(Tentative) Programme of Dagstuhl Seminar „Symmetric Cryptography“

Monday, January 16

Time	Title	Presenter	Duration
- 9:00	Breakfast		
9:00 - 10:45	Tag size does matter: attacks and proofs for the TLS record protocol	Kenny Paterson	45mins
	AES Characteristics	Kerem Varici	30mins
	On the security of key-alternating ciphers	John Steinberger	30mins
10:45-11:15	Coffee		
11:15 – 12:15	Collisions are not Incidental: A Compression Function exploiting Discrete Geometry	Martijn Stam	30mins
	TBD (Related to block ciphers)	Christian Rechberger	30mins
12:15-13:45	Lunch		
13:45 - 15:15	Practical Collisions in Round-Reduced Keccak	Itai Dinur	30mins
	Oracle Reducibility for Hash Functions	Marc Fischlin	30mins
	SIMD BLAKE	Jean-Philippe Aumasson	30mins
15:15-15:45	Coffee and Cake		
15:45 - 18:00	Cryptanalysis on LPMAC	Yu Sasaki	30mins
	GCM Security, Revisited	Tetsu Iwata	45mins
	Authenticated ciphers	Daniel J. Bernstein, Tanja Lange	45mins
18:00-19:00	Dinner		

Tuesday, January 17

Time	Title	Presenter	Duration
- 8:45	Breakfast		
9:00 - 10:45	Cesar	Alex Biryukov	30mins
	Multiple results on multiple encryption	Itai Dinur, Orr Dunkelman, Adi Shamir	75 mins
10:45-11:15	Coffee		
11:15 – 12:15	Two recent topics in linear cryptanalysis	Andrey Bogdanov	30mins
	On the distribution of linear biases, three instructive examples	Gregor Leander	30mins
12:15-13:45	Lunch		
14:00 - 17:00	Hike		
18:00-19:00	Dinner		

Wednesday, January 18

Time	Title	Presenter	Duration
Breakfast			
9:00 - 10:45	New attacks on GOST	Adi Shamir	30 mins
	Some observations on distinguishing-H attacks	Kan Yasuda	30 mins
	Improved rebound attack on the finalist Grøstl	Maria Naya-Plasencia	30 mins
10:45 - 11:15	Coffee		
11:15 - 12:15	Accurate data complexity estimates for χ^2 distinguishers of large distributions	Kaisa Nyberg	30 mins
	McOE authenticated encryption	Christian Forler	30 mins
12:15 - 13:45	Lunch		
13:45 - 15:15	Discussion session		
15:15-15:45	Coffee and Cake		
15:45 - 18:00	Conjectures in mirror theory	Jacques Patarin	30 mins
	KISS: a bit too simple	Greg Rose	30 mins
	Bounds for balanced Feistel networks	Kyoji Shibutani	30 mins
18:00 - 19:00	Dinner		

Thursday, January 19

Time	Title	Presenter	Duration
Breakfast			
9:00 - 10:45	Improved security of balanced and unbalanced contracting Feistel schemes.	Rodolphe Lampe	45 mins
	EAX-Prime	Tetsu Iwata	15 mins
	An IDEA to consider	Orr Dunkelmann	45 mins
10:45 - 11:15	Coffee		
11:15 - 12:15	AES meets Serpent	Jean-Philippe Aumasson	30 mins
	Analysis of ARX-based hash functions	Florian Mendel	30 mins
12:15 - 13:45	Lunch		
13:45 – 15:15	Private discussions		
15:15-15:45	Coffee and Cake		
15:45 - 18:00	Bit splitting for knapsack and codes	Antoine Joux	30 mins
	MARS attacks - revisited	Jakob Wenzel	30 mins
	Security results for SHA3-candidates *and* Some key indifferentiability of block ciphers	Elena Andreeva	30 mins
	A block cipher based on card shuffling	Phil Rogaway	15 mins
18:00 - 19:00	Dinner		

Friday, January 20

Time	Title	Presenter	Duration
Breakfast			
9:00 - 10:45	New stuff on Keccak	Joan Daemen	45 mins
	The preimage security of double-block-length compression functions	Frederik Armknecht	30 mins
	Key-alternating ciphers (continued)	John Steinberger	30 mins
10:45 - 11:15	Coffee		
11:15 - 12:15	Getting results under weak expectations	Yevgeniy Dodis	60 mins
12:15 - 13:45	Lunch		