Rump Session Program CHES 2010
Thursday, August 19, 20:15 – 22:00
Chairs: Cetin Koc and Christof Paar

Announcements
Open Positions in Rainy Bochum (1min)
Christof Paar
International Symposium on Electromagnetic Compatibility 2011 (2min)
Yu-ichi HAYASHI
Why CHES is better than CRYPTO (except the Rump Session) (2min)
Tanja Lange

Cryptanalysis
Characteristics of PRINTcipher's sbox (5min)
Peter Schmidt-Nielsen
Postquantum Algorithms with Unexpected Lengths (PAUL) (5min)
Yvo Desmedt and Jean-Jacques Quisquater
Real world AES key extraction (5min)
Sergei Skorobogatov
ECDLP (7min)
Dan Berstein and Tanja Lange
Fine-Grained Processors for Cryptanalysis (4min)
Tim Güneysu and Christof Paar
Live and Let Die (1min)
Axel Poschmann
Length Extension Attack on Narrow Pipe SHA-3 Candidates (4min)
Danilo Gligoroski

Implementations and Algorithms
Continual Random Number Generation (4min)
Leonard Rarick
How to boost the hardware performance of your SHA-3 candidate (3min)
Stefan Tillich
BMW256 and BMW512 on Virtex 5 (2min)
Mohamed Aly
Faster Exponentiation Using a 2-register Addition Chain (4min)
Bruce Murray

Side-Channel and Fault Attacks
DPA contest v2: debriefing and perspectives (5min)
Guillaume DUC, Sylvain GUILLEY, Laurent SAUVAGE, Florent FLAMENT and Jean-Luc DANGER
Hiding Faulty Output is not enough (4min)
Yang Li, Kazuo Sakiyama, Kazuo Ohta
The New SASEBO Family (3min)
Akashi Satoh
DPA – What's Now Possible (5min)
Josh Jaffe
Faulting for Fun and Profit (5min)
David Oswald
SCARF (4min)
You Sung Kang and Dooho Choi
Improved Trace-Driven Cache-Collision Attacks against Embedded AES Implementations (4min)
Jean-François Gallai, Ilya Kizhvatov and Michael Tunstall