

Lecture Notes in Computer Science

2523

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Burton S. Kaliski Jr. Çetin K. Koç
Christof Paar (Eds.)

Cryptographic Hardware and Embedded Systems – CHES 2002

4th International Workshop
Redwood Shores, CA, USA, August 13-15, 2002
Revised Papers



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Burton S. Kaliski Jr.

RSA Laboratories

174 Middlesex Turnpike, Bedford, MA 01730, USA

E-mail: bkaliski@rsasecurity.com

Çetin K. Koç

Oregon State University

Corvallis, Oregon 97330, USA

E-mail: koc@ece.orst.edu

Christof Paar

Ruhr-Universität Bochum

44780 Bochum, Germany E-mail: cpaar@crypto.rub.de

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress

Bibliographic information published by Die Deutsche Bibliothek

Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data is available in the Internet at [<http://dnb.ddb.de>](http://dnb.ddb.de).

CR Subject Classification (1998): E.3, C.2, C.3, B.7.2, G.2.1, D.4.6, K.6.5, F.2.1, J.2

ISSN 0302-9743

ISBN 3-540-00409-2 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York

a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e. K.

Printed on acid-free paper

SPIN 10873104

06/3142

5 4 3 2 1 0

Preface

These are the proceedings of CHES 2002, the Fourth Workshop on Cryptographic Hardware and Embedded Systems. After the first two CHES Workshops held in Massachusetts, and the third held in Europe, this is the first Workshop on the West Coast of the United States. There was a record number of submissions this year and in response the technical program was extended to 3 days.

As is evident by the papers in these proceedings, there have been again many excellent submissions. Selecting the papers for this year's CHES was not an easy task, and we regret that we could not accept many contributions due to the limited availability of time. There were 101 submissions this year, of which 39 were selected for presentation. We continue to observe a steady increase over previous years: 42 submissions at CHES '99, 51 at CHES 2000, and 66 at CHES 2001. We interpret this as a continuing need for a workshop series that combines theory and practice for integrating strong security features into modern communications and computer applications. In addition to the submitted contributions, Jean-Jacques Quisquater (UCL, Belgium), Sanjay Sarma (MIT, USA) and a panel of experts on hardware random number generation gave invited talks.

As in the previous years, the focus of the Workshop is on all aspects of cryptographic hardware and embedded system security. Of special interest were contributions that describe new methods for efficient hardware implementations and high-speed software for embedded systems, e.g., smart cards, microprocessors, DSPs, etc. CHES also continues to be an important forum for new theoretical and practical findings in the important and growing field of side-channel attacks.

We hope to continue to make the CHES Workshop series a forum for intellectual exchange in creating the secure, reliable, and robust security solutions of tomorrow. CHES Workshops will continue to deal with hardware and software implementations of security functions and systems, including security for embedded wireless ad hoc networks.

We thank everyone whose involvement made the CHES Workshop such a successful event. In particular we would like to thank André Weimerskirch (Ruhr-University, Bochum) for his help again with the website and Gökay Saldamlı and Colin van Dyke (Oregon State University) for their help on registration and local organization.

August 2002

Burton S. Kaliski Jr.
Çetin K. Koç
Christof Paar

Acknowledgements

The organizers express their thanks to the program committee, the external referees for their help in getting the best quality papers selected, and also the companies which provided support to the workshop.

The program committee members for CHES 2002:

- Beni Arazi, arazi@ee.bgu.ac.il
Ben Gurion University, Israel
- Jean-Sébastien Coron, coron@clipper.ens.fr
Gemplus Card International, France
- Kris Gaj, kgaj@gmu.edu
George Mason University, USA
- Craig Gentry, cgentry@docomolabs-usa.com
DoCoMo Communications Laboratories, USA
- Jim Goodman, jing@engim.com
Engim Canada, Canada
- M. Anwar Hasan, ahasan@ece.uwaterloo.ca
University of Waterloo, Canada
- David Jablon, dpj@theworld.com
Phoenix Technologies, USA
- Peter Kornerup, kornerup@imada.sdu.dk
University of Southern Denmark, Odense, Denmark
- Pil Joong Lee, pjl@postech.ac.kr
Pohang Univ. of Sci. & Tech., Korea
- Preda Mihailescu, preda@uni-paderborn.de
University of Paderborn, Germany
- David Naccache, david.naccache@gemplus.com
Gemplus Card International, France
- Bart Preneel, Bart.Preneel@esat.kuleuven.ac.be
Katholieke Universiteit Leuven, Belgium
- Erkey Savaş, savas@ece.orst.edu
Oregon State University, USA
- Joseph Silverman, jhs@math.brown.edu
Brown University and NTRU Cryptosystems, Inc., USA
- Jacques Stern, Jacques.Stern@ens.fr
Ecole Normale Supérieure, France
- Berk Sunar, sunar@ece.wpi.edu
Worcester Polytechnic Institute, USA
- Colin Walter, colin@comodo.net
Comodo Research Labs, UK

The external referees:

- Murat Aydos (Oregon State University, USA)
- Vittorio Bagini (Gemplus, Italy)

- Lejla Batina (KU Leuven, ESAT/COSIC, Belgium / SafeNet, The Netherlands)
- Siddika Berna Örs (KU Leuven, ESAT/COSIC, Belgium)
- Eric Brier (Gemplus, France)
- Marco Bucci (Gemplus, France)
- Jaewook Chung (University of Waterloo, Canada)
- Christophe Clavier (Gemplus International, France)
- Nora Dabbous (Gemplus, France)
- Jean-François Dhem (Gemplus, France)
- Itai Dror (M-Systems Flash Disk Pioneers, Israel)
- Nevine Ebeid (University of Waterloo, Canada)
- Levent Ertaul (Oregon State University, USA)
- Lijun Gao (Bermai Inc., USA)
- Johann Großschädl (IAIK, Graz University of Technology, Austria)
- Frank K. Gürkaynak (Swiss Federal Institute of Technology, Zurich, Switzerland)
- Pascal Guterman (Gemplus, France)
- Helena Handschuh (Gemplus, France)
- Kouichi Itoh (Fujitsu Laboratories Ltd., Japan)
- Marc Joye (Gemplus, France)
- Vangelis Karatsiolis (Technical University of Darmstadt / Fraunhofer Institute of Secure Telecooperation, Germany)
- Chong Hee Kim (Pohang Univ. of Sci. & Tech., Korea)
- Volker Krummel (University of Paderborn, Germany)
- Manuel Leone (Telecom Italia Lab, Italy)
- Albert Levi (Sabancı University, Turkey)
- Pierre-Yvan Liardet (STMicroelectronics, France)
- Renato Menicocci (Gemplus, France)
- Bodo Möller (Technical University of Darmstadt, Germany)
- Olaf Mueller (University of Paderborn, Germany)
- Gerardo Orlando (General Dynamics / WPI, USA)
- Elisabeth Oswald (IAIK TU-Graz, Austria / KU Leuven, Belgium)
- Christof Paar (Ruhr-University, Bochum, Germany)
- Pascal Paillier (Gemplus, France)
- Dong Jin Park (Pohang Univ. of Sci. & Tech., Korea)
- Stephanie Porte (Gemplus, France)
- Vincent Rijmen (Cryptomathic, Belgium)
- Francisco Rodriguez-Henriquez (CINVESTAV-IPN, Mexico)
- Gökay Saldamlı (Oregon State University, USA)
- Tom Schmidt (Oregon State University, USA)
- Jasper Scholten (KU Leuven, ESAT/COSIC, Belgium)
- Stefaan Seys (KU Leuven, ESAT/COSIC, Belgium)
- Jamshid Shokrollahi (University of Paderborn, Germany)
- Sang Gyoo Sim (Pohang Univ. of Sci. & Tech., Korea)
- Tsuyoshi Takagi (Technical University of Darmstadt, Germany)
- Masahiko Takenaka (Fujitsu Laboratories Ltd., Japan)
- Alexandre F. Tenca (Oregon State University, USA)
- Georgi Todorov (Oregon State University, USA)

- Elena Trichina (Gemplus, Italy)
- Christophe Tymen (Gemplus/ENS, France)
- Johannes Wölkerstorfer (Graz University of Technology, Austria)
- Thomas Wollinger (Ruhr-University, Bochum, Germany)
- Yiqun Lisa Yin (NTT MCL, USA)

The companies which provided support to CHES 2002:

- Intel - <http://www.intel.com>
- NTRU Cryptosystems, Inc. - <http://www.ntru.com>
- RSA Security, Inc. - <http://www.rsasecurity.com>

CHES Workshop Proceedings

- Ç.K. Koç and C. Paar (Editors). *Cryptographic Hardware and Embedded Systems*, Lecture Notes in Computer Science No. 1717, Springer-Verlag, Berlin, Heidelberg, New York, 1999.
- Ç.K. Koç and C. Paar (Editors). *Cryptographic Hardware and Embedded Systems - CHES 2000*, Lecture Notes in Computer Science No. 1965, Springer-Verlag, Berlin, Heidelberg, New York, 2000.
- Ç.K. Koç, D. Naccache, and C. Paar (Editors). *Cryptographic Hardware and Embedded Systems - CHES 2001*, Lecture Notes in Computer Science No. 2162, Springer-Verlag, Berlin, Heidelberg, New York, 2001.
- B. Kaliski Jr., Ç.K. Koç, and C. Paar (Editors). *Cryptographic Hardware and Embedded Systems - CHES 2002*, Lecture Notes in Computer Science No. 2523, Springer-Verlag, Berlin, Heidelberg, New York, 2002. (These proceedings).

Table of Contents

Invited Talk

CHES: Past, Present, and Future	1
<i>Jean-Jacques Quisquater</i>	

Attack Strategies

Optical Fault Induction Attacks	2
<i>Sergei P. Skorobogatov, Ross J. Anderson</i>	
Template Attacks	13
<i>Suresh Chari, Josyula R. Rao, Pankaj Rohatgi</i>	
The EM Side-Channel(s)	29
<i>Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, Pankaj Rohatgi</i>	

Finite Field and Modular Arithmetic I

Enhanced Montgomery Multiplication	46
<i>Shay Gueron</i>	
New Algorithm for Classical Modular Inverse	57
<i>Róbert Lórencz</i>	
Increasing the Bitlength of a Crypto-Coprocessor	71
<i>Wieland Fischer, Jean-Pierre Seifert</i>	

Elliptic Curve Cryptography I

Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems	82
<i>Elisabeth Oswald</i>	
Implementation of Elliptic Curve Cryptography with Built-In Counter Measures against Side Channel Attacks	98
<i>Elena Trichina, Antonio Bellezza</i>	
Secure Elliptic Curve Implementations: An Analysis of Resistance to Power-Attacks in a DSP Processor	114
<i>Catherine H. Gebotys, Robert J. Gebotys</i>	
Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA	129
<i>Kouichi Itoh, Tetsuya Izu, Masahiko Takenaka</i>	

AES and AES Candidates

2Gbit/s Hardware Realizations of RIJNDAEL and SERPENT:

A Comparative Analysis	144
<i>A.K. Lutz, J. Treichler, F.K. Gürkaynak, H. Kaeslin, G. Basler, A. Erni, S. Reichmuth, P. Rommens, S. Oetiker, W. Fichtner</i>	

Efficient Software Implementation of AES on 32-Bit Platforms	159
<i>Guido Bertoni, Luca Breveglieri, Pasqualina Fragneto, Marco Macchetti, Stefano Marchesin</i>	

An Optimized S-Box Circuit Architecture for Low Power AES Design ...	172
<i>Sumio Morioka, Akashi Satoh</i>	

Simplified Adaptive Multiplicative Masking for AES	187
<i>Elena Trichina, Domenico De Seta, Lucia Germani</i>	

Multiplicative Masking and Power Analysis of AES	198
<i>Jovan D. Golić, Christophe Tymen</i>	

Tamper Resistance

Keeping Secrets in Hardware: The Microsoft Xbox™ Case Study	213
<i>Andrew Huang</i>	

RSA Implementation

A DPA Attack against the Modular Reduction within a CRT

Implementation of RSA	228
<i>Bert den Boer, Kerstin Lemke, Guntram Wicke</i>	

Further Results and Considerations on Side Channel Attacks on RSA....	244
<i>Vlastimil Klíma, Tomáš Rosa</i>	

Fault Attacks on RSA with CRT: Concrete Results and

Practical Countermeasures	260
<i>Christian Aumüller, Peter Bier, Wieland Fischer, Peter Hofreiter, Jean-Pierre Seifert</i>	

Finite Field and Modular Arithmetic II

Some Security Aspects of the MIST Randomized

Exponentiation Algorithm	276
<i>Colin D. Walter</i>	

The Montgomery Powering Ladder	291
<i>Marc Joye, Sung-Ming Yen</i>	

DPA Countermeasures by Improving the Window Method	303
<i>Kouichi Itoh, Jun Yajima, Masahiko Takenaka, Naoya Torii</i>	

Efficient Subgroup Exponentiation in Quadratic and Sixth Degree Extensions	318
<i>Martijn Stam, Arjen K. Lenstra</i>	

Elliptic Curve Cryptography II

On the Efficient Generation of Elliptic Curves over Prime Fields	333
<i>Elisavet Konstantinou, Yiannis C. Stamatiou, Christos Zaroliagis</i>	
An End-to-End Systems Approach to Elliptic Curve Cryptography	349
<i>Nils Gura, Sheueling Chang Shantz, Hans Eberle, Sumit Gupta, Vipul Gupta, Daniel Finchelstein, Edouard Goupy, Douglas Stebila</i>	
A Low-Power Design for an Elliptic Curve Digital Signature Chip	366
<i>Richard Schroepel, Cheryl Beaver, Rita Gonzales, Russell Miller, Timothy Draelos</i>	
A Reconfigurable System on Chip Implementation for Elliptic Curve Cryptography over $\text{GF}(2^n)$	381
<i>M. Ernst, M. Jung, F. Madlener, S. Huss, R. Blümel</i>	
Genus Two Hyperelliptic Curve Coprocessor	400
<i>N. Boston, T. Clancy, Y. Liow, J. Webster</i>	

Random Number Generation

True Random Number Generator Embedded in Reconfigurable Hardware	415
<i>Viktor Fischer, Miloš Drutarovský</i>	
Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications	431
<i>Werner Schindler, Wolfgang Killmann</i>	
A Hardware Random Number Generator	450
<i>Thomas E. Tkacik</i>	

Invited Talk

RFID Systems and Security and Privacy Implications	454
<i>Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels</i>	

New Primitives

A New Class of Invertible Mappings	470
<i>Alexander Klimov, Adi Shamir</i>	

Finite Field and Modular Arithmetic II

Scalable and Unified Hardware to Compute Montgomery Inverse in $GF(p)$ and $GF(2^n)$	484
<i>Adnan Abdul-Aziz Gutub, Alexandre F. Tenca, ErKay Savaş, Çetin K. Koç</i>	
Dual-Field Arithmetic Unit for $GF(p)$ and $GF(2^m)$	500
<i>Johannes Wolkerstorfer</i>	
Error Detection in Polynomial Basis Multipliers over Binary Extension Fields	515
<i>Arash Reyhani-Masoleh, M.A. Hasan</i>	
Hardware Implementation of Finite Fields of Characteristic Three	529
<i>D. Page, N.P. Smart</i>	

Elliptic Curve Cryptography III

Preventing Differential Analysis in GLV Elliptic Curve Scalar Multiplication	540
<i>Mathieu Ciet, Jean-Jacques Quisquater, Francesco Sica</i>	
Randomized Signed-Scalar Multiplication of ECC to Resist Power Attacks	551
<i>Jae Cheol Ha, Sang Jae Moon</i>	
Fast Multi-scalar Multiplication Methods on Elliptic Curves with Precomputation Strategy Using Montgomery Trick	564
<i>Katsuyuki Okeya, Kouichi Sakurai</i>	

Hardware for Cryptanalysis

Experience Using a Low-Cost FPGA Design to Crack DES Keys	579
<i>Richard Clayton, Mike Bond</i>	
A Time-Memory Tradeoff Using Distinguished Points: New Analysis & FPGA Results	593
<i>Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, Jean-Didier Legat</i>	
Author Index	611

Template Attacks

Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi

No Institute Given