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, jimg@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
- Erkay 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 Superieure, 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)
- Sıddıka 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 Wolkerstorfer (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).