

# 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 Aciğmez	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	Rodriguez-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
Guerrie	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 Tégia
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.

Cryptographic Hardware and Embedded Systems -  
CHES 2004

6th International Workshop Cambridge, MA, USA,

August 11-13, 2004, Proceedings

Joye, M.; Quisquater, J.-J. (Eds.)

2004, XIV, 462 p., Softcover

ISBN: 978-3-540-22666-6