Workshop on Cryptographic Hardware and Embedded Systems 2010 (CHES 2010)

Santa Barbara, California, USA
Tuesday August 17th - Friday August 20th, 2010

Program

Tuesday, August 17

Time	Event
18:00 - 20:00	**Registration** University Center Corwin Pavilion Lobby
18:00 - 23:00	**Joint Rump Session with Crypto** University Center Lagoon Plaza & Corwin Pavilion (A full dinner menu will be served with the Rump Session) Possible submission at **http://rump2010.cr.yp.to/submission.html**

Wednesday, August 18

Time	Event		
	Session	**Authors**	**Title**
	Registration		
07:30 - 08:45	**Breakfast**		
08:45 - 09:00	**Opening Remarks** University Center Corwin Pavilion		
09:00 - 10:15	**Session 1: Low Cost Cryptography** **Chair: Anne Canteaut** University Center Corwin Pavilion	**Jean-Philippe Aumasson and Luca Henzen and Willi Meier and Maria Naya-Plasencia**	**Quark: a lightweight hash**
		Lars Knudsen and Gregor Leander and Axel Poschmann and Matthew J.B. Robshaw	**PRINTcipher: A Block Cipher for IC-Printing**
		Guido Bertoni and Joan Daemen and Michaël Peeters and Gilles Van Assche	**Sponge-based pseudo-random number generators**
10:15 - 10:45	**Morning Break** University Center Lagoon Plaza		
10:45 - 12:00	**Session 2: Efficient Implementations I** **Chair: Tanja Lange** University Center Corwin Pavilion	**Nicolas Guillermin**	**A high speed coprocessor for elliptic curve scalar multiplications over Fp**
		Raveen R. Goundar and Marc Joye and Atsuko Miyaji	**Co-Z Addition Formulae and Binary Ladders on Elliptic Curves**
		Patrick Longa and Catherine Gebotys	**Efficient Techniques for High-Speed Elliptic Curve Cryptography**
12:00 - 14:00	**Lunch** Storke Plaza		
14:00 - 15:40	**Session 3: Side-Channel Attacks & Countermeasures I** **Chair: Emmanuel Prouff** University Center Corwin Pavilion	**Jean-Sebastien Coron and Ilya Kizhvatov**	**Analysis and Improvement of the Random Delay Countermeasure of CHES 2009**
		Onur Aciicmez and Billy Bob Brumley and Philipp Grabher	**New Results on Instruction Cache Attacks**
		Amir Moradi and Oliver Mischke and Thomas Eisenbarth	**Correlation-Enhanced Power Analysis Collision Attack**
		Olivier Benoît and Thomas Peyrin	**Side-channel Analysis of Six SHA-3 Candidates**
15:40 - 16:10	**Crypto/CHES Joint Afternoon Break** Outside Campbell Hall		
16:10 - 17:10	**Invited Talk I: (joint session with Crypto)** **Chair: Bart Preneel** Campbell Hall	**Ivan Damgård (Aarhus University) and David Naccache**	**Is Theoretical Cryptography Any Good in Practice?**
17:15 - 18:00	**IACR Membership Meeting** Campbell Hall		

18:00 - 20:15	Beach Barbecue (joint with Crypto) Goleta Beach
20:00 - 22:30	Crypto Café (joint with Crypto) Anacapa Formal Lounge

Thursday, August 19

Time	Event		
	Session	Authors	Title
	Registration		
07:30 - 08:45	Breakfast		
9:00 - 10:15	Session 4: Tamper Resistance & HW Trojans Chair: Ingrid Verbauwhede University Center Corwin Pavilion	Sergei Skorobogatov	Flash Memory 'Bumping' Attacks
		Dongdong Du and Seetharam Narasimhan and Rajat Subhra Chakraborty and Swarup Bhunia	Self-Referencing: A Scalable Side-Channel Approach for Hardware Trojan Detection
		Jérôme Di-Battista and Jean-Christophe Courrège and Bruno Rouzeyre and Lionel Torres and Philippe Perdu	When Failure Analysis Meets Side-Channel Attacks
10:15 - 10:45	Morning Break University Center Lagoon Plaza		
10:45 - 12:00	Session 5: Efficient Implementations II Chair: Kris Gaj University Center Corwin Pavilion	Charles Bouillaguet and Hsieh-Chung Chen and Chen-Mou Cheng and Tony Tung Chou and Ruben Niederhagen and Adi Shamir and Bo-Yin Yang	Fast Exhaustive Search for Polynomial Systems in F_2
		Axel Poschmann and Huaxiong Wang and San Ling	256 bit Standardized Crypto for 650 GE - GOST Revisited
		Yasuyuki Nogami and Kenta Nekado and Tetsumi Toyota and Naoto Hongo and Yoshitaka Morikawa	Mixed Bases for Efficient Inversion in F_{((2^2)^2)^2} and Conversion Matrices of SubBytes of AES
12:00 - 14:00	Lunch Storke Plaza		
14:00 - 15:40	Session 6: SHA 3 Chair: Akashi Satoh University Center Corwin Pavilion	Luca Henzen and Pietro Gendotti and Patrice Guillet and Enrico Pargaetzi and Martin Zoller and Frank K. Gürkaynak	Developing a Hardware Evaluation Method for SHA-3 Candidates
		Kris Gaj, Ekawat Homsirikamol, Marcin Rogawski	Fair and Comprehensive Methodology for Comparing Hardware Performance of Fourteen Round Two SHA-3 Candidates using FPGAs
		Joppe W. Bos and Deian Stefan	Performance Analysis of the SHA-3 Candidates on Exotic Multi-Core Architectures
		Christian Wenzel-Benner and Jens Graef	XBX: eXternal Benchmarking eXtension for the SUPERCOP crypto benchmarking framework
15:40 - 16:10	Afternoon Break University Center Lagoon Plaza		
16:10 - 17:00	Session 7: Fault Attacks & Countermeasures Chair: Marc Joye University Center Corwin Pavilion	Alexandre Berzati and Cécile Canovas-Dumas and Louis Goubin	Public Key Perturbation of Randomized RSA Implementations
		Yang Li and Kazuo Sakiyama and Shigeto Gomisawa and Toshinori Fukunaga and Junko Takahashi and Kazuo Ohta	Fault Sensitivity Analysis
17:45 starting	Shuttle Service UCSB - Four Seasons Biltmore Buses Depart in front of Anacapa Residence Hall		
18:15 - 18:45	Reception Four Seasons Biltmore		
18:45 - 20:00	Awards Dinner Four Seasons Biltmore		
20:00 - 22:00	Rump Session Four Seasons Biltmore		

Friday, August 20

Time	Event		
	Session	Authors	Title
	Registration		

07:30 - 08:45	Breakfast		
09:00 - 10:15	**Session 8: PUFs and RNGs** **Chair: Guido Bertoni** University Center Corwin Pavilion	**Maximilian Hofer and Christoph Boehm**	**An Alternative to Error Correction for SRAM-Like PUFs**
		Michal Varchola and Milos Drutarovsky	**New High Entropy Element for FPGA Based True Random Number Generators**
		Daisuke Suzuki and Koichi Shimizu	**The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes**
10:15 - 10:45	**Morning Break** University Center Lagoon Plaza		
10:45 - 11:45	**Invited Talk II** **Chair: François-Xavier Standaert** University Center Corwin Pavilion	**Hovav Shacham (University of California San Diego)**	**Cars and Voting Machines: Embedded Systems in the Field**
11:45 - 13:30	**Lunch** Storke Plaza		
13:30 - 14:20	**Session 9: New Designs** **Chair: Lejla Batina** University Center Corwin Pavilion	**Kimmo Järvinen and Vladimir Kolesnikov and Ahmad-Reza Sadeghi and Thomas Schneider**	**Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs**
		Stéphane Badel and Nilay Dağtekin and Jorge Nakahara Jr and Khaled Ouafi and Nicolas Reffé and Pouyan Sepehrdad and Petr Sušil and Serge Vaudenay	**ARMADILLO: a Multi-Purpose Cryptographic Primitive Dedicated to Hardware**
14:20 - 14:50	**Afternoon Break** University Center Lagoon Plaza		
14:50 - 16:05	**Session 10: Side-Channel Attacks & Countermeasures II** **Chair: Wieland Fischer** University Center Corwin Pavilion	**Matthieu Rivain and Emmanuel Prouff**	**Provably Secure Higher-Order Masking of AES**
		Yossef Oren and Mario Kirschbaum and Thomas Popp and Avishai Wool	**Algebraic Side-Channel Analysis in the Presence of Errors**
		Michael Tunstall and Marc Joye	**Coordinate Blinding over Large Prime Fields**
16:05 - 16:15	**Concluding Remarks** University Center Corwin Pavilion		

Financial Support

DPA Cryptography Research DPA Countermeasure Licensing Program CRYPTOGRAPHY RESEARCH

Riscure

technicolor

Oberthur Technologies

SASEBO RCIS Research Center for Information Security

TELECOM ParisTech