

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

Monday, June 17

09:00 - 09:45	Tor Helleseth	Differential Spectrum of Non-binary Kasami Power Functions and Related Topics
09:45 - 10:30	Lilya Budaghyan	On the Carlet-Charpin-Zinoviev Paper
10:30 - 11:00	Coffee break	
11:00 - 11:45	Claude Carlet	Recent Uses and Problems on Boolean and Vectorial Functions
11:45 - 12:05	Patrick Felke	The Multivariate Method Strikes Again: New Power Mappings with Low Differential Uniformity in Odd Characteristic
12:05 - 12:25	Marco Calderini, and Irene Villa	On the Boomerang Uniformity of some Permutation Polynomials
12:25 - 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 Çalık, 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	TBA
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 Çeşmelioglu, 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

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

Thursday, June 20

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	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
11:45 - 12:05	Lilya Budaghyan, Nikolay Kaleyski, Constanza Riera, and Pantelimon Stănică	Partially APN Functions with APN-like Polynomial Representations
12:25 - 14:00	Lunch	
14:00 - 14:45	Yuyin Yu	Classification of Quadratic APN Functions with Coefficients in \mathbb{F}_2
14:45 - 15:05	Faruk Göloğlu, and Jiří Pavlů	Search for APN Permutations Among known APN Functions
15:05 - 15:25	Lilya Budaghyan, Marco Calderini, Claude Carlet, and Nikolay Kaleyski	On a Relationship between Gold and Kasami Functions and other Power APN Functions
15:25 - 15:55	Coffee break	
15:55 - 16:15	Lilya Budaghyan, and Nikolay Kaleyski	Generalized Binomial APN Functions
16:15 - 16:35	Çağdaş Çalık, Meltem Sönmez Turan, and René Peralta	Boolean Functions with Multiplicative Complexity 3 and 4
16:35 - 16:55	Oktay Olmez	Links Between Plateaued Functions and Partial Geometric Difference Sets

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

Friday, June 21

9:00 - 9:45	Emmanuel Prouff	Algorithmic Approaches to Defeat Side Channel Analysis
9:45 - 10:30	Xiangyong Zeng	A survey on complete permutation polynomials
10:30 - 11:00	Coffee break	
11:00 - 11:45	Sylvain Guilley	Substitution boxes in cryptography
11:45 - 12:05	Martianus Frederic Ezerman, Adamas Aqsa Fahreza, and Janusz Szmidt	Perturbation of Binary de Bruijn Sequences and the Spectral Theory of Graphs
11:45 - 12:05	Nurdagül Anbar	Permutations of the Form $x^k - \gamma \text{Tr}(x)$ and Curves over Finite Fields
12:25 - 14:00	Lunch	
14:00 - 14:45	Nian Li	Constructions of linear codes from cryptographic functions
14:45 - 15:05	Romain Alléaume	Quantum-Computational Hybrid Cryptography based on the Boolean Hidden Matching Problem
15:05 - 15:25	Claude Gravel, and Daniel Panario	Squeezing a Vectorial Nonlinear Binary Transformation between the Generator and Parity Check Matrices of a Linear Code
15:25 - 15:55	Coffee break	
15:55 - 16:15	Yuri Borissov	On the Distinctness of Some Kloosterman Sums
16:15 - 16:35	Alexey Oblaukhov	Metrically Regular Subsets of the Boolean cube

SOCIAL ACTIVITIES — BFA 2019

Sunday June 16: Welcoming Dinner

19:00 at the Villa Finally
Via Bolognese, 134 R – 50139 Firenze

Wednesday June 19: Excursion

08:30 - 08:45	Meetup at the Villa Finally
09:00	Departure by bus from the Villa Finally
10:30 - 12:00	Excursion in the Tuscan countryside
12:00 - 14:00	Visit and wine tasting at Lornano wine farm
14:00 - 16:00	Visit to the Castello di Staggia
16:00 - 17:30	Visit to San Gimignano
18:30 - 19:00	Arrival at the Villa Finally

Friday June 21: Banquet

Palazzo Borghese
Via Ghibellina, 110 N – 50122 Firenze

18:15	Arrival at the Palazzo Borghese , aperitif in the <i>Sala degli Specchi</i> (Mirror Room) and <i>Salotti Monumentali</i> (Monumental Rooms)
19:00 - 21:00	Dinner in the <i>Galleria Monumentale</i> (Monumental Gallery)
21:00 - 22:00	Open bar
22:30	Conclusion

SOCIAL ACTIVITIES — BFA 2019

