Symmetric Cryptography 2018

Monday, January 8

Time	Presenter	Title	Duration
7:30-9:00	Breakfast		
9:00-10:30 Chair: Anne Canteaut	Willi Meier	TMD tradeoffs on small-state stream ciphers	15
	Vasily Mikhalev	Towards Low Energy Stream Ciphers	20
	Frederik Armknecht	An LFSR-based Proof of Work	15
	Christoph Dobraunig	Rasta: Designing a cipher with low ANDdepth and few ANDs per bit	15
10:30-11:00	Break		
11:00-12:00 Chair: Yannik Seurin	Stefan Lucks	Leakage-Resilient Authenticated Encryption	25
	Bart Mennink	Key Prediction Security of Keyed Sponges	15
12:15-13:45	Lunch		
14:00-15:30 Chair: Thomas Peyrin	Gilles Van Assche	Tree-searching for trail bounds	25
	Dmitry Khovratovich	Merkle Tree is not Optimal	20
	Yosuke Todo	Fast Correlation Attack Revisited	Long
15:30-16:00	Break		
16:00-16:30	Adi Shamir	Towards Quantitative Analysis of Cyber Security	Long
18:00-19:00	Dinner		

Tuesday, January 9

Time	Presenter	Title	Duration
7:30-9:00	Breakfast		
9:00-10:15 Chair: Gaëtan Leurent	Damian Vizár	Robustness of the CAESAR Candidates	15
	Discussion on CAESAR with focus on robustness		
10:15-10:45	Break		
10:45-12:00 Chair: Gilles Van Assche	Henri Gilbert	Key-Recovery Attacks on Full Kravatte	25
	Maria Eichlseder	Clustering related-tweak characteristics	15
12:15-13:45	Lunch		
14:00-15:30 Chair: Gregor Leander	Stav Perle	Conditional Linear Cryptanalysis	short
	Tomer Ashur	Linear cryptanalysis using low-bias approximations	short
	Kaisa Nyberg	Multidimensional, Affine and Conditional Linear Cryptanalysis	short
15:30-16:00	Break		
16:00-17:30 Chair: Tetsu Iwata	Stefano Tessaro	The Chi-Squared Method	long
	Mridul Nandi	Some applications of the chi square method	long
18:00-19:00	Dinner		

Wednesday, January 10

Time	Title	Presenter	Duration
7:30-9:00	Breakfast		
9:00-10:15 Chair: Stefano Tessaro	Yannick Seurin	Beyond-Birthday-Bound Secure MACs	45
	Kan Yasuda	Recent Advancements in Sponge-Based MACs	short
10:15-10:45	Break		
10:45-12:00 Chair: Christian Rechberger	Joan Daemen	The collision resistance of keyed hashing	20
	Nicky Mouha	Challenges and Opportunities for the Standardization of Threshold Cryptography	15
	Stefan Kölbl	Tools on Cryptanalysis	short
12:15-13:45	Lunch		
14:00- Chair: Joan Daemen	Hike		
18:00-19:00	Dinner		

Thursday, January 11

Time	Presenter	Title	Duration
7:30-9:00	Breakfast		
9:00-10:30 Chair: Joan Daemen	Christian Rechberger	A survey of recent results on AES permutations	25
	Orr Dunkelman	Cryptanalysis of Reduced Round AES, Revisited	25
	Meiqin Wang	Integral Attacks on AES	25
10:30-11:00	Break		
11:00:-12:00 Chair: Kaisa Nyberg	Anne Canteaut	On Sboxes sharing the same DDT	long
	Yu Sasaki	Boomerang Connectivity Table (BCT) for Boomerang Attacks	long
12:15-13:45	Lunch		
14:00-15:30 Chair: Yu Sasaki	Tetsu Iwata	QCCA on Feistel	short
	Arnab Roy	Some Feistel structures with low degree rounds functions	20
	Léo Perrin	Generalized Feistel Networks with Optimal Diffusion	20
15:30-16:00	Break		
16:00-17:30 Chair: Orr Dunkelman	Itai Dinur	An Improved Affine Equivalence Algorithm	long
	Christof Beierle	Invariant Attacks and (Non-)linear Approximations	25
	Maria Naya-Plasencia	recent results on reduced versions of Ketje	15

18:00-19:00	Dinner

Friday, January 12

Time	Presenter	Title	Duration
7:30-9:00	Breakfast		
9:00-10:15	Kazuhiko Minematsu	On the security of LINE messaging application	short
Chair: Joan	Discussion on Mass Surveillance		
10:15-10:45	Break		
10:45-12:00 Chair: Kan Yasuda	Virginie Lallemand	Multiplication Operated Encryption with Trojan Resilience	20
	Gregor	Instantiating the Whitened Swap-or-Not Block Cipher	15
	Dan(?)	Mess of Proofs	25
12:15-13:45	Lunch		