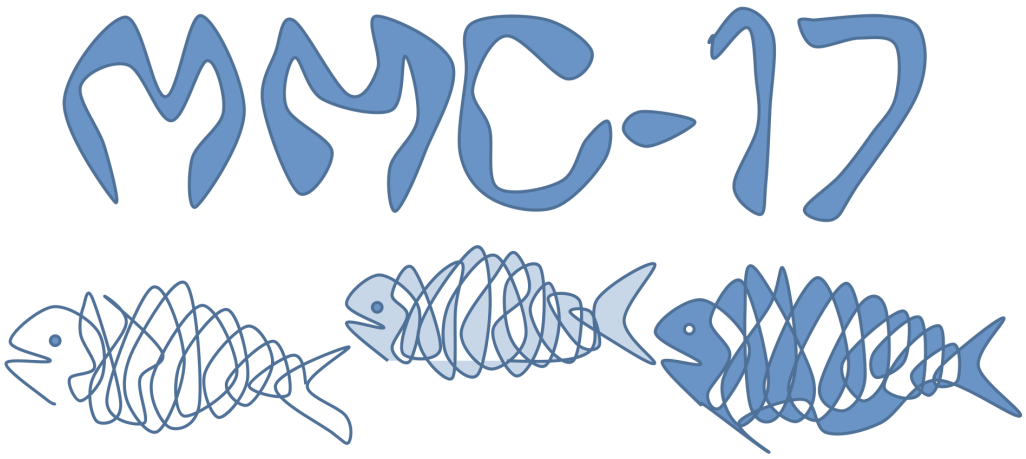

The International Workshop on

Mathematical Methods for Cryptography (MMC)

September 4-8, 2017

Svolvær, Thon Hotel, Lofoten, Norway.

MMC - Program

Monday - 4th September		
09:00-09:50	Thomas Johansson	Combinatorial methods for solving LWE
09:50-10:40	Gregor Leander	Quantum attacks on symmetric crypto
10:40-11:10	**Coffee Break**	
11:10-12:10	Bart Preneel	A perspective on cryptocurrencies
12:10-12:30	Lejla Batina Pedro Maat Masolino Joost Renes	Hardware design for supersingular isogeny Diffie-Hellman key exchange
12:30-14:00	**Lunch**	
14:00-14:50	Sondre Rønjom	Structural cryptanalysis of block ciphers
14:50-15:10	Patrick Felke	On the security of biquadratic C* public-key cryptosystems
15:10-15:30	Håvard Raddum Srimathi Varadharajan	Representing integer multiplication using binary decision diagrams
15:30-16:00	**Coffee Break**	
16:00-17:00	Kaisa Nyberg	Current trends in linear cryptanalysis
17:00-17:20	Ryan Henry	Computing low-weight discrete logarithms
17:20-17:40	Bjørn M. Greve Håvard Raddum Gunnar Fløystad Øyvind Ytrehus	Re-linearization and elimination of variables in boolean equation systems

MMC - Program

Tuesday - 5th September		
09:00-09:50	Igor A. Semaev	Separable statistics in linear cryptanalysis
09:50-10:40	Pingzhi Fan	Recent advances in doppler resilient sequence design and applications
10:40-11:10	**Coffee Break**	
11:10-12:10	Claude Carlet	Characterizations of differentially uniform functions by the Walsh transform and related cyclic difference set-like combinatorial structures
12:10-12:30	Kerem Varici Svetla Nikova Ventzislav Nikov Vincent Rijmen	Constructions of S-boxes with uniform sharing
12:30-14:00	**Lunch**	
14:00-14:50	Victor Zinoviev	On Kloosterman sums
14:50-15:40	P. Vijay Kumar	An explicit construction of a high-rate minimum storage regenerating code with low sub-packetization level and selectable repair degree
15:40-16:10	**Coffee Break**	
16:10-17:10	Guang Gong	On ideal t-tuple distribution of orthogonal functions in filtering de bruijn generators
17:10-17:30	Svetla Nikova Ventzislav Nikov Vincent Rijmen	Decomposition of permutations in a finite field

MMC - Program

Wednesday - 6th September

Excursion (09:30 - 18:00)

- Start from Svolvær : 09:30

- Tour to Trollfjorden (about one hour);

- In Trollfjorden we swerve the fishsoup and then start Sea eagle safari;

- Lunch at Nyvågar rorbuhotell: 12.30 (about 2 hours)

- Go further to Henningsværr to visit the gallerie Lofotens Hus (about 2 hours)

- Back to Svolvær: 18:00

MMC - Program

Thursday - 7th September		
09:00-09:50	Kyeongcheol Yang	Decoding of block Turbo codes
09:50-10:40	Torleiv Kløve	Codes for errors of limited magnitude - a short survey
10:40-11:10	**Coffee Break**	
11:10-12:10	Øyvind Ytrehus	Optimum MDS convolutional codes over $GF(2^m)$ and their relation to the trace function
12:10-12:30	Xiao-Nan Lu Masakazu Jimbo	Locating arrays with error-correcting ability
12:30-14:00	**Lunch**	
14:00-14:50	Jong-Seon No	Code-based post-quantum cryptography
14:50-15:10	László Csirmaz Péter Ligeti	Secret sharing on large girth graphs
15:10-15:30	Assen Bojilov Yuri Borissov	An approach to computing the number of finite field elements with prescribed trace and co-trace
15:30-16:00	**Coffee Break**	
16:00-17:00	Xiaohu Tang	MDS codes for distributed storage system
17:00-17:20	Patrick Holzer Thomas Wunderer Johannes A. Buchmann	Recovering short generators of principal fractional ideals in cyclotomic fields of conductor pq
17:20-17:40	José Manuel E. Valença Óscar Pereira	An algebraic approach to the design of block ciphers

MMC - Program

Friday - 8th September		
09:00-09:50	Joan Daemen	Column-parity mixing layers
09:50-10:40	Christian Rechberger	Rasta and Picnic
10:40-11:10	**Coffee Break**	
11:10-12:10	Chunming Rong	Secure and robust data services in Cloud and Fog
12:10-12:30	Filipp Valovich	A new DDH-based PRF with application to distributed private data analysis
12:30-14:00	**Lunch**