Lecture Notes in Computer Science 3156

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

Springer

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

Collision Attacks

Side Channels II

Fault Attacks

Hardware Implementation I

Side Channels III

Low Resources II

Hardware Implementation II

Authentication and Signatures