

*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

*New York University, NY, 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*

Marc Joye Jean-Jacques Quisquater (Eds.)

# Cryptographic Hardware and Embedded Systems – CHES 2004

6th International Workshop  
Cambridge, MA, USA, August 11-13, 2004  
Proceedings

Volume Editors

Marc Joye  
Gemplus, Card Security Group  
La Vigie, Avenue du Jujubier, ZI Athélia IV  
13705 La Ciotat Cedex, France  
E-mail: marc.joye@gemplus.com

Jean-Jacques Quisquater  
Université Catholique de Louvain  
UCL Crypto Group  
Place du Levant 3  
1348 Louvain-la-Neuve, Belgium  
E-mail: jjq@dice.ucl.ac.be

Library of Congress Control Number: 2004109601

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

ISSN 0302-9743  
ISBN 3-540-22666-4 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  
springeronline.com

© International Association for Cryptologic Research 2004  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH  
Printed on acid-free paper SPIN: 11307204 06/3142 5 4 3 2 1 0

# Preface

These are the proceedings of CHES 2004, the 6th Workshop on Cryptographic Hardware and Embedded Systems. For the first time, the CHES Workshop was sponsored by the International Association for Cryptologic Research (IACR).

This year, the number of submissions reached a new record. One hundred and twenty-five papers were submitted, of which 32 were selected for presentation. Each submitted paper was reviewed by at least 3 members of the program committee. We are very grateful to the program committee for their hard and efficient work in assembling the program. We are also grateful to the 108 external referees who helped in the review process in their area of expertise.

In addition to the submitted contributions, the program included three invited talks, by Neil Gershenfeld (Center for Bits and Atoms, MIT) about “Physical Information Security”, by Isaac Chuang (Medialab, MIT) about “Quantum Cryptography”, and by Paul Kocher (Cryptography Research) about “Physical Attacks”. It also included a rump session, chaired by Christof Paar, which featured informal talks on recent results.

As in the previous years, the workshop focused on all aspects of cryptographic hardware and embedded system security. We sincerely hope that the CHES Workshop series will remain a premium forum for intellectual exchange in this area.

This workshop would not have been possible without the involvement of several persons. In addition to the program committee members and the external referees, we would like to thank Christof Paar and Berk Sunar for their help on local organization. Special thanks also go to Karsten Tellmann for maintaining the Web pages and to Julien Bouchier for installing and running the submission and reviewing softwares of K.U. Leuven. Last but not least, we would like to thank all the authors who submitted papers, making the workshop possible, and the authors of accepted papers for their cooperation.

August 2004

Marc Joye and Jean-Jacques Quisquater

# 6th Workshop on Cryptographic Hardware and Embedded Systems

August 11–13, 2004, Boston/Cambridge, USA

<http://www.chesworkshop.org/>

## Organizing Committee

Christof Paar (Publicity Chair) ..... Ruhr-Universität Bochum, Germany  
Berk Sunar (General Chair) ..... Worcester Polytechnic Institute, USA

## Program Committee

Roberto Avanzi ..... Institute for Experimental Mathematics, Germany  
Benoît Chevallier-Mames ..... Gemplus, France  
Claude Crépeau ..... McGill University, Canada  
Marc Girault ..... France Telecom, France  
Jovan Golić ..... Telecom Italia, Italy  
Marc Joye (Co-chair) ..... Gemplus, France  
Seungjoo Kim ..... Sungkyunkwan University, Korea  
Çetin Koç ..... Oregon State University, USA  
Paul Kocher ..... Cryptography Research, USA  
François Koeune ..... K2Crypt, Belgium  
Tanja Lange ..... Ruhr-Universität Bochum, Germany  
Ruby Lee ..... Princeton University, USA  
Pierre-Yvan Liardet ..... ST Microelectronics, France  
Thomas Messerges ..... Motorola, USA  
Jean-Jacques Quisquater (Co-chair) ..... Université Catholique  
de Louvain, Belgium  
Josyula R. Rao ..... IBM T.J. Watson Research, USA  
Kouichi Sakurai ..... Kyushu University, Japan  
Erkay Savaş ..... Sabanci University, Turkey  
Werner Schindler ..... Bundesamt für Sicherheit in  
der Informationstechnik, Germany  
Jean-Pierre Seifert ..... Infineon Technologies, Germany  
Joseph Silverman ..... Brown University, USA  
Tsuyoshi Takagi ..... Technische Universität Darmstadt, Germany  
Frédéric Valette ..... DCSSI, France  
Serge Vaudenay ..... EPFL, Switzerland  
Colin Walter ..... Comodo Research Lab, UK  
Sung-Ming Yen ..... National Central University, Taiwan

## Steering Committee

Burton Kaliski .....	RSA Laboratories, USA
Çetin Koç .....	Oregon State University, USA
Christof Paar .....	Ruhr-Universität Bochum, Germany
Jean-Jacques Quisquater .....	Université Catholique de Louvain, Belgium
Colin Walter .....	Comodo Research Lab, UK

## External Referees

Onur Aciçmez	Darrel Hankerson	Pascal Paillier
Kazumaro Aoki	Clemens Heuberger	Eric Peeters
Toru Akishita	Chun Pyo Hong	Gerardo Pelosi
Gildas Avoine	Keijirou Ike	Gilles Piret
Thomas Baignères	Joshua Jaffe	Arash Reyhani-Masoleh
Claude Barral	Antoine Joux	Ottavio Rizzo
Lejla Batina	Pascal Junod	Francisco
Florent Bersani	Charanjit Jutla	Rodríguez-Henríquez
Guido Bertoni	Vangelis Karatsiolis	Pankaj Rohatgi
Eric Brier	Masanobu Katagi	Fabrice Romain
Philippe Bulens	Minho Kim	Yasuyuki Sakai
Benoît Calmels	Shinsaku Kiyomoto	Akashi Satoh
Julien Cathalo	Doug Kuhlman	Daniel Schepers
Guy Cathébras	Sébastien Kunz-Jacques	Katja Schmidt-Samoa
Suresh Chari	Soonhak Kwon	Adi Shamir
Jung Hee Cheon	Sandeep Kumar	Atsushi Shimbo
Chien-ning Chen	Gwenaëlle Martinet	Nicolas Sklavos
Che Wun Chiou	Donghoon Lee	Nigel Smart
Mathieu Ciet	Sangjin Lee	Jung Hwan Song
Christophe Clavier	Kerstin Lemke	Fabio Sozzani
Jean-Sébastien Coron	Yi Lu	Martijn Stam
Magnus Daum	Philippe Manet	François-Xavier
Guerric	Stefan Mangard	Standaert
Meurice de Dormale	Natsume Matsuzaki	Michael Steiner
Jean-François Dhem	Renato Menicocci	Daisuke Suzuki
Christophe Doche	Jean Monnerat	Alexei Tchoulkine
Reouven Elbaz	Christophe Mourtel	Yannick Teglia
Wieland Fischer	Frédéric Muller	Alexandre F. Tenca
Jacques Fournier	Michaël Nève	Thomas Tkacik
Pasqualina Fragneto	Kim Nguyen	Lionel Torres
Henri Gilbert	Philippe Oechslin	Eran Tromer
Louis Goubin	Francis Olivier	Michael Tunstall
Johann Großschädl	Kenji Ohkuma	Ingrid Verbauwhede
Jorge Guajardo	Takeshi Okamoto	Karine Villegas
Eric Hall	Katsuyuki Okeya	Andrew Weigl
DongGuK Han	Siddika Berna Örs	Kai Wirt
Helena Handschuh	Elisabeth Oswald	Chi-Dian Wu

## Previous CHES Workshop Proceedings

- CHES 1999:** Çetin K. Koç and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems*, vol. 1717 of *Lecture Notes in Computer Science*, Springer-Verlag, 1999.
- CHES 2000:** Çetin K. Koç and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2000*, vol. 1965 of *Lecture Notes in Computer Science*, Springer-Verlag, 2000.
- CHES 2001:** Çetin K. Koç, David Naccache, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2001*, vol. 2162 of *Lecture Notes in Computer Science*, Springer-Verlag, 2001.
- CHES 2002:** Burton S. Kaliski, Jr., Çetin K. Koç, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2002*, vol. 2523 of *Lecture Notes in Computer Science*, Springer-Verlag, 2002.
- CHES 2003:** Colin D. Walter, Çetin K. Koç, and Christof Paar (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2003*, vol. 2779 of *Lecture Notes in Computer Science*, Springer-Verlag, 2003.

# Table of Contents

## Side Channels I

Towards Efficient Second-Order Power Analysis . . . . .	1
<i>Jason Waddle, David Wagner</i>	
Correlation Power Analysis with a Leakage Model . . . . .	16
<i>Eric Brier, Christophe Clavier, Francis Olivier</i>	
Power Analysis of an FPGA (Implementation of Rijndael: Is Pipelining a DPA Countermeasure?) . . . . .	30
<i>François-Xavier Standaert, Siddika Berna Örs, Bart Preneel</i>	

## Modular Multiplication

Long Modular Multiplication for Cryptographic Applications . . . . .	45
<i>Laszlo Hars</i>	
Leak Resistant Arithmetic . . . . .	62
<i>Jean-Claude Bajard, Laurent Imbert, Pierre-Yvan Liardet, Yannick Teglia</i>	
Efficient Linear Array for Multiplication in $GF(2^m)$ Using a Normal Basis for Elliptic Curve Cryptography . . . . .	76
<i>Soonhak Kwon, Kris Gaj, Chang Hoon Kim, Chun Pyo Hong</i>	

## Low Resources I

Low-Power Elliptic Curve Cryptography Using Scaled Modular Arithmetic . . . . .	92
<i>E. Öztürk, B. Sunar, E. Savaş</i>	
A Low-Cost ECC Coprocessor for Smartcards . . . . .	107
<i>Harald Aigner, Holger Bock, Markus Hütter, Johannes Wolkerstorfer</i>	
Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs . . . . .	119
<i>Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, Sheueling Chang Shantz</i>	

## Implementation Aspects

Instruction Set Extensions for Fast Arithmetic in Finite Fields $GF(p)$ and $GF(2^m)$ . . . . .	133
<i>Johann Großschädl, ErKay Savaş</i>	



Aspects of Hyperelliptic Curves over Large Prime Fields in  
Software Implementations ..... 148  
*Roberto Maria Avanzi*

**Collision Attacks**

A Collision-Attack on AES (Combining Side Channel-  
and Differential-Attack)..... 163  
*Kai Schramm, Gregor Leander, Patrick Felke, Christof Paar*

Enhancing Collision Attacks..... 176  
*Hervé Ledig, Frédéric Muller, Frédéric Valette*

**Side Channels II**

Simple Power Analysis of Unified Code for ECC Double and Add ..... 191  
*Colin D. Walter*

DPA on  $n$ -Bit Sized Boolean and Arithmetic Operations and Its  
Application to IDEA, RC6, and the HMAC-Construction ..... 205  
*Kerstin Lemke, Kai Schramm, Christof Paar*

Side-Channel Attacks in ECC: A General Technique for Varying  
the Parametrization of the Elliptic Curve ..... 220  
*Loren D. Olson*

Switching Blindings with a View Towards IDEA ..... 230  
*Olaf Neißé, Jürgen Pulkus*

**Fault Attacks**

Fault Analysis of Stream Ciphers ..... 240  
*Jonathan J. Hoch, Adi Shamir*

A Differential Fault Attack Against Early Rounds of (Triple-)DES ..... 254  
*Ludger Hemme*

**Hardware Implementation I**

An Offset-Compensated Oscillator-Based Random Bit Source  
for Security Applications ..... 268  
*Holger Bock, Marco Bucci, Raimondo Luzzi*

Improving the Security of Dual-Rail Circuits ..... 282  
*Danil Sokolov, Julian Murphy, Alex Bystrov, Alex Yakovlev*

**Side Channels III**

A New Attack with Side Channel Leakage During Exponent Recoding Computations .....	298
<i>Yasuyuki Sakai, Kouichi Sakurai</i>	
Defeating Countermeasures Based on Randomized BSD Representations .....	312
<i>Pierre-Alain Fouque, Frédéric Muller, Guillaume Poupard, Frédéric Valette</i>	
Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems .....	328
<i>Pradeep Kumar Mishra</i>	
Efficient Countermeasures Against RPA, DPA, and SPA .....	343
<i>Hideyo Mamiya, Atsuko Miyaji, Hiroaki Morimoto</i>	

**Low Resources II**

Strong Authentication for RFID Systems Using the AES Algorithm .....	357
<i>Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfer</i>	
TTS: High-Speed Signatures on a Low-Cost Smart Card .....	371
<i>Bo-Yin Yang, Jiun-Ming Chen, Yen-Hung Chen</i>	

**Hardware Implementation II**

XTR Implementation on Reconfigurable Hardware .....	386
<i>Eric Peeters, Michael Neve, Mathieu Ciet</i>	
Concurrent Error Detection Schemes for Involution Ciphers .....	400
<i>Nikhil Joshi, Kaijie Wu, Ramesh Karri</i>	

**Authentication and Signatures**

Public Key Authentication with One (Online) Single Addition .....	413
<i>Marc Girault, David Lefranc</i>	
Attacking DSA Under a Repeated Bits Assumption .....	428
<i>P.J. Leadbitter, D. Page, N.P. Smart</i>	
How to Disembed a Program? .....	441
<i>Benoît Chevallier-Mames, David Naccache, Pascal Paillier, David Pointcheval</i>	

<b>Author Index</b> .....	455
---------------------------	-----