PROGRAM

The 2nd International Workshop on

Boolean Functions and their Applications (BFA)

July 3-8, 2017

Sosltrand, Hotel, Os, Norway.

BFA - Schedule

	Tuesday	**Wednesday**	**Friday**
09:00-09:45	Kaisa Nyberg	Pante Stanica	Alexander Pott
09:45 - 10:30	Marco Calderini	Yue Zhou	Levina Alla
10:30 - 11:00	**Coffee Break**		
11:00 - 11:45	Léo P. Perrin	Patrick Solé	Chunlei Li
11:45 - 12:05	Stjepan Picek	Bimal Mandal	Nikolay S. Kaleyski
12:05 - 12:30	Valeriya Idrisova	Wilfried Meidl	Fuad Hamidli
12:30 - 14:00	**Lunch**		
14:00 - 14:45	Claude Carlet	Sihem Mesnager	Ashley Montanaro
14:45 - 15:30	Pierrick Meaux	Nian Li	Matthew G. Parker
15:30 - 16:00	**Coffee Break**		
16:00 - 16:20	Xi Chen	Yi Lu	Joan Boyar
16:20 - 16:40	Irene Villa	Meltem S. Turan	Stian Fauskanger
16:40 - 17:00	Bo Sun	Bjørn Greve	**End**
17:00 - 17:45	Anne Canteaut	Natalia Tokareva	
Monday - Friday	Dinners 19:00 (for participants staying in Solstrand hotel)		
Thursday	Excursion 08:15 - 18:40 (stop in Bergen at 18:00)		

BFA Program

Tuesday		
09:00-09:45	Kaisa Nyberg	Linear and statistical independence of linear approximations
09:45-10:30	Marco Calderini	On APN permutations
10:30-11:00	**Break**	
11:00-11:45	Léo Perrin	On S-box reverse-engineering: from cryptanalysis to the big APN problem
11:45-12:05	Stjepan Picek	On the S-boxes generated via cellular automata rules
12:05-12:30	Valeriya Idrisova	On APN functions EA-equivalent to permutations
12:30-14:00	**Lunch**	
14:00-14:45	Claude Carlet	On the possible exponents of APN power functions and their relation with Sidon sets and sum-free sets
14:45-15:30	Pierrick Meaux	Symmetric encryption scheme adapted to fully homomorphic encryption scheme: new criteria for Boolean functions
15:30-16:00	**Break**	
16:00-16:20	Xi Chen, Longjiang Qu, Chao Li	Investigating the CCZ-equivalence between functions with low differential uniformity by projected differential spectrum
16:20-16:40	Irene Villa	On some properties of quadratic APN functions of a special form
16:40-17:00	Bo Sun	Quadratic APN polynomials in few terms in small dimensions
17:00-17:45	Anne Canteaut	Proving resistance of a block cipher against invariant attacks

BFA Program

Wednesday		
09:00-09:45	Pante Stanica	(Generalized) Boolean functions: invariance under some groups of transformations and differential properties
09:45-10:30	Yue Zhou	Rank metric codes and related structures
10:30-11:00	**Break**	
11:00-11:45	Patrick Solé	Orthogonal group and Boolean functions
11:45-12:05	Bimal Mandal, Pantelimon Stanica, Sugata Gangopadhyay	New classes of generalized bent functions
12:05-12:30	Wilfried Meidl, Alexander Pott	Generalized bent functions from spreads and their spectra
12:30-14:00	**Lunch**	
14:00-14:45	Sihem Mesnager	Generalized plateaued functions and admissible (plateaued) functions
14:45-15:30	Nian Li	Some recent progress in the applications of Niho exponents
15:30-16:00	**Break**	
16:00-16:20	Yi Lu, Ziran Tu, Dan Zhang	Efficient numerical approximation of the DMC channel capacity
16:20-16:40	Cagdas Calik, Meltem S. Turan, Rene Peralta	On the multiplicative complexity of 6-variable Boolean functions
16:40-17:00	Bjørn M. Greve, Håvard Raddum, Gunnar Fløystad, Øyvind Ytrehus	Solving polynomial systems over Boolean rings by elimination of variables
17:00-17:45	Natalia Tokareva	On structural properties of the class of bent functions

BFA Program

Friday		
09:00-09:45	Alexander Pott	Duality of bent functions in odd characteristic
09:45-10:30	Levina Alla	Wavelets transformation and its applications in information security
10:30-11:00	**Break**	
11:00-11:45	Chunlei Li	On the periodic sequences with maximal nonlinear complexity
11:45-12:05	Nikolay S. Kaleyski	PI is not at least as succinct as MODS
12:05-12:30	Fuad Hamidli, Ferruh Ozbudak	On alltop functions
12:30-14:00	**Lunch**	
14:00-14:45	Ashley Montanaro	Boolean functions in quantum computation
14:45-15:30	Matthew G. Parker	Boolean functions in a message-passing, quantum, and machine learning context
15:30-16:00	**Break**	
16:00-16:20	Joan Boyar, Magnus G. Find, Rene Peralta	Low-depth, low-size circuits for cryptographic applications
16:20-16:40	Stian Fauskanger, Igor Semaev	Separable statistics and multivariate linear cryptanalysis
End		

fjordtours

Norway in a nutshell® Bergen via Voss 6/7-2017

Local guide from Bergen ByExpert will meet the group by Solstrand Hotel before departure.

Departure from Solstrand 08:30
Private coach from Tide Turbuss
Arrival Gudvangen 11:30

(Telephone number Tide in emergency: +47 91 77 97 30)

Departure from Gudvangen 11:45
Fjord cruise with the Fjords boat Vision of the Fjords
Arrival Flam 13:15
You must enter the boat as a group

Lunchbuffet at Flåmstova in Furukroa 13:30
Starters, warm main courses and desserts and coffee/tee
Other drinks must be paid directly

Departure from Flåm 14:50
The Flam Railway – own section marked UIB – Informatics
You must enter the train as a group and use the reserved section
Arrival Myrdal 15:46

Departure from Myrdal 15:52
The Bergen Railway – own section marked UIB - Informatics
You must enter the train as a group and use the reserved section
Arrival Bergen 17:57

Departure from Bergen railway station 18:05
Private coach from Tide Turbuss
Arrival Solstrand 18:45

(Telephone number Tide in emergency: +47 91 77 97 30)

The local guide will stay with you until the bus leaves from Bergen railway station

We wish you a nice trip!