

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Christophe Clavier Kris Gaj (Eds.)

Cryptographic Hardware and Embedded Systems – CHES 2009

11th International Workshop
Lausanne, Switzerland, September 6-9, 2009
Proceedings

Volume Editors

Christophe Clavier
Université de Limoges
Département de Mathématiques et d'Informatique
83 rue d'Isle, 87000 Limoges, France
E-mail: christophe.clavier@unilim.fr
and
Institut d'Ingénierie Informatique de Limoges (3iL)
42 rue Sainte Anne, 87000 Limoges, France
E-mail: christophe.clavier@3il.fr

Kris Gaj
George Mason University
Department of Electrical and Computer Engineering
Fairfax, VA 22030, USA
E-mail: kgaj@gmu.edu

Library of Congress Control Number: 2009933191

CR Subject Classification (1998): E.3, D.4.6, K.6.5, E.4, C.2, H.2.7

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-04137-X Springer Berlin Heidelberg New York
ISBN-13	978-3-642-04137-2 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© International Association for Cryptologic Research 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12753017 06/3180 5 4 3 2 1 0

Preface

CHES 2009, the 11th workshop on Cryptographic Hardware and Embedded Systems, was held in Lausanne, Switzerland, September 6–9, 2009. The workshop was sponsored by the International Association for Cryptologic Research (IACR).

The workshop attracted a record number of 148 submissions from 29 countries, of which the Program Committee selected 29 for publication in the workshop proceedings, resulting in an acceptance rate of 19.6%, the lowest in the history of CHES. The review process followed strict standards: each paper received at least four reviews, and some as many as eight reviews. Members of the Program Committee were restricted to co-authoring at most two submissions, and their papers were evaluated by an extended number of reviewers.

The Program Committee included 53 members representing 20 countries and five continents. These members were carefully selected to represent academia, industry, and government, as well as to include world-class experts in various research fields of interest to CHES. The Program Committee was supported by 148 external reviewers. The total number of people contributing to the review process, including Program Committee members, external reviewers, and Program Co-chairs, exceeded 200.

The papers collected in this volume represent cutting-edge worldwide research in the rapidly growing and evolving area of cryptographic engineering. The submissions were sought in several general areas, including, but not limited to, cryptographic hardware, cryptographic software, attacks against implementations and countermeasures against these attacks, tools and methodologies of cryptographic engineering, and applications and implementation environments of cryptographic systems. Ten years after its first workshop, CHES is now very firmly established as the premier international forum for presenting scientific and technological advances in cryptographic engineering research, the event that bridges the gap between theoretical advances and their practical application in commercial products.

In order to further extend the scope of CHES, this year's CHES included for the first time a special Hot Topic Session. The goal of this session was to attract new authors and attendees to CHES by highlighting a new area, not represented at CHES before, but of potential interest to CHES participants. The topic of this year's Hot Topic Session was: Hardware Trojans and Trusted ICs. The session was chaired by Anand Raghunathan from Purdue University, USA, who prepared a separate call for papers, and oversaw an evaluation of papers submitted to this session. This evaluation was supported by a special Hot Topic Session Committee, composed of six experts in the field of trusted integrated circuit manufacturing. The session included two regular presentations, and an

invited talk, entitled “The State-of-the-Art in IC Reverse Engineering,” delivered by Randy Torrance from Chipworks, Inc., Canada.

Additionally, the workshop included two other excellent invited talks. Christof Paar from Ruhr-Universität Bochum, one of the two founders of CHES, discussed his vision of cryptographic engineering, and its evolution over years, in a talk entitled “Crypto Engineering: Some History and Some Case Studies.” Srinivas Devasadas, MIT, an inventor of PUF (Physical Unclonable Function), and a founder of a company that develops practical products based on this new technology, described his experiences in a talk entitled “Physical Unclonable Functions and Secure Processors.”

The workshop also included two special sessions. Elisabeth Oswald chaired a session on the DPA contest, which included an introduction and discussion of the contest by one of the primary contest organizers, Sylvain Guilley from Telecom ParisTech. Following the introduction was a short presentation by the winners of the contest and a panel discussion devoted to the current and future rules of the contest and the ethical issues associated with inadvertently facilitating through the contest practical attacks against implementations of cryptography. The second special session, chaired by Patrick Schaumont from Virginia Tech, was on benchmarking of cryptographic hardware. The session included several interesting short talks on problems and solutions related to fair and comprehensive evaluation of the performance of cryptographic hardware. This session was of particular significance in light of the ongoing evaluation of the SHA-3 candidates competing to become a new American, and a de-facto worldwide, hash function standard. Additionally, the workshop included two traditional events: a rump session, chaired by Guido Bertoni from STMicroelectronics, Italy, and a poster session chaired by Stefan Mangard, Infineon Technologies, Germany. Our great thanks go to all Special Session Chairs for their initiative, enthusiasm, commitment, innovative spirit, and attention to every detail of their respective sessions.

Through a nomination process and a vote, the Program Committee awarded three CHES 2009 Best Paper Awards. The selected papers represent three distinct areas of cryptographic engineering research: efficient hardware implementations of public key cryptography, efficient and secure software implementations of secret key cryptography, and side-channel attacks and countermeasures. The winners of the three equivalent awards were: Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto, and Francisco Rodríguez-Henríquez for their paper “Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers,” Emilia Käsper and Peter Schwabe for their paper “Faster and Timing-Attack Resistant AES-GCM,” and Thomas Finke, Max Gebhardt, and Werner Schindler for their paper “A New Side-Channel Attack on RSA Prime Generation.”

The selection of 29 best papers out of 148 predominantly very strong submissions was a very challenging and difficult task. The Program Committee members dedicated a very significant amount of time and effort in order to comprehensively and fairly evaluate all submitted papers and provide useful feedback to

the authors. Our deepest thanks go to the members of the Program Committee for their hard work, expertise, dedication, professionalism, fairness, and team spirit.

We deeply thank Marcelo Kaihara, the General Chair of CHES 2009, for his excellent and always timely work on managing the local organization and orchestrating conference logistics. Only because of his tireless effort, flexibility, and team spirit were we able to fit so many additional events and special sessions in the program of this year's CHES. We would like to also thank EPFL for providing an excellent venue for holding the workshop, and for assisting with many local arrangements. Our gratitude also goes to the generous sponsors of CHES 2009, namely, Cryptography Research, Inc., Nagravision Kudelski Group, Oberthur Technologies, RCIS AIST Japan, Riscure, and Telecom ParisTech.

We are also very grateful to Çetin Kaya Koç for managing conference announcements and advertising as the Publicity Chair, and to Jens-Peter Kaps for diligently maintaining the CHES website. The review and discussion process was run using an excellent Web Submission and Review System developed and maintained by Shai Halevi, who was always very quick and precise in addressing our questions and concerns regarding the operation of the system.

We would like to deeply thank the Steering Committee of CHES, for their trust, constant support, guidance, and kind advice on many occasions. Special thanks go to Jean-Jacques Quisquater and Colin Walter, who were always first to respond to our questions and concerns, and often volunteered the advice and support needed to resolve a wide array of challenging issues associated with the fair, firm, and transparent management of the evaluation process.

Finally, we would like to profoundly thank and salute all the authors from all over the world who submitted their papers to this workshop, and entrusted us with a fair and objective evaluation of their work. We appreciate your creativity, hard work, and commitment to push forward the frontiers of science. All your submissions, no matter whether accepted or rejected at this year's CHES, represent the vibrant field of research that CHES is proud to exemplify.

September 2009

Christophe Clavier
Kris Gaj

CHES 2009

Workshop on Cryptographic Hardware and Embedded Systems
Lausanne, Switzerland, September 6–9, 2009

Sponsored by *International Association for Cryptologic Research*

General Chair

Marcelo Kaihara EPFL, Switzerland

Program Co-chairs

Christophe Clavier Université de Limoges, France
Kris Gaj George Mason University, USA

Publicity Chair

Çetin Kaya Koç University of California Santa Barbara, USA

Program Committee

Lejla Batina	Katholieke Universiteit Leuven, Belgium
Daniel J. Bernstein	University of Illinois at Chicago, USA
Guido Bertoni	STMicroelectronics, Italy
Jean-Luc Beuchat	University of Tsukuba, Japan
Luca Breveglieri	Politecnico di Milano, Italy
Ernie Brickell	Intel, USA
Dipanwita Roy Chowdhury	Indian Institute of Technology, Kharagpur, India
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Joan Daemen	STMicroelectronics, Belgium
Ricardo Dahab	University of Campinas, Brazil
Markus Dichtl	Siemens AG, Germany
Benoît Feix	Inside Contactless, France
Viktor Fischer	Université de Saint-Étienne, France
Pierre-Alain Fouque	ENS, France
Catherine H. Gebotys	University of Waterloo, Canada
Christophe Giraud	Oberthur Technologies, France

Louis Goubin	Université de Versailles, France
Jorge Guajardo	Philips Research Europe, The Netherlands
Frank K. Gürkaynak	ETH Zurich, Switzerland
Peter Gutmann	University of Auckland, New Zealand
Helena Handschuh	Katholieke Universiteit Leuven, Belgium
Naofumi Homma	Tohoku University, Japan
Josh Jaffe	Cryptography Research, USA
Marc Joye	Thomson R&D, France
Jens-Peter Kaps	George Mason University, USA
Howon Kim	Pusan National University, South Korea
Çetin Kaya Koç	University of California Santa Barbara, USA
Markus Kuhn	University of Cambridge, UK
Soonhak Kwon	Sungkyunkwan University, South Korea
Kerstin Lemke-Rust	University of Applied Sciences Bonn-Rhein-Sieg, Germany
Marco Macchetti	Nagracard SA, Switzerland
Stefan Mangard	Infineon Technologies, Germany
Liam Marnane	University College Cork, Ireland
Mitsuru Matsui	Mitsubishi Electric, Japan
David Naccache	ENS, France
Dag Arne Osvik	EPFL, Switzerland
Elisabeth Oswald	University of Bristol, UK
Christof Paar	Ruhr-Universität Bochum, Germany
Dan Page	University of Bristol, UK
Pascal Paillier	Gemalto, France
Jean-Jacques Quisquater	Université catholique de Louvain, Belgium
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Pankaj Rohatgi	IBM T.J. Watson Research Center, USA
Erkay Savas	Sabanci University, Turkey
Patrick Schaumont	Virginia Tech, USA
Rainer Steinwandt	Florida Atlantic University, USA
Berk Sunar	Worcester Polytechnic Institute, USA
Elena Trichina	STMicroelectronics, France
Colin Walter	Royal Holloway, UK
Michael J. Wiener	Cryptographic Clarity, Canada
Johannes Wolkerstorfer	IAIK TU Graz, Austria
Sung-Ming Yen	National Central University, Taiwan

Program Committee Advisory Member

François-Xavier Standaert	Université catholique de Louvain, Belgium
---------------------------	---

Hot Topic Session Committee

Anand Raghunathan
(Chair)

Purdue University, USA

Farinaz Koushanfar

Rice University, USA

Jim Plusquellic

University of New Mexico, USA

Pankaj Rohatgi

IBM T.J. Watson Research Center, USA

Patrick Schaumont

Virginia Tech, USA

Berk Sunar

Worcester Polytechnic Institute, USA

External Reviewers

Onur Aciicmez

Guerric Meurice

Markus Kasper

Guido Costa Souza

de Dormale

Chang Hoon Kim

de Araújo

Emmanuelle Dottax

Chong Hee Kim

Kubilay Atasul

Saar Drimer

Minkyu Kim

Alain Aubert

Milos Drutarovsky

Mario Kirschbaum

Maxime Augier

Sylvain Duquesne

Ilya Kizhvatov

Jean-Claude Bajard

Thomas Eisenbarth

Thorsten Kleinjung

Brian Baldwin

Nicolas Estibals

Heiko Knospe

Alessandro Barenghi

Martin Feldhofer

Sandeep S. Kumar

Florent Bernard

Wieland Fischer

Yun-Ki Kwon

Alex Biryukov

Georges Gagnerot

Tanja Lange

Andrey Bogdanov

Berndt Gammel

Cédric Lauradoux

Simone Borri

Pierrick Gaudry

Hee Jung Lee

Joppe Bos

Willi Geiselmann

Arjen K. Lenstra

Arnaud Boscher

Benedikt Gierlichs

Gaëtan Leurent

Lilian Bossuet

Guy Gogniat

Yann L'Hyver

Nicolas Brisebarre

Michael Gora

Wei-Chih Lien

Marco Bucci

Aline Gouget

Feng-Hao Liu

Philippe Bulens

Johann Großschädl

Pierre Loidreau

Anne Canteaut

Sylvain Guillet

Raimondo Luzzi

Nathalie Casati

Eric Xu Guo

François Mace

Mathieu Chartier

Ghaith Hammouri

Abhranil Maiti

Sanjit Chatterjee

Dong-Guk Han

Theo Markettos

Chien-Ning Chen

Neil Hanley

Marcel Medwed

Zhimin Chen

Guillaume Hanrot

Filippo Melzani

Ray Cheung

Christoph Herbst

Nele Mentens

Fred Chong

Clemens Heuberger

Giacomo de Meulenaer

Baudoin Collard

Michael Hutter

Bernd Meyer

René Cumpulido

Laurent Imbert

Atsushi Miyamoto

Jean-Luc Danger

Seyyd Hasan Mir Jalili

Amir Moradi

Pascal Delaunay

Pascal Junod

Csaba Andras Moritz

Elke De Mulder

Marcelo Kaihara

Sergey Morozov

Jérémie Detrey

Deniz Karakoyunlu

Andrew Moss

Debdeep Mukhopadhyay	Mylène Roussellet	Kris Tiri
David Oswald	Christian Rust	Arnaud Tisserand
Siddika Berna Ors Yalcin	Akashi Satoh	Lionel Torres
Young-Ho Park	Werner Schindler	Michael Tunstall
Hervé Pelletier	Jörn-Marc Schmidt	Jonny Valamehr
Gerardo Pelosi	Michael Scott	Gilles Van Assche
Christophe Petit	Christian Schwarz	Jérôme Vasseur
Gilles Piret	Hermann Seuschek	Ihor Vasytsov
Thomas Plos	Chang Shu	Vincent Verneuil
Thomas Popp	Hervé Sibert	Nicolas Veyrat-
Axel Poschmann	Sergei Skorobogatov	Charvillon
Bart Preneel	Takeshi Sugawara	Karine Villegas
Emmanuel Prouff	Ruggero Susella	Hassan Wassel
Carine Raynaud	Daisuke Suzuki	Christopher Wolf
Francesco Regazzoni	Yannick Tegli	Tugrul Yanik
Mathieu Renauld	Nicolas Thériault	Yu Yu
Matthieu Rivain	Hugues Thiebauld	
Bruno Robisson	Stefan Tillich	

Table of Contents

Software Implementations

Faster and Timing-Attack Resistant AES-GCM	1
<i>Emilia Käsper and Peter Schwabe</i>	
Accelerating AES with Vector Permute Instructions	18
<i>Mike Hamburg</i>	
SSE Implementation of Multivariate PKCs on Modern x86 CPUs	33
<i>Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, and Bo-Yin Yang</i>	
MicroEliece: McEliece for Embedded Devices	49
<i>Thomas Eisenbarth, Tim Güneysu, Stefan Heyse, and Christof Paar</i>	

Invited Talk 1

Physical Unclonable Functions and Secure Processors	65
<i>Srini Devadas</i>	

Side Channel Analysis of Secret Key Cryptosystems

Practical Electromagnetic Template Attack on HMAC	66
<i>Pierre-Alain Fouque, Gaëtan Leurent, Denis Réal, and Frédéric Valette</i>	
First-Order Side-Channel Attacks on the Permutation Tables Countermeasure	81
<i>Emmanuel Prouff and Robert McEvoy</i>	
Algebraic Side-Channel Attacks on the AES: Why Time also Matters in DPA	97
<i>Mathieu Renaud, François-Xavier Standaert, and Nicolas Veyrat-Charvillon</i>	
Differential Cluster Analysis	112
<i>Lejla Batina, Benedikt Gierlichs, and Kerstin Lemke-Rust</i>	

Side Channel Analysis of Public Key Cryptosystems

Known-Plaintext-Only Attack on RSA-CRT with Montgomery Multiplication	128
<i>Martin Hlaváč</i>	

A New Side-Channel Attack on RSA Prime Generation	141
<i>Thomas Finke, Max Gebhardt, and Werner Schindler</i>	

Side Channel and Fault Analysis Countermeasures

An Efficient Method for Random Delay Generation in Embedded Software	156
<i>Jean-Sébastien Coron and Ilya Kizhvatov</i>	
Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers	171
<i>Matthieu Rivain, Emmanuel Prouff, and Julien Doget</i>	
A Design Methodology for a DPA-Resistant Cryptographic LSI with RSL Techniques	189
<i>Minoru Saeki, Daisuke Suzuki, Koichi Shimizu, and Akashi Satoh</i>	
A Design Flow and Evaluation Framework for DPA-Resistant Instruction Set Extensions	205
<i>Francesco Regazzoni, Alessandro Cevrero, François-Xavier Standaert, Stephane Badel, Theo Kluter, Philip Brisk, Yusuf Leblebici, and Paolo Ienne</i>	

Invited Talk 2

Crypto Engineering: Some History and Some Case Studies (Extended Abstract)	220
<i>Christof Paar</i>	

Pairing-Based Cryptography

Hardware Accelerator for the Tate Pairing in Characteristic Three Based on Karatsuba-Ofman Multipliers	225
<i>Jean-Luc Beuchat, Jérémie Detrey, Nicolas Estibals, Eiji Okamoto, and Francisco Rodríguez-Henríquez</i>	
Faster $\mathbb{F}_p$ -Arithmetic for Cryptographic Pairings on Barreto-Naehrig Curves	240
<i>Junfeng Fan, Frederik Vercauteren, and Ingrid Verbauwhede</i>	
Designing an ASIP for Cryptographic Pairings over Barreto-Naehrig Curves	254
<i>David Kammler, Diandian Zhang, Peter Schwabe, Hanno Scharwaechter, Markus Langenberg, Dominik Auras, Gerd Ascheid, and Rudolf Mathar</i>	

New Ciphers and Efficient Implementations

KATAN and KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers	272
<i>Christophe De Cannière, Orr Dunkelman, and Miroslav Knežević</i>	
Programmable and Parallel ECC Coprocessor Architecture: Tradeoffs between Area, Speed and Security	289
<i>Xu Guo, Junfeng Fan, Patrick Schaumont, and Ingrid Verbauwhede</i>	
Elliptic Curve Scalar Multiplication Combining Yao's Algorithm and Double Bases	304
<i>Nicolas Méloni and M. Anwar Hasan</i>	

TRNGs and Device Identification

The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators	317
<i>A. Theodore Markettos and Simon W. Moore</i>	
Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs	332
<i>Roel Maes, Pim Tuyls, and Ingrid Verbauwhede</i>	
CDs Have Fingerprints Too	348
<i>Ghaith Hammouri, Aykutlu Dana, and Berk Sunar</i>	

Invited Talk 3

The State-of-the-Art in IC Reverse Engineering	363
<i>Randy Torrance and Dick James</i>	

Hot Topic Session: Hardware Trojans and Trusted ICs

Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering	382
<i>Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson</i>	
MERO: A Statistical Approach for Hardware Trojan Detection	396
<i>Rajat Subhra Chakraborty, Francis Wolff, Somnath Paul, Christos Papachristou, and Swarup Bhunia</i>	

Theoretical Aspects

On Tamper-Resistance from a Theoretical Viewpoint: The Power of Seals	411
<i>Paulo Mateus and Serge Vaudenay</i>	

Mutual Information Analysis: How, When and Why?	429
<i>Nicolas Veyrat-Charvillon and François-Xavier Standaert</i>	

Fault Analysis

Fault Attacks on RSA Signatures with Partially Unknown Messages	444
<i>Jean-Sébastien Coron, Antoine Joux, Ilya Kizhvatov,</i> <i>David Naccache, and Pascal Paillier</i>	
Differential Fault Analysis on DES Middle Rounds	457
<i>Matthieu Rivain</i>	

Author Index	471
-------------------------------	-----