

PROGRAM — BFA 2019 (June 16-21, Florence, Italy)

Monday, June 17

09:00 - 09:05	Lilya Budaghyan	Welcoming
09:05 - 09:50	Tor Helleseth	Differential Spectrum of Non-binary Kasami Power Functions and Related Topics
09:50 - 10:35	Lilya Budaghyan	On the Carlet-Charpin-Zinoviev Paper
10:35 - 11:05	Coffee break	
11:05 - 11:50	Claude Carlet	Recent Uses and Problems on Boolean and Vectorial Functions
11:50 - 12:10	Patrick Felke	The Multivariate Method Strikes Again: New Power Mappings with Low Differential Uniformity in Odd Characteristic
12:10 - 12:30	Marco Calderini, and Irene Villa	On the Boomerang Uniformity of some Permutation Polynomials
12:30 - 14:00	Lunch	
14:00 - 14:45	Daniel Katz	Differential Spectra of Power Permutations
14:45 - 15:05	Canan Kaşıkçı	Shifted Plateaued Functions and Their Differential Properties
15:05 - 15:25	Matúš Jókay, Peter Špaček, and Pavol Zajac	Linear and Differential Properties of S-boxes with Respect to Modular Addition
15:25 - 15:55	Coffee break	
15:55 - 16:15	Yongbo Xia, Xianglai Zhang, and Chunlei Li	The Differential Spectrum of A Ternary Power Mapping
16:15 - 16:35	Luís T. A. N. Brandão, Çağdaş Çalk, Morris Dworkin, Nathan Dykas, René Peralta, and Meltem Sönmez Turan	Research Directions on the Complexity of Boolean Circuits for Codes and Cryptography
16:35 - 16:55	Nikolay Kaleyski	Announcement of the Boolean Functions Website

PROGRAM — BFA 2019 (June 16-21, Florence, Italy)

Tuesday, June 18

09:00 - 09:45	Marco Calderini	EA-equivalence Classes of Known APN Functions in Small Dimensions
09:45 - 10:30	Robert Coulter	Planar Functions and Commutative Semifields: A Status Report and Beyond
10:30 - 11:00	Coffee break	
11:00 - 11:45	Sihem Mesnager	Equations over the Finite Field \mathbb{F}_{2^n}
11:45 - 12:05	Aleksandr Kutsenko	Isometric Mappings of the Set of all Boolean Functions into Itself which Preserve Self-duality and the Rayleigh Quotient
12:05 - 12:25	Lilya Budaghyan, Claude Carlet, Diana Davidova, Tor Helleseeth, Ferdinand Ihringer, and Tim Penttila	Relation between o-equivalence and EA-equivalence for Niho Bent Functions
12:25 - 14:00	Lunch	
14:00 - 14:45	Ulrich Dempwolff	Equivalence of Functions over Finite Spaces via Group Theory
14:45 - 15:05	Ayça Çeşmeliolu, Wilfried Meidl, and Alexander Pott	Vectorial Bent Functions in Odd Characteristic and their Components
15:05 - 15:25	Petr Lisoněk	Kloosterman Zeros and Vectorial Bent Functions
15:25 - 15:55	Coffee break	
15:55 - 16:40	Chunming Tang	Combinatorial t-designs from Special Functions
16:40 - 16:55	Nicolas T. Courtois	On the Existence of Boolean Functions Resistant Against Non-Linear Invariant Attacks
17:00 - 18:00	CCDS Associate Editors' Meeting	

PROGRAM — BFA 2019 (June 16-21, Florence, Italy)

Wednesday, June 19

9:00 - 9:45	Daniel Panario	Ambiguity, Deficiency and Differential spectrum of Low Degree Normalized Permutation Polynomials over Finite Fields
9:45 - 10:30	Chunlei Li	On Decoding of Maximum Rank Distance Codes
10:30 - 11:00	Coffee break	
11:00 - 11:45	Nian Li	Constructions of linear codes from cryptographic functions
11:45 - 12:05	Lilya Budaghyan, Marco Calderini, Claude Carlet, and Nikolay Kaleyski	On a Relationship between Gold and Kasami Functions and other Power APN Functions
12:05 - 12:25	Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski	Generalized Binomial APN Functions
12:25 - 14:00	Lunch	
14:00 - 14:20	Lilya Budaghyan, Nikolay Kaleyski, Constanza Riera, and Pantelimon Stănică	Partially APN Functions with APN-like Polynomial Representations
14:20 - 14:40	Yuri Borissov	On the Distinctness of Some Kloosterman Sums
14:40 - 15:00	Claude Gravel, and Daniel Panario	Squeezing a Vectorial Nonlinear Binary Transformation between the Generator and Parity Check Matrices of a Linear Code
15:00 - 15:20	Nurdagül Anbar	Permutations of the Form $x^2 + ax + b$ and Curves over Finite Fields
15:20 - 15:55	Coffee break	

Thursday, June 20

09:00 – 09:45	Emmanuel Prouff	Algorithmic Approaches to Defeat Side Channel Analysis
09:45 – 10:05	Martianus Frederic Ezerman, Adamas Aqsa Fahreza, and Janusz Szmidt	Perturbation of Binary de Bruijn Sequences and the Spectral Theory of Graphs
10:05 – 10:25	Romain Alléaume	Quantum-Computational Hybrid Cryptography based on the Boolean Hidden Matching Problem
10:25 – 11:00	Coffee break	
11:00 – 11:45	Alev Topuzoğlu	Permutation Polynomials over Finite Fields and Factorization
11:45 – 12:05	Augustine Musukwa, Massimiliano Sala, and Marco Zaninelli	On the Derivatives of Balanced Functions
12:05 – 12:25	Faruk Göloğlu, and Jiří Pavlů	Search for APN Permutations Among known APN Functions
12:25 – 14:00	Lunch	
14:00 – 14:45	Yuyin Yu	Classification of Quadratic APN Functions with Coefficients in GF(2)
14:45 – 15:05	Alexey Oblaukhov	Metrically Regular Subsets of the Boolean cube
15:05 – 15:25	Çağdaş Çalık, Meltem Sönmez Turan, and René Peralta	Boolean Functions with Multiplicative Complexity 3 and 4
15:25 – 15:55	Coffee break	
15:55 – 16:15	Oktay Olmez	Links Between Plateaued Functions and Partial Geometric Difference Sets
16:15 – 16:20	Lilya Budaghyan	Farewell