FSE 2007

26 March, Monday

8:00 – 8:45	Registration
8:45 – 8:55	Welcome notes
Rolf Tarrach, rector of University of Luxembourg	
8:55 – 9:00	Overview of the submissions and the review process
Alex Biryukov	
Session 1. CRYPTANALYSIS and DESIGN of HASH FUNCTIONS (I) (chair: Bart Preneel)	
9:00 – 9:25	Producing Collisions for PANAMA, Instantaneously
Joan Daemen and Gilles Van Assche	
9:25 – 9:50	Cryptanalysis of FORK-256
Krystian Matusiewicz, Thomas Peyrin, Olivier Billet	
9:50 – 10:15	Grindahl — a family of hash functions
Lars R. Knudsen, Christian Rechberger, Søren S. Thomsen	
10:15 – 10:45	**BREAK**
Session 2. STREAM CIPHER CRYPTANALYSIS (I) (chair: Willi Meier)	
10:45 – 11:10	Overtaking VEST
Antoine Joux and Jean-Rene Reinhard	
11:10 – 11:35	Differential-Linear Attacks against the Stream Cipher Phelix
Hongjun Wu and Bart Preneel	
11:35 – 12:00	Cryptanalysis of Achterbahn-128/80
Maria Naya Plasencia	
12:00 – 14:00	**LUNCH**

Session 3. THEORY **(chair: Tetsu Iwata)**	
14:00 – 14:25	How to Enrich an Enciphering Scheme's Domain
Thomas Ristenpart and Phillip Rogaway	
14:25 – 14:50	Security Analysis of Constructions Combining FIL Random Oracles
Yannick Seurin and Thomas Peyrin	
14:50 – 15:15	Bad and Good Ways of Post-Processing Biased Random Numbers
Markus Dichtl	
15:15 – 15:45	**BREAK**
Session 4.1. FAST TALKS: BLOCK CIPHER CRYPTANALYSIS **(chair: Pascal Junod)**	
15:45 – 16:00	Improved Slide Attacks
Eli Biham, Orr Dunkelman, and Nathan Keller	
16:00 – 16:15	A New Class of Weak Keys for Blowfish
Orhun Kara, Cevat Manap	
Session 4.2 FAST TALKS: BLOCK CIPHER DESIGN **(chair: Pascal Junod)**	
16:15 – 16:30	The 128-bit Blockcipher CLEFIA
Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata	
16:30 – 16:45	New Light-Weight DES Variants Suited for RFID Applications
Axel Poschmann, Gregor Leander, Kai Schramm, Christof Paar	
27 March, Tuesday	
Session 5. BLOCK CIPHER CRYPTANALYSIS **(chair: Lars Knudsen)**	
9:00 – 9:25	A New Attack on 6-Round IDEA
Eli Biham, Orr Dunkelman and Nathan Keller	

9:25 – 9:50	Related-Key Rectangle Attacks on Reduced AES-192 and AES-256
Jongsung Kim and Seokhie Hong and Bart Preneel	
9:50 – 10:15	Detailed Analysis on XSL Applied to BES
Chu-Wee Lim and Khoongming Khoo	
10:15 – 10:45	**BREAK**
Session 6. STREAM CIPHER CRYPTANALYSIS (II) **(chair: Kaisa Nyberg)**	
10:45 – 11:10	On the Security of IV Dependent Stream Ciphers
Come Berbain and Henri Gilbert	
11:10 – 11:35	Two General Attacks on Pomaranch-like Keystream Generators
Håkan Englund, Martin Hell, Thomas Johansson	
11:35 – 12:00	Analysis of QUAD
Bo-Yin Yang, Owen Chia-Hsin Chen, Daniel J. Bernstein, Jiun-Ming Chen	
12:00 – 14:00	**LUNCH**
14:00 – 14:50	**INVITED TALK**
Jean-Charles Faugere	
15:00 – 16:00	**RUMP SESSION**
(chair: Joan Daemen)	
16:00 – 19:00	**SIGHTSEEING ACTIVITY**
19:30	**CONFERENCE DINNER in the Bourglinster castle**
28 March, Wednesday	
Session 7. CRYPTANALYSIS of HASH FUNCTIONS (II) **(chair: Mitsuru Matsui)**	
9:00 – 9:25	Message Freedom in MD4 and MD5 Collisions: Application to APOP
Gaëtan Leurent	

9:25 – 9:50	New Message Difference for MD4
Yu Sasaki, Lei Wang, Kazuo Ohta, Noboru Kunihiro	
9:50 – 10:15	Gröbner Basis based Cryptanalysis of SHA-1
Makoto Sugita, Mitsuru Kawazoe, Hideki Imai	
10:15 – 10:45	**BREAK**
Session 9. THEORY of STREAM CIPHERS **(chair: Orr Dunkelman)**	
10:45 – 11:10	Algebraic Immunity of S-boxes and Augmented Functions
Simon Fischer and Willi Meier	
11:10 – 11:35	Generalized Correlation Analysis of Vectorial Boolean Functions
Claude Carlet, Khoongming Khoo, Chu-Wee Lim, Chuan-Wen Loe	
Session 10. SIDE CHANNEL ATTACKS **(chair: Jin Hong)**	
11:35 – 12:00	An Analytical Model for Time-Driven Cache Attacks
Kris Tiri, Onur Acıiçmez, Michael Neve, and Flemming Andersen	
12:00 – 14:00	**LUNCH**
Session 11. MACs and SMALL BLOCK CIPHERS **(chair: Stefan Lucks)**	
14:00 – 14:25	Improving the Security of MACs via Randomized Message Preprocessing
Yevgeniy Dodis and Krzysztof Pietrzak	
14:25 – 14:50	New Bounds for PMAC, TMAC, and XCBC
Kazuhiko Minematsu and Toshiyasu Matsushima	
14:50 – 15:15	Perfect Block Ciphers With Small Blocks
Louis Granboulan and Thomas Pornin	
15:15	**Workshop closing**
Jean-Claude Asselborn	
Extra sightseeing activities with luxembourgian guides	