- *Jonathan Jedwab, Kai-Uwe Schmidt*: Appended m-Sequences with Merit Factor Greater Than 3.34

17h-17h30 **Best paper award ceremony**

Wednesday (morning)

9h-10h30 **FCSR**

- *Andrew Klapper, Mark Goresky*: A With-Carry Walsh Transform
- *Zhen Pan, Wei Su, Xiaohu Tang*: Clock-Controlled FCSR Sequence with Large Linear Complexity
- *Abdelaziz Marjane, Boufeldja Allailou*: Vectorial Conception of FCSR

10h30-11h Coffee break

11h-12h **Hadamard matrices and transforms**

- *Branislav Popovic*: Fourier Duals of Björck Sequences
- *Krystal Guo, Guang Gong*: New Constructions of Complete Non-cyclic Hadamard Matrices, Related Function Families and LCZ Sequences

Thursday

Morning

9h-10h30 **Cryptography**

- *Zoubida Jadda, Patrice Parraud*: Z_4 -Nonlinearity of a Constructed Quaternary Cryptographic Functions Class
- *Pascal Véron, Fabien Herbaut*: A Public Key Cryptosystem Based Upon Euclidean Addition Chains
- *Yang Yang, Xiaohu Tang, Udaya Parampalli*: Optimal Authentication Codes from Difference Balanced Functions

10h30-11h Coffee break

- 11h-12h **Invited Talk**: *James Massey*: New Extensions and Applications of Welch-Bound-Equality Sequence Sets

Afternoon

14h-15h **Statistical analysis**

- *Fatih Sulak, Ali Doğanaksoy, Barış Ege, Onur Koçak*: Evaluation of Randomness Test Results for Short Sequences
- *Dragana Bajic, Cedomir Stefanovic*: Statistical Analysis of Search for Set of Sequences in Random and Framed Data

15h-15h30 Coffee break

15h30-17h30 **Boolean functions and related problems**

- *Risto Hakala, Kaisa Nyberg*: On the Nonlinearity of Discrete Logarithm in F_{2^n}
- *Jean-Pierre Flori, Hugues Randriambololona, Gérard Cohen, Sihem Mesnager*: On a Conjecture About Binary Strings Distribution
- *Pantelimon Stanica, Sugata Gangopadhyay, Ankita Chaturvedi, Aditi Kar Gangopadhyay, Subhamoy Maitra*: Nega-Hadamard transform, Bent and Negabent Functions
- *Jérémy Parriaux, Philippe Guillot, Gilles Millérioux*: Synchronization of Boolean Dynamical Systems: a Spectral Characterization

Friday

Morning

9h-10h30 **Nonbinary sequences**

- *Evgeny Krenzel*: Some constructions of almost-perfect, odd-perfect and perfect polyphase and almost-polyphase sequences
- *Yeow Meng Chee, Yin Tan, Yue Zhou*: Almost p -ary Perfect Sequences
- *Tor Helleseth, Alexander Kholosha*: Sequences, Bent Functions and Jacobsthal Sums

10h30-11h Coffee break

11h-11h30 **Infinite sequences**

Solomon Golomb: Infinite Sequences With Finite Cross-Correlation.

11h30-12h30 **Invited Talk**: *Rob Calderbank*: Reed Muller Sensing Matrices and the LASSO.