CHES 2014 Rump Session

Helena Handschuh, Tim Güneysu

Paradise Hotel, Busan, Korea

25.09.2014

Rump Session Program

21:00	Yuichi Hayashi, Naofumi Homma, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, Takafumi Aoki	EM Attack Is Non-Invasive? - Design Methodology and Validity Verification of EM Attack Sensor
21:03	Jakub Breier, Chien-Ning Chen, Wei He, Alexander Herrmann, Marc Stöttinger	Low Cost Laser Fault Target
21:07	Luke Mather	High-performance computing & side-channels
21:10	Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Peter Schwabe	DH speed news
21:13	Guillaume Duc, Jean-Luc Danger, Sylvain Guilley, Zakaria Najm	DPA contests: from V4 to V4.2!
21:17	Akashi Satoh	Special SAKURA gift
21:20	Jake Longo	Sharing Data
21:22	Adam Ding	A database for side-channel attacks: TeSCASE - Testbed for Side-channel Analysis and Security Evaluation
21:26	Léo Ducas	Accelerating Bliss: the geometry of random binary polynomials
21:29	Gilles Barthe, Sonia Belaid, François Dupressoir, Benjamin Grégoire, Pierre-Alain Fouque, Pierre-Yves Strub	Automatic proofs of correctness and security for masked programs
21:33	Daniel J. Bernstein, Tanja Lange	EM key extraction from constant-time software on fast ARMs
21:37	Randy Bush, Joachim Strömbergson	The Cryptech HSM - An Open, Testable HSM that You can trust
21:41	Stefan Mangard, Axel Poschmann, Jean-Pierre Seifert	COSADE 2015 conference announcement
21:43	Nele Mentens, Lejla Batina	Summer school on real-world crypto and privacy
21:46	Emmanuel Prouff, Guénaël Renault and Matthieu Rivain	CHES 2015 announcement