SESSION 1: SIGNATURE SCHEMES, CHAIR:

08:40 – 09:10 Batch Verification of ECDSA Signatures
Sabyasachi KARATI, Abhijit DAS, Dipanwita ROYCHOWDHURY, Bhargav BELLUR, Debojyoti BHATTACHARYA, Aravind LYER

09:10 – 09:40 Extended Security Arguments for (Ring) Signature Schemes
Sidi Mohammed EL YOUSFI ALAOUI, Özgür DAGDELEN, Pascal VERON, David GALINDO, Pierre-Louis CAYREL

09:40 – 10:10 Sanitizable Signatures with Several Signers and Sanitizers
Sébastien CANARD, Amandine JAMBERT, Roch LESCUYER

10:20 – 11:20 Official Opening Ceremony

11:20 – 11:30 Coffee Break

SESSION 2: STREAM CIPHERS, CHAIR:

11:40 – 12:10 Attack Based on Direct Sum Decomposition against the Nonlinear Filter Generator
Jingjing WANG, Xiangxue LI, Kefei CHEN, Wenzheng ZHANG

12:10 – 13:10 Invited Talk, Stream Ciphers, a Perspective by Willi MEIER

13:10 – 15:10 Lunch Break

SESSION 3: APPLICATIONS OF INFORMATION THEORY, CHAIR:

15:10 – 15:40 Fuzzy Vault for Multiple Users
Julien BRINGER, Hervé CHABANNE, Mélanie FAVRE

15:40 – 16:10 Bounds and Constructions for 1-Round (0, delta)-Secure Message Transmission against Generalized Adversary
Reihaneh SAFAVI-NAINI, Mohammed ASHRAFUL ALAM TUHIN

16:10 – 16:40 Improving the Performance of the SYND Stream Cipher
Mohammed MEZIANI, Gerhard HOFFMANN, Pierre-Louis CAYREL

16:40 – 17:00 Coffee Break

17:00 – 17:30 Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT
Jiazhe CHEN, Meiqin WANG, Bart PRENEEL
SESSION 4: BLOCK CIPHERS, CHAIR:

17:30 – 18:00 Three-Subset Meet-in-the-Middle Attack on Reduced XTEA
Yu SASAKI, Lei WANG, Yasuhide SAKAI, Kazuo SAKIYAMA, Kazuo OHTA

18:00 – 18:30 Differential Cryptanalysis of Reduced-Round ICEBERG
Yue SUN, Meiqin WANG, Shujia JIANG, Qiumei SUN

18:30 – 19:00 Compact Implementation and Performance Evaluation of Block Ciphers in ATtiny Devices
Thomas EISENBARTH, Zheng GONG, Tim GUNEYSU, Stefan HEYSE, Sebastiaan INDESTEEGE, Stéphanie KERCKHOF, François KOEUNE, Tomislav NAD, Thomas PLOS, France REGAZZONI, François-Xavier STANDAERT, Loïc van Oldeneel tot Oldenzeel

END of DAY 1 at 19:00

Wednesday, July 11, 2012

SESSION 5: NETWORK SECURITY PROTOCOLS, CHAIR:

9:00 – 9:30 Cryptanalysis of Enhanced TTS, STS and all its Variants, or: Why Cross-Terms are important
Enrico THOMAE, Christopher WOLF

9:30 – 10:00 A Complementary Analysis of the (s)YZ and DIKE Protocols
Augustin P. SARR, Philippe ELBAZ-VICENT

10:00 – 10:30 Coffee Break

SESSION 6: PUBLIC-KEY CRYPTOGRAPHY, CHAIR:

10:30 – 11:00 A new attack on RSA and CRT-RSA
Abderrahmane NITAJ

11:00 – 11:30 Shift-Type Homomorphic Encryption and its Application to Fully Homomorphic Encryption
Frederik ARMKNECHT, Stefan KATZENBEISSER, Andreas PETER

11:30 – 12:30 Invited Talk, Fully Homomorphic Encryption: Current State of the Art, by Craig GENTRY

12:40 – 14:30 Lunch Break

SESSION 7: CRYPTANALYSIS OF HASH FUNCTIONS, CHAIR:

14:30 – 15:00 The Collision Security of MDC-4
Ewan FLEISCHMANN, Christian FORLER, Stefan LUCKS

15:00 – 15:30 SPN-Hash: Improving the Provable Resistance Against Differential Collision Attacks
15:30 – 16:00 Security Analysis and Comparison of the SHA-3 Finalists BLAKE, Groestl, JH, Keccak, and Skein
   Elena ANDREEVA, Bart MENNINK, Bart PRENEEL, Marjan SKROBOT

16:00 – 16:30 Coffee Break

SESSION 8: HASH FUNCTIONS: DESIGN AND IMPLEMENTATION, CHAIR:

16:30– 17:00 The GLUON family: a lightweight Hash function family based on FCSRs
   Thierry P. BERGER, Joffrey D’HAYER, Kevin MARQUET, Marine MINIER, Gaël THOMAS

17:00 – 17:30 SHA-3 on ARM11 processors
   Peter SCHAWABE, Bo-Yin YANG, Shang-Yi YANG

17:40 – 18:30 Rump Session, Chair:

END of DAY 1 at 18:30

Thursday, July 12, 2012

SESSION 9: ALGORITHMS FOR PUBLIC-KEY CRYPTOGRAPHY, CHAIR:

9:00 – 9:30 Improved Fixed-base Comb Method for Fast Scalar Multiplication
   Mohameda. F. NASHWA, Mohsin H. A. HASHIM, Michael HUTTER

9:30 – 10:00 Optimal First-Order Masking with Linear and Non-Linear Bijections
   Houssem MAGHREBI, Claude CARLET, Sylvain GUILLEY, Jan-Luc DANGER

10:00 – 10:30 Coffee Break

SESSION 10: CRYPTOGRAPHIC PROTOCOLS, CHAIR:

10:30 – 11:00 Size-Hiding in Private Set Intersection: Existential Results and Constructions
   Paolo D’ARCO, María Isabel González VASCO, Ángel L. Pérez DEL POZO, Claudio SORIENTE

11:00 – 11:30 Round-optimal black-box statistically binding selective-opening secure commitments
   David XIAO

11:30 – 12:30 Invited Talk, Black-Box Reductions and Separations in Cryptography, by Marc FISCHLIN

12:30 – 12:45 Closing remarks

12:45 – 14:30 Lunch break

14:30 – 19:30 Social program: Excursion to FEZ

20:45 – 23:30 Gala Dinner