

Preface

These are the proceedings of CHES 2001, the third Workshop on Cryptographic Hardware and Embedded Systems. The first two CHES Workshops were held in Massachusetts, and this was the first Workshop to be held in Europe. There was a large number of submissions this year, and in response the technical program was extended to 2 1/2 days.

As is evident by the papers in these proceedings, many excellent submissions were made. Selecting the papers for this year's CHES was not an easy task, and we regret that we had to reject several very interesting papers due to the lack of time. There were 66 submitted contributions this year, of which 31, or 47%, were selected for presentation. If we look at the number of submitted papers at CHES '99 (42 papers) and CHES 2001 (51 papers), we observe a steady increase. We interpret this as a continuing need for a workshop series which combines theory and practice for integrating strong security features into modern communications and computer applications. In addition to the submitted contributions, Ross Anderson from Cambridge University, UK, and Adi Shamir from The Weizmann Institute, Israel, gave invited talks.

As in previous years, the focus of the workshop is on all aspects of cryptographic hardware and embedded system design. 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 of intellectual exchange in creating 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 from WPI, and Delphine Abecassis and Cécile Osta from Novamedia for their efforts.

May 2001

Çetin K. Koç
David Naccache
Christof Paar

Acknowledgements

The program chairs express their thanks to the program committee, the referees for their help in selecting the best quality papers, and also the companies which provided support to the workshop.

The program committee members of CHES 2001:

- Ross Anderson (Ross.Anderson@cl.cam.ac.uk)
University of Cambridge, U.K.
- Jean-Sebastien Coron (Jean-Sebastien.CORON@gemplus.com)
Gemplus, France
- Kris Gaj (kgaj@gmu.edu)
George Mason University, USA
- Jim Goodman (JGoodman@chrysalis-its.com)
Chrysalis-ITS, Canada
- Anwar Hasan (ahasan@arith1.vlsi.uwaterloo.ca)
University of Waterloo, Canada
- Peter Kornerup (kornerup@imada.sdu.dk)
Odense University, Denmark
- Bart Preneel (Bart.Preneel@esat.kuleuven.ac.be)
Université Catholique de Louvain, Belgium
- Jean-Jacques Quisquater (jjq@dice.ucl.ac.be)
Université Catholique de Louvain, Belgium
- Patrice L. Roussel (proussel@ichips.intel.com)
Intel Corporation, USA
- Christoph Ruland (RULAND@nue.et-inf.uni-siegen.de)
Universität Siegen, Germany
- Erkay Savaş (erkay@rTrust.com)
rTrust, USA
- Joseph Silverman (jhs@ntru.com)
Brown University and NTRU Cryptosystems, Inc., USA
- Jacques Stern (Jacques.Stern@ens.fr)
Ecole Normale Supérieure, France
- Colin Walter (C.Walter@sna.co.umist.ac.uk)
Computation Department - UMIST, U.K.
- Michael Wiener (michael.wiener@entrust.com)
Entrust Technologies, Canada

The referees of CHES 2001:

- Tolga Acar (tacar@novell.com)
- Andre Adelsbach (anadel@cs.uni-sb.de)
- Ross Anderson (Ross.Anderson@cl.cam.ac.uk)
- Philippe Anguita (Philippe.Anguita@gemplus.com)
- Eric Brier (Eric.Brier@gemplus.com)
- Marco Bucci (Marco.Bucci@gemplus.com)

VIII Acknowledgements

- Denis Carabin (Denis.Carabin@gemplus.com)
- Mahieu Ciet (ciet@dice.ucl.ac.be)
- Christophe Clavier (Christophe.Clavier@gemplus.com)
- Jean-Sebastien Coron (coron@clipper.ens.fr)
- Nora Dabbous (nora.dabbous@gemplus.com)
- Jean-Francois Dhem (Jean-Francois.Dhem@gemplus.com)
- Adam Elbirt (aelbirt@nac.net)
- Nathalie Feyt (Nathalie.Feyt@gemplus.com)
- Kris Gaj (kgaj@gmu.edu)
- Jovan Golic (Jovan.Golic@gemplus.com)
- Guang Gong (ggong@cacr.math.uwaterloo.ca)
- Jim Goodman (jimg@mtl.mit.edu)
- Jorge Guajardo (guajardo@ece.wpi.edu)
- Frank Gurkaynak (kgf@WPI.EDU)
- Helena Handschuh (Helena.Handschuh@gemplus.com)
- Anwar Hasan (ahasan@claude.uwaterloo.ca)
- Marc Joye (Marc.Joye@gemplus.com)
- Cetin Koc (koc@ece.orst.edu)
- Francois Koeune (koeune@dice.ucl.ac.be)
- Peter Kornerup (kornerup@imada.sdu.dk)
- Spyros Magliveras (spyros@cse.unl.edu)
- Bill Martin (martin@WPI.EDU)
- Renato Menicocci (Renato.Menicocci@gemplus.com)
- Tom Messerges (Tom_Messerges-ADTL01@email.mot.com)
- Pascal Moitrel (Pascal.Moitrel@gemplus.com)
- Guglielmo Morgari (Guglielmo.MORGARI@gemplus.com)
- Christophe Mourtel (Christophe.Mourtel@gemplus.com)
- David Mraihi (David.Mraihi@gemplus.com)
- Gerardo Orlando (Gerardo.Orlando@GSC.GTE.Com)
- Christof Paar (christof@ece.wpi.edu)
- Marco Paggio (Marco.Paggio@gemplus.com)
- Pascal Paillier (Pascal.Paillier@gemplus.com)
- Bart Preneel (bart.preneel@esat.kuleuven.ac.be)
- Florence Ques (Florence.Ques@gemplus.com)
- Jean-Jacques Quisquater (jjq@dice.ucl.ac.be)
- Jean-Marc Robert (jean-marc.robert@gemplus.com)
- Francisco Rodriguez (rodrigfr@ece.orst.edu)
- Ludovic Rousseau (Ludovic.Rousseau@gemplus.com)
- Patrice Roussel (proussel@ichips.intel.com)
- Christoph Ruland (RULAND@nue.et-inf.uni-siegen.de)
- ErKay Savas (savas@ece.orst.edu)
- Tom Schmidt (toms@math.orst.edu)
- Joseph Silverman (jhs@ntru.com)
- Nigel Smart (nigel@cs.bris.ac.uk)
- Jacques Stern (jacques.stern@ens.fr)
- Berk Sunar (sunar@ece.wpi.edu)

- Alex Tenca (tenca@ece.orst.edu)
- van Trung Tran (trung@exp-math.uni-essen.de)
- Michael Tunstall (Michael.Tunstall@gemplus.com)
- Christophe Tymen (Christophe.Tymen@gemplus.com)
- Colin Walter (C.Walter@co.umist.ac.uk)
- Andre Weimerskirch (weika@ece.wpi.edu)
- Michael Wiener (michael.wiener@entrust.com)
- Ed Witzke (elwitzk@sandia.gov)
- Huapeng Wu (h3wu@cacr.math.uwaterloo.ca)

The companies which provided support to CHES 2001:

- Gemplus - <http://www.gemplus.com>
- NTRU Cryptosystems, Inc. - <http://www.ntru.com>
- rTrust - <http://www.rtrust.com>
- Secusys - <http://www.secusys.com>