

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

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

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Pascal Paillier Ingrid Verbauwhede (Eds.)

Cryptographic Hardware and Embedded Systems - CHES 2007

9th International Workshop, Vienna, Austria
September 10-13, 2007
Proceedings

Volume Editors

Pascal Paillier
37 cours de Vincennes
75020 Paris, France
E-mail: pascal.paillier@gemalto.com

Ingrid Verbauwhede
Katholieke Universiteit Leuven, ESAT/COSIC
Kasteelpark Arenberg 10
B-3001 Leuven, Belgium
E-mail: iverbauw@esat.kuleuven.be

Library of Congress Control Number: 2007933579

CR Subject Classification (1998): E.3, C.2, C.3, B.7, G.2.1, D.4.6, K.6.5, F.2.1, J.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-74734-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74734-5 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 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12118106 06/3180 5 4 3 2 1 0

Preface

CHES 2007, the ninth workshop on Cryptographic Hardware and Embedded Systems, was sponsored by the International Association for Cryptologic Research (IACR) and held in Vienna, Austria, September 10–13, 2007. The workshop received 99 submissions from 24 countries, of which the Program Committee (39 members from 15 countries) selected 31 for presentation. For the first time in the history of CHES, each submission was reviewed by at least four reviewers instead of three (and at least five for submissions by PC members, those now being limited to two per member) and many submitted papers have received plenty of extra reviews (some papers received up to nine reviews), thus totalling the unprecedented record of 483 reviews overall.

The papers collected in this volume represent cutting-edge worldwide research in the rapidly evolving fields of crypto-hardware, fault-based and side-channel cryptanalysis, and embedded cryptography, at the crossing of academic and industrial research. The wide diversity of subjects appearing in these proceedings covers virtually all related areas and shows our efforts to extend the scope of CHES more than usual. Although a relatively young workshop, CHES is now firmly established as a scientific event of reference appreciated by more and more renowned experts of theory and practice: many high-quality works were submitted, all of which, sadly, could not be accepted. Selecting from so many good works is no easy task and our deepest thanks go to the members of the Program Committee for their involvement, excellence, and team spirit. We are grateful to the numerous external reviewers listed below for their expertise and assistance in our deliberations.

In addition to the contributions appearing in these proceedings, the workshop program included two invited lectures given by Kim Nguyen and Pankaj Rohatgi. The program also included the traditional rump session, chaired by Nigel Smart, featuring short informal talks on late-breaking research news. This year's rump session was augmented with a parallel demo and poster session welcoming informal presentations of prototypes, attack demos and research works. The Program and Steering Committees commonly agreed on giving the CHES 2007 Best Paper Award to two papers: "Arithmetic Operators for Pairing-Based Cryptography" by Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey and Eiji Okamoto (University of Tsukuba, Université Monnet and École Normale Supérieure de Lyon) and "Side Channel Cryptanalysis of a Higher Order Masking" by Jean-Sébastien Coron, Emmanuel Prouff and Matthieu Rivain (University of Luxembourg and Oberthur Card Systems). The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize excellence in their research works. Interestingly, these two works represent well the two sides of our field: efficient implementations and hardware-based cryptanalysis.

Ingrid and myself deeply thank Elisabeth Oswald (University of Bristol, UK, and Graz University of Technology, Austria), the General Chair of CHES 2007, for her excellent work managing the local organization and orchestrating the conference logistics. We are grateful to Thomas Herlea (KUL, Belgium) for diligently maintaining the Web system. The review and discussion process was run using e-mail and the WebReview software by Wim Moreau and Joris Claessens. We also owe our gratitude to Lejla Batina (also from KUL) for her help in preparing the call for papers and the proceedings. We would like to deeply thank the Steering Committee and personally Jean-Jacques Quisquater (UCL, Belgium) for his support, trust and kind advice at many occasions. We would also like to thank the Institute for Applied Information Processing and Communications (IAIK) of Graz University of Technology for assisting with local arrangements. Our gratitude also goes to our generous sponsors, namely, Cryptography Research, Comodo, Novacard, Thomson, Infineon and IBM. We heartily thank all those who have contributed to make this workshop a reality: we are forever in your debt.

Finally, we would like to profoundly thank and salute all those who, from all over the world, submitted their work to this workshop as well as all the speakers who provided the scientific contents of CHES 2007: the success of the CHES series is their success and reflects every year the vitality of our community.

July 2007

Pascal Paillier
Ingrid Verbauwhede

Organization

Organizational Committee

| | |
|-------------------|--|
| Program Co-chairs | Pascal Paillier (Gemalto, France) Ingrid Verbauwhede (KUL, Belgium) |
| General Chair | Elisabeth Oswald (University of Bristol, UK) and Graz University of Technology, Austria |
| Publicity Chair | Çetin Kaya Koç (Oregon State University, USA) |

Program Committee

| | |
|----------------------|---|
| Lejla Batina | Katholieke Universiteit Leuven, Belgium |
| Guido Bertoni | STMicroelectronics, Italy |
| Christophe Clavier | Gemalto, France |
| Jean-Sébastien Coron | University of Luxembourg, Luxembourg |
| Joan Daemen | STMicroelectronics, Belgium |
| Ricardo Dahab | Universidade Estadual de Campinas, Brazil |
| Pierre-Alain Fouque | ENS, France |
| Kris Gaj | George Mason University, USA |
| Henri Gilbert | Orange Labs, France |
| Jim Goodman | ATI Technologies, Canada |
| Louis Goubin | Université de Versailles, France |
| Louis Granboulan | EADS, France |
| Helena Handschuh | Spansion, France |
| Tetsuya Izu | Fujitsu Laboratories Ltd, Japan |
| Marc Joye | Thomson R&D, France |
| Çetin Kaya Koç | Oregon State University, USA |
| Markus Kuhn | University of Cambridge, UK |
| Pil Joong Lee | Postech, South Korea |
| Stefan Mangard | Infineon Technologies, Germany |
| Tsutomu Matsumoto | Yokohama National University, Japan |
| David Naccache | ENS, France |
| Christof Paar | Ruhr-Universität Bochum, Germany |
| Anand Ragnathan | NEC labs, USA |
| Josyula R. Rao | IBM T.J. Watson Research Center, USA |
| Pankaj Rohatgi | IBM T.J. Watson Research Center, USA |
| Ahmad-Reza Sadeghi | Ruhr-Universität Bochum, Germany |
| Akashi Satoh | IBM, Japan |
| Erkay Savas | Sabanci University, Turkey |
| Patrick Schaumont | Virginia Tech, USA |

| | |
|---------------------|--------------------------------------|
| Kai Schramm | Reneesas, UK |
| Jean-Pierre Seifert | University of Innsbruck, Austria |
| Berk Sunar | Worcester Polytechnic Institute, USA |
| Tsuyoshi Takagi | Future University Hakodate, Japan |
| Alexander Taubin | Boston University, USA |
| Pim Tuyls | Philips Research, Netherlands |
| Kris Tiri | Intel, USA |
| Frédéric Valette | DGA/CELAR, France |
| Serge Vaudenay | EPFL, Switzerland |
| Colin Walter | Comodo CA, UK |

External Referees

| | | |
|-------------------------|-----------------------|------------------------|
| Onur Aciçmez | Sergiu Ghetie | Filippo Melzani |
| Dakshi Agrawal | Benedikt Gierlichs | Bodo Möller |
| Toru Akishita | Damien Giry | José R. M. Monteiro |
| Didier Alquié | Gary Graunke | Shiho Moriai |
| Frédéric Amiel | Johann Groszschaedl | Christophe Mourtel |
| Diego Aranha | Jorge Guajardo | Seiji Munetoh |
| Guido Araujo | Tamer Gudu | Toshiya Nakajima |
| Gildas Avoine | Sylvain Guilley | Michael Neve |
| Thomas Baignères | Tim Güneysu | Katsuyuki Okeya |
| Selcuk Baktir | DongGuk Han | Francis Olivier |
| Johann Barbier | Naofumi Homma | Berna Örs |
| Paulo S. L. M. Barreto | Kouichi Itoh | Dag Arne Osvik |
| Come Berbain | Jens-Peter Kaps | Renaud Pacalet |
| Jean-Luc Beuchat | Mohamed Karroumi | Dan Page |
| Olivier Billet | Timo Kasper | Sylvain Pasini |
| Alex Biryukov | Stefan Katzenbeisser | Thomas B. Pedersen |
| Andrey Bogdanov | Jin Ho Kim | Eric Peeters |
| Arnaud Boscher | Tae Hyun Kim | Gerardo Pelosi |
| Luca Breveglieri | Young Mok Kim | Jan Pelzl |
| Rafael Dantas de Castro | Giray Komurcu | Thomas Peyrin |
| Benoit Chevallier-Mames | Ulrich Kuehn | Raphael C.-W. Phan |
| Christophe De Cannière | Konrad Kulikowski | Gilles Piret |
| Marco De Fazio | Sandeep Kumar | Thomas Popp |
| Hüseyin Demirci | Noboru Kunihiro | Denis Real |
| Augusto Jun Devegili | Eun Jeong Kwon | Francesco Regazzoni |
| Alain Durand | Tanja Lange | Jean-Rene Reinhard |
| Thomas Eisenbarth | Eunjeong Lee | Matthew Robshaw |
| M. Tolga Eren | Kerstin Lemke-Rust | F. Rodríguez-Henríquez |
| Benoit Feix | Gaetan Leurent | Andy Rupp |
| Martin Feldhofer | Albert Levi | Yasuyuki Sakai |
| Wieland Fischer | J. C. López-Hernández | Kazuo Sakiyama |
| Berndt M. Gammel | Theo Markettos | Werner Schindler |

Michael Scott
Jae Woo Seo
Yannick Seurin
Jong Hoon Shin
Masaaki Shirase
Jamshid Shokrollahi
Eric Simpson
Daisuke Suzuki
Boris Škorić

Masahiko Takenaka
Laurent Théry
Stefan Tillich
Elena Trichina
Michael Tunstall
Gilles Van Assche
Ihor Vasylytsov
Fré Vercauteren
David Vigilant

Martin Vuagnoux
Camille Vuillaume
Marcel Winandy
Johannes Wolkerstorfer
Paul Wooderson
Yeon-Hyeong Yang
Sebastien Zimmer
Xinwen Zhang

Table of Contents

Differential and Higher Order Attacks

| | |
|---|----|
| A First-Order DPA Attack Against AES in Counter Mode with Unknown Initial Counter | 1 |
| <i>Josh Jaffe</i> | |
| Gaussian Mixture Models for Higher-Order Side Channel Analysis | 14 |
| <i>Kerstin Lemke-Rust and Christof Paar</i> | |
| Side Channel Cryptanalysis of a Higher Order Masking Scheme | 28 |
| <i>Jean-Sébastien Coron, Emmanuel Prouff, and Matthieu Rivain</i> | |

Random Number Generation and Device Identification

| | |
|--|----|
| High-Speed True Random Number Generation with Logic Gates Only | 45 |
| <i>Markus Dichtl and Jovan Dj. Golić</i> | |
| FPGA Intrinsic PUFs and Their Use for IP Protection | 63 |
| <i>Jorge Guajardo, Sandeep S. Kumar, Geert-Jan Schrijen, and Pim Tuyls</i> | |

Logic Styles: Masking and Routing

| | |
|---|-----|
| Evaluation of the Masked Logic Style MDPL on a Prototype Chip | 81 |
| <i>Thomas Popp, Mario Kirschbaum, Thomas Zefferer, and Stefan Mangard</i> | |
| Masking and Dual-Rail Logic Don't Add Up | 95 |
| <i>Patrick Schaumont and Kris Tiri</i> | |
| DPA-Resistance Without Routing Constraints? | 107 |
| <i>Benedikt Gierlichs</i> | |

Efficient Algorithms for Embedded Processors

| | |
|---|-----|
| On the Power of Bitslice Implementation on Intel Core2 Processor | 121 |
| <i>Mitsuru Matsui and Junko Nakajima</i> | |
| Highly Regular Right-to-Left Algorithms for Scalar Multiplication | 135 |
| <i>Marc Joye</i> | |

MAME: A Compression Function with Reduced Hardware Requirements 148
Hiroataka Yoshida, Dai Watanabe, Katsuyuki Okeya, Jun Kitahara, Hongjun Wu, Özgül Küçük, and Bart Preneel

Collision Attacks and Fault Analysis

Collision Attacks on AES-Based MAC: Alpha-MAC 166
Alex Biryukov, Andrey Bogdanov, Dmitry Khovratovich, and Timo Kasper

Secret External Encodings Do Not Prevent Transient Fault Analysis... 181
Christophe Clavier

Two New Techniques of Side-Channel Cryptanalysis 195
Alex Biryukov and Dmitry Khovratovich

High Speed AES Implementations

AES Encryption Implementation and Analysis on Commodity Graphics Processing Units 209
Owen Harrison and John Waldron

Multi-gigabit GCM-AES Architecture Optimized for FPGAs 227
Stefan Lemsitzer, Johannes Wolkerstorfer, Norbert Felber, and Matthias Braendli

Public-Key Cryptography

Arithmetic Operators for Pairing-Based Cryptography 239
Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, and Eiji Okamoto

FPGA Design of Self-certified Signature Verification on Koblitz Curves 256
Kimmo Järvinen, Juha Forsten, and Jorma Skyttä

How to Maximize the Potential of FPGA Resources for Modular Exponentiation 272
Daisuke Suzuki

Implementation Cost of Countermeasures

TEC-Tree: A Low-Cost, Parallelizable Tree for Efficient Defense Against Memory Replay Attacks 289
Reouwen Elbaz, David Champagne, Ruby B. Lee, Lionel Torres, Gilles Sassatelli, and Pierre Guillemin

| | |
|---|-----|
| Power Analysis Resistant AES Implementation with Instruction Set Extensions | 303 |
| <i>Stefan Tillich and Johann Großschädl</i> | |

Security Issues for RF and RFID

| | |
|---|-----|
| Power and EM Attacks on Passive 13.56 MHz RFID Devices | 320 |
| <i>Michael Hutter, Stefan Mangard, and Martin Feldhofer</i> | |
| RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? | 334 |
| <i>O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert, and J. Reverdy</i> | |
| RF-DNA: Radio-Frequency Certificates of Authenticity | 346 |
| <i>Gerald DeJean and Darko Kirovski</i> | |

Special Purpose Hardware for Cryptanalysis

| | |
|--|-----|
| CAIRN 2: An FPGA Implementation of the Sieving Step in the Number Field Sieve Method | 364 |
| <i>Tetsuya Izu, Jun Kogure, and Takeshi Shimoyama</i> | |
| Collision Search for Elliptic Curve Discrete Logarithm over $GF(2^m)$ with FPGA | 378 |
| <i>Guerric Meurice de Dormale, Philippe Bulens, and Jean-Jacques Quisquater</i> | |
| A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations | 394 |
| <i>Andrey Bogdanov, Thomas Eisenbarth, and Andy Rupp</i> | |

Side Channel Analysis

| | |
|---|-----|
| Differential Behavioral Analysis | 413 |
| <i>Bruno Robisson and Pascal Manet</i> | |
| Information Theoretic Evaluation of Side-Channel Resistant Logic Styles | 427 |
| <i>François Macé, François-Xavier Standaert, and Jean-Jacques Quisquater</i> | |

Problems and Solutions for Lightweight Devices

| | |
|--|-----|
| On the Implementation of a Fast Prime Generation Algorithm | 443 |
| <i>Christophe Clavier and Jean-Sébastien Coron</i> | |

| | |
|---|-----|
| PRESENT: An Ultra-Lightweight Block Cipher | 450 |
| <i>A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Viskkelsoe</i> | |
| Author Index | 467 |