Monday, 21st February

08:00 Registration and Morning Coffee
09:00 Opening

1. New Designs
   09:15 A New MAC Construction ALRED and a Specific Instance Alpha-MAC
          Joan Daemen and Vincent Rijmen
   09:40 New Applications of T-functions in Block Ciphers and Hash Functions
          Alexander Klimov and Adi Shamir
   10:05 The Poly1305-AES Message-Authentication Code
          Daniel J. Bernstein
   10:30 Coffee Break

2. Stream Ciphers I
   11:00 Narrow T-functions
          Magnus Daum
   11:25 A New Class of Single Cycle T-functions
          Jin Hong, Dong Hoon Lee, Yongjin Yeom, and Daewan Han
   11:50 F-FCSR: Design of a New Class of Stream Ciphers
          François Arnault and Thierry P. Berger
   12:15 Lunch (Restaurant Chez Clement)

3. Invited Talk
   14:00 Attacks and Protection of Hash Functions
          Xuejia Lai

4. Boolean Functions
   14:45 Cryptographically Significant Boolean Functions: Construction and Analysis in Terms of Algebraic Immunity
          Deepak Kumar Dalai, Kishan Chand Gupta, and Subhamoy Maitra
   15:10 The ANF of the Composition of Addition and Multiplication mod $2^n$ with a Boolean Function
          An Braeken and Igor Semaev
   15:35 Coffee Break

5. Rump Session 16:00 – 17:00
   19:00 Cocktail (ENSTA)
Tuesday, 22\textsuperscript{nd} February

6. Block Ciphers I
09:00 New Combined Attacks on Block Ciphers
   Eli Biham, Orr Dunkelman, and Nathan Keller
09:25 Small Scale Variants of the AES
   Carlos Cid, Sean Murphy, and Matt Robshaw

7. Stream Ciphers II
09:50 Unbiased Random Sequences from Quasigroup String Transformations
   Smile Markovski, Danilo Gligoroski, and Ljupco Kocarev
10:15 Coffee Break
10:45 A New Distinguisher for Clock Controlled Stream Ciphers
   Håkan Englund and Thomas Johansson
11:10 Analysis of the Bit-Search Generator and Sequence Compression Techniques
   Aline Gouget, Hervé Sibert, Côme Berbain, Nicolas Courtois, Blandine Debraize, and Chris Mitchell
11:35 Some Attacks on the Bit-Search Generator
   Martin Hell and Thomas Johansson
12:00 Lunch (Restaurant \textit{Chez Clement})

8. Hash Functions
14:00 SMASH – A Cryptographic Hash Function
   Lars R. Knudsen
14:25 Security Analysis of a 2/3-rate Double Length Compression Function in Black-Box Model
   Mridul Nandi, Wonil Lee, Kouichi Sakurai, and Sangjin Lee
14:50 Preimage and Collision Attacks on MD2
   Lars R. Knudsen and John E. Mathiassen
15:15 Coffee Break

9. Modes of Operation
15:45 How to Enhance the Security of the 3GPP Confidentiality and Integrity Algorithms
   Tetsu Iwata and Kaoru Kurosawa
16:10 Two-Pass Authenticated Encryption Faster than Generic Composition
   Stefan Lucks
16:35 Padding Oracle Attacks on CBC-mode Encryption with Random and Secret IVs
   Arnold K.L. Yau, Kenneth G. Paterson, and Chris J. Mitchell
20:00 Banquet
Wednesday, 23rd February

10. Stream Ciphers III

09:00 Analysis of the Non-linear Part of Mugi
Alex Biryukov and Adi Shamir

09:25 Two Attacks Against the HBB Stream Cipher
Antoine Joux and Frédéric Muller

09:50 Two Linear Distinguishing Attacks on VMPC and RC4A and Weakness of the RC4 Family of Stream Ciphers
Alexander Maximov

10:15 Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4
Eli Biham, Louis Granboulan, and Phong Q. Nguyen

10:40 Coffee Break

11. Block Ciphers II

11:10 Related-Key Rectangle Attacks on Reduced Version of SHACAL-1 and AES-192
Seokhie Hong, Jongsung Kim, Sangjin Lee, and Bart Preneel

11:35 New Attacks against Reduced-Round Versions of IDEA
Pascal Junod

12:00 Lunch (Restaurant Chez Clement)

12. Implementations

14:00 How to Maximize Software Performance of Symmetric Primitives on Pentium III and 4 Processors
Mitsuru Matsui and Sayaka Fukuda

14:25 A Side-Channel Analysis Description of the AES S-box
Elisabeth Oswald, Stefan Mangard, Norbert Pramstaller, and Vincent Rijmen

14:50 DPA attacks and S-boxes
Emmanuel Prouff

15:15 Closing