EC 2013 Rump Session

19:30 Aggelos Kiayias
Cryptographic Puzzles : The Introduction

19:35 Thomas Johansson and Phong Nguyen:
Cryptanalysis of EUROCRYPT 2013

19:45 Nigel Smart:
Revolutionizing IACR Publications

20:00 Tsukasa Ishiguro and Shinsaku Kiyomoto and Yutaka Miyake and Tsuyohsi Takagi:
Parallel Gauss Sieve Algorithm : Solving the SVP in the Ideal Lattice of 128 dimens
ions

20:05 Alptekin Kupcu
Password-based Football

20:10 Sergey Gorbunov and Vinod Vaikuntanathan and Hoeteck Wee:
Attribute-Based Encryption for Circuits

20:15 Itai Dinur and Orr Dunkelman and Nathan Keller and Adi Shamir:
How to Efficiently Compute the Diagonal of a Difference Distribution Table

20:20 Itai Dinur and Orr Dunkelman and Nathan Keller and Adi Shamir:
Key Recovery Attacks on 3-round Even-Mansour (with Applications!)

20:25 Steven Meyer:
Physical Quantum Computers are an Illusion

20:30 Break

21:00 Aggelos Kiayias
Cryptographic Puzzles : The Finalists

21:05 Christian Cachin:
Verifiable Computation with Multiple Clients

21:10 Daniel J. Bernstein:
Cryptographic competitions

21:15 Stefan Kolbl and Florian Mendel and Tomislav Nad and Martin Schlaffer:
Collisions for SHA-3

21:20 Luis Brandao:
The forge-and-lose technique

21:25 Nora Malamidou and Yiannis Tsiounis
The Invasion of the Crypto Gamers!

21:30 Foteini Baldimtsi and Anna Lysyanskaya and Gesine Hinterwalder and Christian T.
Zenger and Wayne P. Burleson and Christof Paar
New results in e-cash

21:35 Orr Dunkelman
Practical Attacks on Reduced-Round Misty1

21:40 Aggelos Kiayias
Cryptographic Puzzles: The Winners