

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

Massachusetts Institute of Technology, 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

Elisabeth Oswald Pankaj Rohatgi (Eds.)

Cryptographic Hardware and Embedded Systems – CHES 2008

10th International Workshop
Washington, D.C., USA, August 10-13, 2008
Proceedings

Volume Editors

Elisabeth Oswald
University of Bristol
Department of Computer Science
Merchant Venturers Building, Woodland Road, BS8 1UB, Bristol, UK
E-mail: elisabeth.oswald@bristol.ac.uk

Pankaj Rohatgi
IBM T.J. Watson Research Center
19 Skyline Drive, Hawthorne, NY 10532, USA
E-mail: rohatgi@us.ibm.com

Library of Congress Control Number: 2008931306

CR Subject Classification (1998): E.3, E.4, D.4.6, C.2.0, I.3.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-540-85052-X Springer Berlin Heidelberg New York
ISBN-13	978-3-540-85052-6 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 is a part of Springer Science+Business Media
springer.com

© International Association for Cryptologic Research 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12441693 06/3180 5 4 3 2 1 0

Preface

These are the proceedings of the 10th Workshop on Cryptographic Hardware and Embedded Systems (CHES), held in Washington D.C., USA, August 10–13, 2008. This workshop was sponsored by the International Association for Cryptologic Research (IACR).

The CHES 2008 workshop attracted 107 submissions from 23 countries, of which the program committee selected 27 papers for publication. The review process followed strict standards: each paper received at least four reviews; members of the program committee were restricted to submitting at most two papers. The 42 Program Committee members from 13 countries were selected carefully to ensure that different fields, such as hardware and software implementations, active and passive implementation attacks, cryptanalysis and cryptography including random number generation, embedded systems, and trusted computing, were well represented and a balance between academia and industry was achieved. Counting all Program Committee members, external reviewers, and the Program Co-chairs, we had 158 people contributing to the review process. We would like to thank all Program Committee members and external reviewers for their contribution to the review process.

In just 10 years, the CHES workshop has grown to become the flagship event in its area, attracting high-profile papers and attendees from academia and industry. This excellence is reflected in the quality of the contributed papers and invited talks. In cooperation with the CHES Steering Committee, the Program Committee awarded the CHES 2008 Best Paper Award to two contributions: “Attack and Improvement of a Secure S-box Calculation Based on the Fourier Transform” by Jean-Sébastien Coron, Christophe Giraud, Emmanuel Prouff and Matthieu Rivain, and “Time-Area Optimized Public-Key Engines: MQ-Cryptosystems as Replacement for Elliptic Curves?” by Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp and Christopher Wolf. The purpose of the award is to formally acknowledge excellence in research. We would like to congratulate the authors of these two papers. In addition to presentations of peer-reviewed papers there were excellent invited presentations. At the time of compiling the proceedings, an invited talk by Adi Shamir on “RSA: Past, Present and Future”, and an invited talk by Ernie Brickell from Intel on “A Vision for Platform Security” had been confirmed.

In order to celebrate the 10th anniversary of CHES, the workshop program included a tour of the National Cryptologic Museum in Fort Mead and a talk by Christof Paar and Çetin Kaya Koç on the history of CHES. In addition there was a rump session and a panel discussion. Special thanks for making these possible and taking care of the local organization go to the General Co-chairs Kris Gaj and Jens-Peter Kaps (both from George Mason University). We are also greatly indebted to the CHES Steering Committee for their guidance

and support throughout the process of putting this program together. The peer review process and the production of these proceedings were greatly facilitated by the IACR Webreview System. Shai Halevi (IBM) receives our sincere gratitude for providing and maintaining this software, and for always being prepared to help.

We would also like to acknowledge and thank our sponsors, many of whom have generously supported the workshop over the years. At the time of writing this preface a number of companies had been confirmed as sponsors: Cryptography Research, Inc., CygnaCom Solutions, escrypt GmbH, IBM Research, Oberthur Technologies, Philips Intrinsic-ID, Research Center of Information Security (RCIS) Japan, and Thomson R&D France.

Finally, we would like to thank all the researchers and authors from all over the world who submitted their work to the CHES 2008 conference and whose efforts create the vibrant field of research that CHES is proud to represent.

August 2008

Elisabeth Oswald
Pankaj Rohatgi

CHES 2008

Workshop on Cryptographic Hardware and Embedded Systems
Washington DC, USA, August 10–13, 2008

Sponsored by the *International Association for Cryptologic Research*

General Co-chairs

Kris Gay, George Mason University
Jens-Peter Kaps, George Mason University

Program Co-chairs

Elisabeth Oswald, University of Bristol
Pankaj Rohatgi, IBM Research

Program Committee

Daniel V. Bailey	RSA Laboratories, USA
Lejla Batina	Katholieke Universiteit Leuven, Belgium
Feng Bao	Institute for Infocomm Research, Singapore
Daniel J. Bernstein	Univ. of Illinois, Chicago, USA
Suresh Chari	IBM Research, USA
Christophe Clavier	Gemalto, France
Jean-Sebastien Coron	University of Luxembourg, Luxembourg
Markus Dichtl	Siemens AG, Germany
Louis Goubin	Université de Versailles, France
Anwar Hasan	Univ. of Waterloo, Canada
Joshua Jaffe	Cryptography Research, USA
Marc Joye	Thomson R&D, France
Çetin Kaya Koç	Oregon State University, USA
Markus Kuhn	University of Cambridge, UK
Klaus Kursawe	Philips Research, Netherlands
Ruby Lee	Princeton University, USA
Kerstin Lemke-Rust	T-Systems, Germany
Arjen Lenstra	EPFL, Switzerland, and Alcatel-Lucent Bell Laboratories, USA
Stefan Mangard	Infineon Technologies, Germany
Mitsuru Matsui	Mitsubishi Electric, Japan
Máaire McLoone	Queens University Belfast, UK

David Naccache	ENS, France
Katsuyuki Okeya	Hitachi, Japan
Christof Paar	Ruhr-Universität Bochum, Germany
Dan Page	Univ. of Bristol, UK
Pascal Paillier	Gemalto, France
Emmanuel Prouff	Oberthur Card Systems, France
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Anand Raghunathan	NEC labs, USA
Josyula R. Rao	IBM Research, USA
Ahmad-Reza Sadeghi	Ruhr-Universität Bochum, Germany
Akashi Satoh	AIST, Japan
Erkay Savas	Sabanci University, Turkey
Patrick Schaumont	Virginia Tech, USA
Jean-Pierre Seifert	Samsung R&D, USA
Berk Sunar	Worcester Polytechnic Institute, USA
Masahiko Takenaka	Fujitsu Laboratories Ltd, Japan
Kris Tiri	Intel, USA
Elena Trichina	Spansion, France
Ingrid Verbauwhede	Katholieke Universiteit Leuven, Belgium
Colin Walter	Comodo CA, UK
Johannes Wolkerstorfer	TU Graz, Austria

External Reviewers

Onur Aciçmez	Thomas Eisenbarth	Kouichi Itoh
Manfred Aigner	Takashi Endo	Tetsuya Izu
Kahraman Akdemir	Benoit Feix	Charanjit Jutla
Toru Akishita	Martin Feldhofer	Marcelo Kaihara
Frédéric Amiel	Berndt M. Gammel	Jens-Peter Kaps
Frederik Armknecht	Sergiu Ghetie	Anton Kargl
Muhammad Asim	Benedikt Gierlichs	Markus Kasper
Guido Bertoni	Kevin Gotze	Timo Kasper
Sumeer Bhola	Aline Gouget	Chong Hee Kim
Alex Biryukov	Rob Granger	Ovunc Kocabas
Andrey Bogdanov	Vanessa Gratzner	Masanobu Koike
Joseph Bonneau	Johann Großschädl	Konrad Kulikowski
Joppe Bos	Jorge Guajardo	Hans Lähr
Arnaud Boscher	Shay Gueron	T. Lan
Marco Bucci	Sylvain Guilley	Tanja Lange
Philippe Bulens	Tim Güneysu	Albert Levi
David Champagne	Xu Guo	Yingxi Lu
Zhimin Chen	Ghaith Hammouri	Raimondo Luzzi
Benoit Chevallier-Mames	Matt Henricksen	François Macé
Emmanuelle Dottax	Christoph Herbst	Sandra Marcello
Saar Drimer	Naofumi Homma	Mark Marson

Nele Mentens	Gilles Piret	Dave Singelee
Giacomo de Meulenaer	Thomas Plos	Boris Skoric
Amir Moradi	Thomas Popp	Martijn Stam
Shiho Moriai	Axel Poschmann	François-Xavier
Andrew Moss	Stefan Pyka	Standaert
Michael Naehrig	Matthieu Rivain	Daisuke Suzuki
Michael Neve	Francisco	Hugues Thiebault
Yasuyuki Nogami	Rodriguez-Henriquez	Elena Trichina
Ersin Oksuzoglu	Minoru Saeki	Toyohiro Tsurumaru
Francis Olivier	Ghazanfar A. Safdar	Michael Tunstall
Ahmet Onur Durahim	Gokay Saldamli	Pim Tuyls
Alina Oprea	Palash Sarkar	Frédéric Valette
Berna Ors	Vincent Scarlata	Frederik Vercauteren
Toru Owada	Dries Schellekens	Camille Vuillaume
Erdinc Ozturk	Werner Schindler	Z. Wang
Pujan Patel	Jörn-Marc Schmdit	Sung-Ming Yen
Fabrice Pautot	Peter Schwabe	Huafei Zhu
Thomas B. Pedersen	Hermann Seuschek	

Table of Contents

Side-Channel Analysis 1

Attack and Improvement of a Secure S-Box Calculation Based on the Fourier Transform.....	1
<i>Jean-Sébastien Coron, Christophe Giraud, Emmanuel Prouff, and Matthieu Rivain</i>	
Collision-Based Power Analysis of Modular Exponentiation Using Chosen-Message Pairs	15
<i>Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, and Adi Shamir</i>	
Multiple-Differential Side-Channel Collision Attacks on AES	30
<i>Andrey Bogdanov</i>	

Implementations 1

Time-Area Optimized Public-Key Engines: MQ -Cryptosystems as Replacement for Elliptic Curves?.....	45
<i>Andrey Bogdanov, Thomas Eisenbarth, Andy Rupp, and Christopher Wolf</i>	
Ultra High Performance ECC over NIST Primes on Commercial FPGAs	62
<i>Tim Güneysu and Christof Paar</i>	
Exploiting the Power of GPUs for Asymmetric Cryptography	79
<i>Robert Szerwinski and Tim Güneysu</i>	

Fault Analysis 1

High-Performance Concurrent Error Detection Scheme for AES Hardware	100
<i>Akashi Satoh, Takeshi Sugawara, Naofumi Homma, and Takafumi Aoki</i>	
A Lightweight Concurrent Fault Detection Scheme for the AES S-Boxes Using Normal Basis	113
<i>Mehran Mozaffari-Kermani and Arash Reyhani-Masoleh</i>	
RSA with CRT: A New Cost-Effective Solution to Thwart Fault Attacks	130
<i>David Vigilant</i>	

Random Number Generation

A Design for a Physical RNG with Robust Entropy Estimators	146
<i>Wolfgang Killmann and Werner Schindler</i>	
Fast Digital TRNG Based on Metastable Ring Oscillator	164
<i>Ihor Vasylytsov, Eduard Hambardzumyan, Young-Sik Kim, and Bohdan Karpinskyy</i>	
Efficient Helper Data Key Extractor on FPGAs	181
<i>Christoph Bösch, Jorge Guajardo, Ahmad-Reza Sadeghi, Jamshid Shokrollahi, and Pim Tuyls</i>	

Side-Channel Analysis 2

The Carry Leakage on the Randomized Exponent Countermeasure	198
<i>Pierre-Alain Fouque, Denis Réal, Frédéric Valette, and Mhamed Drissi</i>	
Recovering Secret Keys from Weak Side Channel Traces of Differing Lengths	214
<i>Colin D. Walter</i>	
Attacking State-of-the-Art Software Countermeasures—A Case Study for AES	228
<i>Stefan Tillich and Christoph Herbst</i>	

Cryptography and Cryptanalysis

Binary Edwards Curves	244
<i>Daniel J. Bernstein, Tanja Lange, and Reza Rezaeian Farashahi</i>	
A Real-World Attack Breaking A5/1 within Hours	266
<i>Timo Gendrullis, Martin Novotný, and Andy Rupp</i>	
Hash Functions and RFID Tags: Mind the Gap	283
<i>Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, Matt J.B. Robshaw, and Yannick Seurin</i>	

Implementations 2

A New Bit-Serial Architecture for Field Multiplication Using Polynomial Bases	300
<i>Arash Reyhani-Masoleh</i>	
A Very Compact Hardware Implementation of the MISTY1 Block Cipher	315
<i>Dai Yamamoto, Jun Yajima, and Kouichi Itoh</i>	

Light-Weight Instruction Set Extensions for Bit-Sliced Cryptography . . .	331
<i>Philipp Grabher, Johann Großschädl, and Dan Page</i>	

Fault Analysis 2

Power and Fault Analysis Resistance in Hardware through Dynamic Reconfiguration	346
<i>Nele Mentens, Benedikt Gierlichs, and Ingrid Verbauwhede</i>	
RFID and Its Vulnerability to Faults	363
<i>Michael Hutter, Jörn-Marc Schmidt, and Thomas Plos</i>	
Perturbating RSA Public Keys: An Improved Attack	380
<i>Alexandre Berzati, Cécile Canovas, and Louis Goubin</i>	

Side-Channel Analysis 3

Divided Backend Duplication Methodology for Balanced Dual Rail Routing	396
<i>Karthik Baddam and Mark Zwolinski</i>	
Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages	411
<i>François-Xavier Standaert and Cedric Archambeau</i>	
Mutual Information Analysis: A Generic Side-Channel Distinguisher	426
<i>Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel</i>	

Invited Talks

RSA—Past, Present, Future	443
<i>Adi Shamir</i>	
A Vision for Platform Security	444
<i>Ernie Brickell</i>	

Author Index	445
------------------------	-----