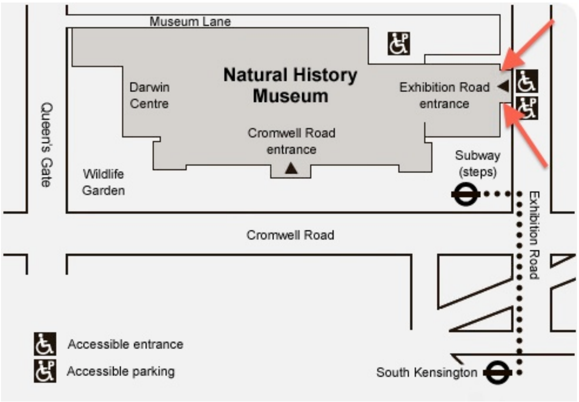
FSE 2014 – Program

All talks will be held in the *Flett Theatre* at the *Natural History Museum*, in South Kensington. To reach the Flett Theatre, FSE 2014 participants **should use the museum's entrance located at the Exhibition Road (NOT the main entrance at Cromwell Road)**.



Coffee breaks will be in the theatre foyer. Lunch on Monday and Tuesday will be served in the adjacent *From the Beginning gallery*; on Wednesday it will be served in the foyer.

Monday, 03 March 2014

08:30 - 09:30: Registration and coffee at the foyer of the Flett Theatre

09:30 - 09:40: *Workshop Opening*
FSE 2014 general chairs

09.40 - 10.55: *Session 1 - Designs* (chair: Mitsuru Matsui)
Direct Construction of Recursive MDS Diffusion Layers using Shortened BCH Codes
Daniel Augot and Matthieu Finiasz
(INRIA Saclay - Île-de-France and LIX - École Polytechnique)

LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations
Vicente Grosso, Gaëtan Leurent, François-Xavier Standaert and Kerem Varici
(UCL Crypto Group, Belgium, and INRIA, France)

SPRING: Fast Pseudorandom Functions from Rounded Ring Products
Abhishek Banerjee, Hai Brenner, Gaëtan Leurent, Chris Peikert and Alon Rosen
(Georgia Institute of Technology, INRIA Team SECRET and IDC Herzliya)

10.55 - 11.20: *Coffee break*

11.20 - 12.10: *Session 2 - Invited Talk I* (chair: Christian Rechberger)
Low weight polynomials and crypto
Thomas Johansson (Lund University)

12.10 - 13.30: *Lunch* (in the *From the Beginning gallery*)

13:30 - 15:10: *Session 3 - Cryptanalysis I* (chair: Orr Dunkelman)

Match Box Meet-in-the-Middle Attack against KATAN
Thomas Fuhr and Brice Minaud
(ANSSI, France)

Collision Spectrum, Entropy Loss, T-Sponges, and Cryptanalysis of GLUON-64
Leo Paul Perrin and Dmitry Khovratovich
(University of Luxembourg)

Improved All-Subkeys Recovery Attacks on FOX, KATAN and SHACAL-2 Block cipher
Takanori Isobe and Kyoji Shibutani
(Sony Corporation, Japan)

Improved Single-Key Attacks on 9-Round AES-192/256
Leibo Li, Keting Jia and Xiaoyun Wang
(Shandong University and Tsinghua University, China)

15.10 - 15.35: *Coffee break*

15.35 - 17.45: *Session 4 - Authenticated Encryption* (chair: Serge Vaudenay)

CLOC: Authenticated Encryption for Short Input
Tetsu Iwata, Kazuhiko Minematsu, Jian Guo and Sumio Morioka
(Nagoya University, NEC Corporation, Nanyang Technological University and NEC Europe)

APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography
Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha and Kan Yasuda
(KU Leuven, University of Twente, Technical University of Denmark and NTT Secure Platform Laboratories)

COBRA: A Parallelizable Authenticated Online Cipher Without Block Cipher Inverse
Elena Andreeva, Atul Luykx, Bart Mennink and Kan Yasuda
(KU Leuven and NTT Secure Platform Laboratories)

Pipelineable On-Line Encryption
David McGrew, Scott Fluhrer, Stefan Lucks, Christian Forler, Jakob Wenzel, Farzaneh Abed and Eik List
(Cisco Systems and Bauhaus-Universität Weimar)

Cryptanalysis of FIDES
Itai Dinur and Jeremy Jean
(Ecole Normale Supérieure, Paris, France)

FSE 2014 – Program

Tuesday, 04 March 2014

08:30: Registration and coffee at the foyer of the Flett Theatre

08.45 - 10.25: *Session 5 - Foundations and Theory* (chair: Elena Andreeva)

Security Analysis of Key-Alternating Feistel Ciphers
Rodolphe Lampe and Yannick Seurin
(University of Versailles and ANSSI, France)

The Related-Key Analysis of Feistel Constructions
Manuel Barbosa and Pooya Farshim
(HASLab - INESC TEC and Univ. Minho, and TU Darmstadt)

The Indistinguishability of the XOR of k permutations
Benoît Cogliati, Rodolphe Lampe and Jacques Patarin
(Université de Versailles Saint-Quentin-en-Yveline)

Impact of ANSI X9.24-1:2009 Key Check Value on ISO/IEC 9797-1:2011 MACs
Tetsu Iwata and Lei Wang
(Nagoya University and Nanyang Technological University)

10.25 - 10.50: *Coffee break*

10.50 - 11.40: *Session 6 - Stream Ciphers* (chair: Thomas Johansson)

Plaintext Recovery Attacks Against WPA/TKIP
Kenneth G. Paterson, Jacob C. N. Schuldt and Bertram Poettering
(Royal Holloway, University of London)

Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WPA
Sourav Sen Gupta, Subhamoy Maitra, Willi Meier, Goutam Paul and Santanu Sarkar
(Indian Statistical Institute, FHNW Switzerland and Chennai Mathematical Institute)

11.40 - 13.10: *Lunch* (in the *From the Beginning gallery*)

13.10 - 15.15: *Session 7 - Cryptanalysis II* (chair: Anne Canteaut)

Probabilistic Slide Cryptanalysis and Its Applications to LED-64 and Zorro
Hadi Soleimany
(Aalto University)

Improved Linear Sieving Techniques with Applications to Step-Reduced LED-64
Itai Dinur, Orr Dunkelman, Nathan Keller and Adi Shamir
(ENS-Paris, University of Haifa, Bar-Ilan University, and Weizmann Institute, Israel)

Differential-Linear Cryptanalysis Revisited
Céline Blondeau, Gregor Leander and Kaisa Nyberg
(Aalto University and Ruhr University Bochum)

Improved Slender-set Linear Cryptanalysis
Guo-Qiang Liu, Chen-Hui Jin and Chuan-Da Qi
(Information Science Technology Institute, Zhengzhou, and Xinyang Normal University)

Cryptanalysis of KLEIN
Virginie Lallemand and María Naya-Plasencia
(INRIA Paris-Rocquencourt)

15.15 - 15.35: *Coffee break*

15.35 - 16.50: *Session 8 - Hash Functions* (chair: Thomas Peyrin)

Branching Heuristics in Differential Collision Search with Applications to SHA-512
Maria Eichlseder, Florian Mendel and Martin Schläffer
(Graz University of Technology)

On the Minimum Number of Multiplications Necessary for Universal Hash Constructions
Mridul Nandi
(Indian Statistical Institute)

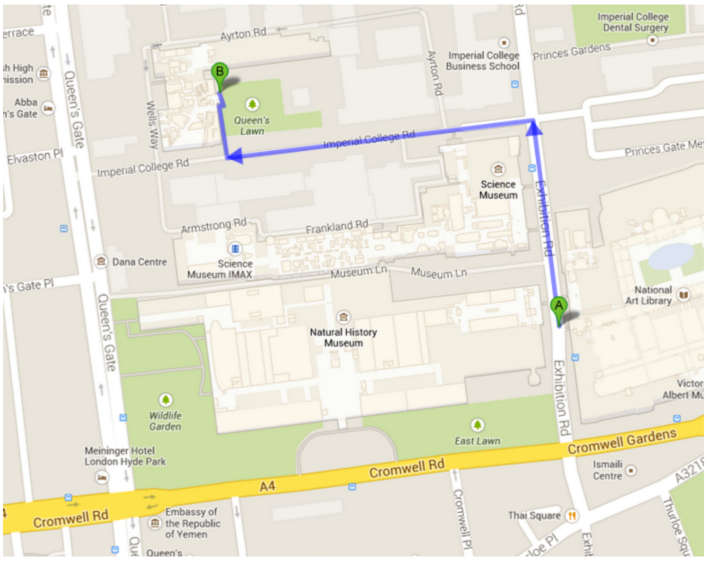
Collision Attack on 5 Rounds of Groestl
Florian Mendel, Vincent Rijmen and Martin Schläffer
(TU Graz and KU Leuven)

16.50 - 17.50: *Rum(p) session* (chairs: Dan Bernstein and Tanja Lange)

Talks in the Flett Theatre, with *refreshments* served in the foyer

19:30 - 23:00: *Workshop Banquet*

Queens Tower Rooms, Sherfield Building, Imperial College (5-min walk from the museum)



FSE 2014 – Program

Wednesday, 05 March 2014

08:45: Coffee served at the foyer of the Flett Theatre

09.15 - 10.55: *Session 9 - Cryptanalysis III* (chair: Frederik Armknecht)

Differential Cryptanalysis of round-reduced Simon and speck
Farzaneh Abed, Eik List, Jakob Wenzel and Stefan Lucks
(Bauhaus Universität Weimar)

Differential Analysis of Block Ciphers SIMON and SPECK
Alex Biryukov, Arnab Roy and Vesselin Velichkov
(University of Luxembourg)

Equivalent Key Recovery Attacks against HMAC and NMAC with Whirlpool Reduced to 7 Rounds
Jian Guo, Yu Sasaki, Lei Wang, Meiqin Wang and Long Wen
(Nanyang Technological University, NTT Secure Platform Laboratories and Shandong University)

Multiple Differential Cryptanalysis of Round-Reduced PRINCE
Anne Canteaut, Thomas Fuhr, Henri Gilbert, María Naya-Plasencia and Jean-René Reinhard
(INRIA and ANSSI, France)

10.55 - 11.20: *Coffee break*

11.20 - 12.35: *Session 10 - Advanced Constructions* (chair: Carlos Cid)

Efficient Fuzzy Search on Encrypted Data
Alexandra Boldyreva and Nathan Chenette
(Georgia Institute of Technology and Clemson University)

Invited talk II
New Encryption Primitives for Uncertain Times
Thomas Ristenpart (University of Wisconsin-Madison)

12:35 - 14:00: *Lunch and workshop closing* (at the foyer of the Flett Theatre)