Lecture Notes in Computer Science 3659

*Commenced Publication in 1973*
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

Josyula R. Rao  Berk Sunar (Eds.)

# Cryptographic Hardware and Embedded Systems – CHES 2005

7th International Workshop
Edinburgh, UK, August 29 – September 1, 2005
Proceedings

Springer

Volume Editors

Josyula R. Rao
IBM T.J. Watson Research Center
19 Skyline Drive, Hawthorne, NY 10532, USA
E-mail: jrrao@us.ibm.com

Berk Sunar
Worcester Polytechnical Institute
Department of Electrical and Computer Engineering
100 Institute Road, Worcester, MA 01609, USA
E-mail: sunar@wpi.edu

Library of Congress Control Number: 2005931119

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-10 3-540-28474-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-28474-1 Springer Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11545262 06/3142 5 4 3 2 1 0

# Preface

These are the proceedings of the 7th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005) held in Edinburgh, Scotland from August 29 to September 1, 2005. The CHES workshop has been sponsored by the International Association for Cryptologic Research (IACR) for the last two years.

We received a total of 108 paper submissions for CHES 2005. The double-blind review process involved a 27-member program committee and a large number of external sub-referees. The review process concluded with a two week discussion process which resulted in 32 papers being selected for presentation. We are grateful to the program committee members and the external sub-referees for carrying out such an enormous task. Unfortunately, there were many strong papers that could not be included in the program due to a lack of space. We would like to thank all our colleagues who submitted papers to CHES 2005.

In addition to regular presentations, there were three excellent invited talks given by Ross Anderson (University of Cambridge) on "What Identity Systems Can and Cannot Do", by Thomas Wille (Philips Semiconductors Inc) on "Security of Identification Products: How to Manage", and by Jim Ward (Trusted Computing Group and IBM) on "Trusted Computing in Embedded Systems". It also included a rump session, chaired by Christof Paar, featuring informal talks on recent results.

The focus of CHES 2005 was similar to that of the earlier CHES workshops with the addition of a few new topics of emerging interest among which were smart card attacks and architectures, tamper resistance on the chip and board level, true and pseudo random number generators, special-purpose hardware for cryptanalysis, embedded security, cryptography for pervasive computing (e.g., RFID, sensor networks), device identification, non-classical cryptographic technologies, and side channel cryptanalysis. Special attention was paid to trusted computing platforms.

Special compliments go out to Colin D. Walter, the general chair and local organizer of CHES 2005, who brought the workshop to the beautiful historic town of Edinburgh, Scotland making it as much of a cultural event as a stimulating technical gathering. Christof Paar held the publicity Chair of CHES and was helpful at all stages of the organization. We would like to thank our corporate sponsors Cryptography Research Inc., escrypt GmbH, Gemplus, IBM, and RSA Security, who made it possible to have a lively event with their generous contributions. We would like to thank our dedicated webmaster Jens-Peter Kaps for maintaining the CHES website and review system even when he was travelling. Finally, we would like to thank the CHES steering committee members for giving us the honor of being part of such an influential conference.

August 2005 Josyula R. Rao and Berk Sunar

# 7th Workshop on Cryptographic Hardware and Embedded Systems

August 29 – September 1, 2005, Edinburgh, Scotland
http://www.chesworkshop.org/

## Organizing Committee

Colin D. Walter (General Chair) ..... Comodo Research Lab, UK
Christof Paar (Publicity Chair) ..... Ruhr-Universität Bochum, Germany
Josyula R. Rao (Program Co-chair) .. IBM T.J. Watson Research Center, USA
Berk Sunar (Program Co-chair) ..... Worcester Polytechnic Institute, USA

## Program Committee

Ross Anderson ..... Cambridge University, UK
Mohammed Benaissa ..... The University of Sheffield, UK
Suresh Chari ..... IBM T.J. Watson Research Center, USA
Kris Gaj ..... George Mason University, USA
Louis Goubin ..... Université de Versailles-St-Quentin-en-Yvelines, France
Jorge Guajardo ..... Infineon Technologies, Germany
Çetin Kaya Koç ..... Oregon State University, USA
Peter Kornerup ..... University of Southern Denmark, Denmark
Pil Joong Lee ..... Postech, South Korea
David Naccache ..... Gemplus, France and
Royal Holloway, University of London, UK
Elisabeth Oswald ..... Graz University of Technology, Austria
Christof Paar ..... Ruhr-Universität Bochum, Germany
Daniel Page ..... University of Bristol, UK
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Pankaj Rohatgi ..... IBM T.J. Watson Research Center, USA
Ahmad Sadeghi ..... Ruhr-University Bochum, Germany
Kouichi Sakurai ..... Kyushu University, Japan
David Samyde ..... FemtoNano, France
Erkay Savaş ..... Sabanci University, Turkey
Werner Schindler ..... Bundesamt für Sicherheit
in der Informationstechnik, Germany
Jean-Pierre Seifert ..... Intel, USA
Nigel Smart ..... University of Bristol, UK
Francois-Xavier Standaert ..... Université Catholique de Louvain, Belgium

Tsuyoshi Takagi ..... Future University, Hakodate, Japan
Elena Trichina ..... Spansion, USA
Ingrid Verbauwhede .. ESAT/COSIC Division, Katholieke Universiteit, Leuven
Colin Walter ..... Comodo Research Lab, UK

## Steering Committee

Marc Joye ..... Gemplus, Card Security Group, France
Burt Kaliski ..... RSA Laboratories, USA
Çetin Kaya Koç ..... Oregon State University, USA
Christof Paar ..... Ruhr-Universität Bochum, Germany
Jean-Jacques Quisquater ..... Université Catholique de Louvain, Belguim
Josyula R. Rao ..... IBM T.J. Watson Research Center, USA
Berk Sunar ..... Worcester Polytechnic Institute, USA
Colin D. Walter ..... Comodo Research Lab, UK

## External Referees

Onur Acıiçmez
Dakshi Agrawal
Mehdi-Laurent Akkar
Roberto Avanzi
Murat Aydos
Yoo Jin Baek
Lelia Barlow
Lejla Batina
Chevallier-Mames Benoit
Guido Bertoni
Régis Bevan
Mike Bond
Eric Brier
Julien Brouchier
Christophe De Cannière
Dario Carluccio
Laurent Caussou
Juyoung Cha
Herve Chabanne
Nam Su Chang
Kookrae Cho
Mathieu Ciet
Jolyon Clulow
Jean-Sbastien Coron
Nicolas Courtois
Colin van Dyke
Serdar S. Erdem
Martin Feldhofer
Patrick Felke
Wieland Fischer
Jacques J.A. Fournier
Patrick George
Christophe Giraud
Robert Granger
Johann Großschädl
Adnan Gutub
Ghaith Hammouri
Dong Guk Han
Helena Handschuh
Oliver Hauck
Alireza Hodjat
Tetsuya Izu
Mark Jung
Charanjit Jutla
Deniz Karakoyunlu
Paul Karger
Manabu Katagi
Alisher Anatolyevich Kholmatov
Tae Hyun Kim
Minho Kim
Shinsaku Kiyomoto
François Koeune
Sandeep Kumar
Klaus Kursawe
Soonhak Kwon
Gerard Lai
Joe Lano
Peter Leadbitter
Hyang-Sook Lee
Jung Wook Lee
Kerstin Lemke
HuiYun Li
Marco Macchetti
François Macé
Stefan Mangard
Marian Margraf
Nele Mentens
Atsuko Miyaji
Christophe Mourtel
Elke de Mulder
Robert Mullins

Michael Neve
Richard Noad
Francis Olivier
Gerardo Orlando
Siddika Berna Ors
Pascal Paillier
Fabrice Pautot
Matthew Parker
Eric Peeters
Jan Pelzl
Gilles Piret
Thomas Popp
Axel Poschmann
Christine Priplata
Kumar Ranganathan
Nalini Ratha
Arash Reyhani-Masoleh
Gaël Rouvroy
Andy Rupp
Reiner Sailer
Junichiro Saito
Ryuichi Sakai
Yasuyuki Sakai
Kazuo Sakiyama
Gökay Saldamlı
Hisayoshi Sato
Akashi Satoh
Daniel Schepers
Jörg Schwenk
Kai Schramm
Jong Hoon Shin
Jamshid Shokrollahi
Nicolas Sklavos
Sergei Skorobogatov
Colin Stahlke
Martijn Stam
Makoto Sugita
Katsuyuki Takashima
Stefan Tillich
Michael Tunstall
Shigenori Uchuyama
Guy Vandenbosch
Ihor Vasylstov
Frederik Vercauteren
Karine Villegas
Camille Vuillaume
Andre Weimerskirch
Claire Whelan
Christopher Wolf
Johannes Wolkerstorfer
Thomas Wollinger
Yeon Hyeong Yang
Jeong Il Yoon
Young Tae Youn

## 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, 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.

**CHES 2004:** Marc Joye and Jean-Jacques Quisquater (Editors). *Cryptographic Hardware and Embedded Systems – CHES 2004*, vol. 3156 of *Lecture Notes in Computer Science*, Springer-Verlag, 2004.

# Table of Contents

## Side Channels I

Resistance of Randomized Projective Coordinates Against Power Analysis
*William Dupuy, Sébastien Kunz-Jacques* . . . . . 1

Templates as Master Keys
*Dakshi Agrawal, Josyula R. Rao, Pankaj Rohatgi, Kai Schramm* . . . . . 15

A Stochastic Model for Differential Side Channel Cryptanalysis
*Werner Schindler, Kerstin Lemke, Christof Paar* . . . . . 30

## Arithmetic for Cryptanalysis

A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis
*Jean Sébastien Coron, David Lefranc, Guillaume Poupard* . . . . . 47

Further Hidden Markov Model Cryptanalysis
*P.J. Green, R. Noad, N.P. Smart* . . . . . 61

## Low Resources

Energy-Efficient Software Implementation of Long Integer Modular Arithmetic
*Johann Großschädl, Roberto M. Avanzi, Erkay Savaş, Stefan Tillich* . . . . . 75

Short Memory Scalar Multiplication on Koblitz Curves
*Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume* . . . . . 91

Hardware/Software Co-design for Hyperelliptic Curve Cryptography (HECC) on the 8051 $\mu P$
*Lejla Batina, David Hwang, Alireza Hodjat, Bart Preneel, Ingrid Verbauwhede* . . . . . 106

## Special Purpose Hardware

SHARK: A Realizable Special Hardware Sieving Device for Factoring 1024-Bit Integers
*Jens Franke, Thorsten Kleinjung, Christof Paar, Jan Pelzl, Christine Priplata, Colin Stahlke* . . . . . 119

Scalable Hardware for Sparse Systems of Linear Equations, with Applications to Integer Factorization
*Willi Geiselmann, Adi Shamir, Rainer Steinwandt, Eran Tromer* .... 131

Design of Testable Random Bit Generators
*Marco Bucci, Raimondo Luzzi* ..... 147

## Hardware Attacks and Countermeasures I

Successfully Attacking Masked AES Hardware Implementations
*Stefan Mangard, Norbert Pramstaller, Elisabeth Oswald* ..... 157

Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints
*Thomas Popp, Stefan Mangard* ..... 172

Masking at Gate Level in the Presence of Glitches
*Wieland Fischer, Berndt M. Gammel* ..... 187

## Arithmetic for Cryptography

Bipartite Modular Multiplication
*Marcelo E. Kaihara, Naofumi Takagi* ..... 201

Fast Truncated Multiplication for Cryptographic Applications
*Laszlo Hars* ..... 211

Using an RSA Accelerator for Modular Inversion
*Martin Seysen* ..... 226

Comparison of Bit and Word Level Algorithms for Evaluating Unstructured Functions over Finite Rings
*B. Sunar, D. Cyganski* ..... 237

## Side Channel II (EM)

EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA
*Catherine H. Gebotys, Simon Ho, C.C. Tiu* ..... 250

Security Limits for Compromising Emanations
*Markus G. Kuhn* ..... 265

Security Evaluation Against Electromagnetic Analysis at Design Time
*Huiyun Li, A. Theodore Markettos, Simon Moore* ..... 280

## Side Channel III

On Second-Order Differential Power Analysis
*Marc Joye, Pascal Paillier, Berry Schoenmakers* . . . . . 293

Improved Higher-Order Side-Channel Attacks with FPGA Experiments
*Eric Peeters, François-Xavier Standaert, Nicolas Donckers, Jean-Jacques Quisquater* . . . . . 309

## Trusted Computing

Secure Data Management in Trusted Computing
*Ulrich Kühn, Klaus Kursawe, Stefan Lucks, Ahmad-Reza Sadeghi, Christian Stüble* . . . . . 324

## Hardware Attacks and Countermeasures II

Data Remanence in Flash Memory Devices
*Sergei Skorobogatov* . . . . . 339

Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment
*Kris Tiri, David Hwang, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, Ingrid Verbauwhede* . . . . . 354

## Hardware Attacks and Countermeasures III

DPA Leakage Models for CMOS Logic Circuits
*Daisuke Suzuki, Minoru Saeki, Tetsuya Ichikawa* . . . . . 366

The "Backend Duplication" Method
*Sylvain Guilley, Philippe Hoogvorst, Yves Mathieu, Renaud Pacalet* . . . . . 383

## Efficient Hardware I

Hardware Acceleration of the Tate Pairing in Characteristic Three
*P. Grabher, D. Page* . . . . . 398

Efficient Hardware for the Tate Pairing Calculation in Characteristic Three
*T. Kerins, W.P. Marnane, E.M. Popovici, P.S.L.M. Barreto* . . . . . 412

## Efficient Hardware II

AES on FPGA from the Fastest to the Smallest
*Tim Good, Mohammed Benaissa* . . . . . 427

A Very Compact S-Box for AES
*D. Canright* . . . . . 441

**Author Index** . . . . . 457