



Workshop on Cryptographic Hardware and Embedded Systems (CHES 2006)

www.chesworkshop.org

Yokohama, Japan
October 10 – 13, 2006

sponsored by IACR



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 eighth 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, and CHES 2005 in Edinburgh. The number of participants has grown to more than 200, with attendees coming from industry, academia, and government organizations. The topics of CHES 2006 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*

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*. Moreover authors have to be aware that the IACR Policy on Irregular Submissions <<http://www.iacr.org/irregular.html>> will be strictly enforced.

Important Dates

Submission deadline:	April 10th, 2006.	Acceptance notification:	June 12th, 2006.
Final Version due:	July 10th, 2006.	Workshop presentations:	October 11th – 13th, 2006

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

- Mehdi-Laurent Akkar, Texas Instruments, Villeneuve-Loubet, France
- Jean-Sébastien Coron, University of Luxembourg, Luxembourg
- Nicolas T. Courtois, Axalto, Louveciennes, France
- Joan Daemen, STMicroelectronics, Belgium
- Pierre-Alain Fouque, ENS, Paris, France
- Jim Goodman, ATI Technologies, Canada
- Helena Handschuh, Gemplus, Issy-les-Moulineaux, France
- Laszlo Hars, Seagate Research, Pittsburgh, USA
- Tetsuya Izu, Fujitsu Laboratories Ltd, Japan
- Marc Joye, Gemplus & CIM-PACA, France
- Seungjoo Kim, Sungkyunkwan University, South Korea
- Çetin Kaya Koç, Oregon State University, USA
- Pil Joong Lee, Postech, South Korea
- Frédéric Muller, DCSSI, Paris, France
- Katsuyuki Okeya, Hitachi, Kawasaki, Japan
- Elisabeth Oswald, Graz University of Technology, Austria
- Christof Paar, Ruhr Universität, Bochum, Germany
- Josyula R. Rao, IBM T.J. Watson Research Center, USA
- Erkay Savaş, Sabanci University, Turkey
- Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik, Germany
- Nigel Smart, University of Bristol, UK
- François-Xavier Standaert, Université Catholique de Louvain-la-Neuve, Belgium
- Berk Sunar, Worcester Polytechnic Institute, USA
- Frédéric Valette, DGA/CELAR, France
- Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium
- Colin Walter, Comodo CA, UK
- Sung-Ming Yen, National Central University, Taiwan

Organizational Committee

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

Louis Goubin (Program co-Chair)
PRiSM Laboratory
Versailles St-Quentin-en-Yvelines University
45 avenue des États-Unis
F-78035 Versailles, France
Phone: +33 1 39 25 43 29
Fax: +33 1 39 25 40 57
Email: Louis.Goubin@prism.uvsq.fr

Tsutomu Matsumoto (General Chair)
Graduate School of EIS
(Environment and Information Sciences)
Yokohama National University
79-5 Tokiwadai, Hodogaya-ku
Yokohama 240-8501, Japan,
Phone: +81 45 339 4134
Fax: +81 45 339 4338
Email: tsutomu@mlab.jks.ynu.ac.jp

Mitsuru Matsui (Program co-Chair)
Mitsubishi Electric Corporation
Information Technology R&D Center
5-1-1 Ofuna, Kamakura
Kanagawa 247-8501, Japan
Phone: +81 467 41 2190
Fax: +81 467 41 2185
Email: Matsui.Mitsuru@ab.MitsubishiElectric.co.jp

Çetin Kaya Koç (Publicity Chair)
School of EECS
(Electrical Engineering and Computer Science)
Oregon State University
1148 Kelley Engineering Center
Corvallis, OR 97331-5501, USA
Phone: +1 541 737 4853
Fax: +1 541 737 1300
Email: koc@eeecs.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”). 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.