Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005)

sponsored by IACR

www.chesworkshop.org

Edinburgh, Scotland, UK
August 29 – September 1, 2005

Call for Papers

The focus of this workshop is on all aspects of cryptographic hardware and security in embedded systems. The workshop is a forum for new results from the research community as well as from the industry. Of special interest are contributions that describe new methods for secure and efficient hardware implementations, 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.

This will be the seventh 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, and CHES 2004 in Boston. The number of participants has grown to more than 200, with attendees coming from industry, academia, and government organizations. The topics of CHES 2005 include but are not limited to:

- *Computer architectures for public-key and secret-key cryptosystems*
- *Reconfigurable computing in cryptography & FPGAs*
- *Cryptography for pervasive computing (RFID, sensor networks, etc.)*
- *Device identification*
- *Cryptography in wireless applications (mobile phone, LANs, etc.)*
- *Smart card attacks and architectures*
- *True and pseudo random number generators*
- *Embedded security*
- *Efficient algorithms for embedded processors*
- *Cryptographic processors and co-processors*
- *Nonclassical cryptographic technologies*
- *Security in pay-TV systems*
- *Tamper resistance on the chip and board level*
- *Special-purpose hardware for cryptanalysis*
- *Side Channel Cryptanalysis*
- *Trusted computing platforms*

Fault Detection and Tolerance in Cryptography Workshop 2005

CHES will be followed on 2nd September by the related, one day, *Fault Detection and Tolerance in Cryptography Workshop* at the same location. A separate call for papers is available for that workshop via the CHES web site.

Instructions for CHES Authors

Authors are invited to submit original papers. Electronic submission is strongly encouraged. A detailed description of the electronic submission procedure appears on the CHES webpages.

The submission must be **anonymous**, with no author names, affiliations, acknowledgements, 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.

Only original research contributions will be considered. Submissions which 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.*

Important Dates

Submission deadline:	**March 1st, 2005.**	Acceptance notification:	April 29th, 2005.
Final Version due:	May 29th, 2005.	Workshop presentations:	Aug 29th – Sept 1st, 2005

(CRYPTO 2005 takes place August 14th – 18th).

Mailing List

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

Program Committee

- Ross Anderson, Cambridge University, UK
- Mohammed Benaissa, The University of Sheffield, UK
- Suresh Chari, IBM Thomas J. Watson Research Center, USA
- Kris Gaj, George Mason University, USA
- Louis Goubin, Universite 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 Thomas J. Watson Research Center, USA
- Ahmad Sadeghi, Ruhr-Universität 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, TU Darmstadt, Germany
- Elena Trichina, Spansion, USA
- Ingrid Verbauwhede, ESAT/COSIC Division, Katholieke Universiteit, Leuven
- Colin Walter, Comodo CA, UK

Organizational Committee

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

Berk Sunar (Program co-Chair)
Electrical and Computer Eng. Dept.
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609-2280, USA
Phone: +1 508 831 5494
Fax: +1 508 831 5491
Email: sunar@ece.wpi.edu

Josyula R Rao (Program co-Chair)
IBM Watson Research Center
P.O. Box 704
Yorktown Heights
NY 10598, USA
Phone: +1 914 784-6692
Fax: +1 914 784-7455
Email: jrrao@us.ibm.com

Colin Walter (General Chair)
Cryptography Dept.
Comodo CA
7 Campus Road
Bradford, BD7 1HR, UK
Phone: +44 (0)1274 730505
Fax: +44 (0)1274 730909
Email: colin.walter@comodo.com

Christof Paar (Publicity Chair)
Electrical Eng. & Information Sciences Dept.
Ruhr-Universität Bochum
Universitätsstraße 150
Bochum, D-44780, Germany
Phone: +49 (0)234/32-22994
Fax: +49 (0)234/32-14389
Email: cpaar@crypto.rub.de

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`"). Notice that in order to be included in the proceedings, the authors of an accepted paper must guarantee to present their contribution at the workshop.

CD-ROM 5 Years CHES – Proceedings 1999–2003

Springer-Verlag issued a CD which contains the full text of all proceedings of the CHES conferences 1999–2003. The CD can be ordered exclusively from the CHES webpage: `<http://www.chesworkshop.org/>`.