



# Workshop on Cryptographic Hardware and Embedded Systems (CHES 2008)

www.chesworkshop.org  
Washington, D.C., USA  
August 10 – 13, 2008

sponsored by IACR



## Call for Papers

CHES is the premier forum for presenting new results and scientific advances in all aspects of cryptographic hardware and security for embedded systems. Of special interest are contributions that describe new methods for secure and efficient hardware implementation of cryptography, hardware support for secure and trustworthy software and high-speed or leak-resistant software for embedded systems, e.g. smart cards, microprocessors, DSPs, etc. The workshop helps to bridge the gap between the cryptography research community and the application areas of cryptography. Consequently, we encourage submissions from academia, industry, and other organizations. All submitted papers will be reviewed and the conference proceedings will be published by Springer as part of the Lecture Notes in Computer Science (LNCS) series.

This will be the tenth CHES workshop. CHES '99 and CHES 2000 were held at WPI, CHES 2001 in Paris, CHES 2002 in the San Francisco Bay Area, CHES 2003 in Cologne, CHES 2004 in Boston, CHES 2005 in Edinburgh, CHES 2006 in Yokohama and CHES 2007 in Vienna. The number of participants has grown to more than 250, with attendees coming from industry, academia, and government organizations. The topics of CHES 2008 include but are not limited to:

- \* Architectures for public-key & secret-key cryptosystems
- \* Reconfigurable hardware & FPGAs for cryptography
- \* Cryptography for ubiquitous computing and wireless applications
- \* Efficient arithmetic algorithms
- \* Special-purpose hardware for cryptanalysis
- \* Architectures for trusted computing
- \* Device identification
- \* Smart card architectures and attacks
- \* True and pseudorandom number generators
- \* Security for embedded software and systems
- \* Efficient software algorithms for embedded processors
- \* Formal methods and tools for secure hardware design
- \* Cryptographic processors and co-processors
- \* Security in commercial consumer applications (pay-TV, automotive, etc)
- \* Hardware tamper resistance
- \* Technologies and hardware for content protection
- \* Side channel attacks and countermeasures
- \* Non-classical cryptographic technologies

## Instructions for CHES Authors

Authors are invited to submit original papers in PDF format at the electronic submission site: [<https://s1.iacr.org/websubrev/ches2008/submit/>](https://s1.iacr.org/websubrev/ches2008/submit/). Instructions and details of the submission process are posted at that site.

The submission must be **anonymous**, with no author names, affiliations, acknowledgments, or obvious references. It should begin with a title, a short abstract, and a list of keywords. The paper should be at most 12 pages (excluding the bibliography and clearly marked appendices), and at most 15 pages in total, using at least 11-point font and reasonable margins. Submissions not meeting these guidelines risk rejection without consideration of their merits. All submissions will be blind-refereed.

### Policy against double submissions

Only original research contributions will be considered. Submissions that substantially duplicate work that any of the authors have published elsewhere, or have submitted in parallel to any other conferences or workshops that have proceedings, *will be instantly rejected*. Authors should be aware that we will co-operate with other conference committees to identify potential double-submissions and strictly enforce the IACR Policy on Irregular Submissions ([<http://www.iacr.org/irregular.html>](http://www.iacr.org/irregular.html)).

## Important Dates

Submission deadline:	<b>Feb 29th, 2008, 23:59 EST.</b>	Acceptance notification:	April 25th, 2008.
Final version due:	May 16th, 2008.	Workshop presentations:	August 11th – 13th, 2008.

## Mailing List

If you wish to receive subsequent Call for Papers and registration information, please send a brief mail to [mailinglist@chesworkshop.org](mailto:mailinglist@chesworkshop.org). Your details will only be used for sending CHES related information.

## Program Committee

- Daniel V. Bailey, RSA Laboratories, USA
- Lejla Batina, Katholieke Universiteit Leuven, Belgium
- Feng Bao, Institute for Infocomm Research, Singapore
- Daniel J. Bernstein, Univ. of Illinois, Chicago, USA
- Suresh Chari, IBM Research, USA
- Christophe Clavier, Gemalto, France
- Jean-Sébastien Coron, Univ. of Luxembourg, Luxembourg
- Markus Dichtl, Siemens AG, Germany
- Louis Goubin, Université de Versailles, France
- Anwar Hasan, Univ. of Waterloo, Canada
- Joshua Jaffe, Cryptography Research, USA
- Marc Joye, Thomson R&D, France
- Çetin Kaya Koç, Oregon State University, USA
- Markus Kuhn, University of Cambridge, UK
- Klaus Kursawe, Philips Research, Netherlands
- Ruby Lee, Princeton University, USA
- Kerstin Lemke-Rust, T-Systems, Germany
- Arjen Lenstra, EPFL, Switzerland, and Alcatel-Lucent Bell Laboratories, USA
- Stefan Mangard, Infineon Technologies, Germany
- Mitsuru Matsui, Mitsubishi Electric, Japan
- Máire McLoone, Queens University Belfast, UK
- David Naccache, ENS, France
- Katsuyuki Okeya, Hitachi, Japan
- Christof Paar, Ruhr-Universität Bochum, Germany
- Dan Page, Univ. of Bristol, UK
- Pascal Paillier, Gemalto, France
- Emmanuel Prouff, Oberthur Card Systems, France
- Jean-Jacques Quisquater, Université Catholique de Louvain, Belgium
- Anand Raghunathan, NEC Labs, USA
- Josyula R. Rao, IBM Research, USA
- Ahmad-Reza Sadeghi, Ruhr-Universität Bochum, Germany
- Akashi Satoh, AIST, Japan
- Erkay Savaş, Sabanci University, Turkey
- Patrick Schaumont, Virginia Tech, USA
- Jean-Pierre Seifert, Samsung R&D, USA
- Berk Sunar, Worcester Polytechnic Institute, USA
- Masahiko Takenaka, Fujitsu Laboratories Ltd, Japan
- Kris Tiri, Intel, USA
- Elena Trichina, Spansion, France
- Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium
- Colin Walter, Comodo CA, UK
- Johannes Wolkerstorfer, TU Graz, Austria

## Organizational Committee

All correspondence and/or questions should be directed to one of the Organizational Committee members:

**Elisabeth Oswald** (Program co-Chair)  
*University of Bristol*  
*Email: [Elisabeth.Oswald@bristol.ac.uk](mailto:Elisabeth.Oswald@bristol.ac.uk)*

**Pankaj Rohatgi** (Program co-Chair)  
*IBM T.J. Watson Research Center*  
*Email: [rohatgi@us.ibm.com](mailto:rohatgi@us.ibm.com)*

**Kris Gaj** (General co-Chair)  
*George Mason University*  
*Email: [kgaj@gmu.edu](mailto:kgaj@gmu.edu)*

**Jens-Peter Kaps** (General co-Chair)  
*George Mason University*  
*Email: [jkaps@gmu.edu](mailto:jkaps@gmu.edu)*

**Çetin Kaya Koç** (Publicity Chair)  
*Oregon State University*  
*Email: [koc@eecs.oregonstate.edu](mailto:koc@eecs.oregonstate.edu)*

## Workshop Proceedings

The proceedings will be published in the Springer Lecture Notes in Computer Science (LNCS) series in time for distribution at the Workshop. Accepted papers should be formatted according to the LNCS default author instructions at URL <http://www.springer.de/comp/lncs/authors.html> (see file “typeinst.pdf”). Note that in order to be included in the proceedings, the authors of an accepted paper must guarantee to present their contribution at the workshop.