Workshop on Cryptographic Hardware and Embedded Systems (CHES 2009)

sponsored by IACR

www.chesworkshop.org

Lausanne, Switzerland
September 6 – 9, 2009

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 eleventh CHES workshop. Previous editions from 1999 to 2008 were successively held in Worcester (twice), Paris, San Francisco, Cologne, Boston, Edinburgh, Yokohama, Vienna and Washington. The number of participants has grown to more than 250, with attendees coming from industry, academia, and government organizations. The topics of CHES 2009 include but are not limited to:

Cryptographic Hardware

- *Hardware architectures for public-key & secret-key cryptography*
- *Special-purpose hardware for cryptanalysis*
- *Cryptographic processors and co-processors*
- *Hardware accelerators for security protocols (security processors, network processors, etc.)*
- *True and pseudorandom number generators*
- *Physically Unclonable Functions (PUFs)*

Cryptographic Software for Embedded Systems

- *Efficient software implementations of cryptography for embedded processors*
- *Efficient and secure implementations of cryptography using multiprocessor cores*
- *Cryptographic libraries*
- *Cryptographic algorithms targeting embedded devices*

Attacks Against Implementations and Countermeasures Against These Attacks

- *Side channel attacks and countermeasures*
- *Faults and fault models for cryptographic devices*
- *Fault attacks and countermeasures*
- *Hardware tamper resistance*
- *Trojan hardware*

Tools and Methodologies

- *Computer aided cryptographic engineering*
- *Methodologies and environments for fair comparison of hardware and software efficiency of cryptographic algorithms, architectures, and implementations*
- *Partial and run-time reconfiguration of cryptographic systems*
- *Reliability and fault tolerance in cryptography and cryptanalysis*
- *Architectures for trusted computing*

Applications & Implementation Environments

- *Cryptography in wireless applications (mobile phone, WLANs, etc.)*
- *Cryptography for pervasive computing (RFID, sensor networks, etc.)*
- *FPGA design security*
- *Hardware IP protection and anti-counterfeiting techniques*
- *Reconfigurable hardware for cryptography*
- *Smart card processors, systems and applications*
- *Security in commercial consumer applications (pay-TV, automotive, etc.)*
- *Secure storage devices (memories, disks, etc.)*
- *Technologies and hardware for content protection*
- *Security for embedded software and systems*

Instructions for CHES Authors

Authors are invited to submit original papers via electronic submission. Details of the electronic submission procedure will be posted on the CHES webpage (`<http://www.chesworkshop.org>`) when the system is activated, *a month* before the submission deadline.

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:	**March 16th, 2009, 23:59 Pacific Daylight Time (UTC minus 7 hrs)**
Acceptance notification:	May 18th, 2009
Final version due:	June 15th, 2009
Workshop presentations:	September 7th – 9th, 2009

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

- Lejla Batina, Katholieke Universiteit Leuven, Belgium
- Daniel J. Bernstein, University of Illinois, USA
- Guido Bertoni, STMicroelectronics, Italy
- Jean-Luc Beuchat, University of Tsukuba, Japan
- Luca Breveglieri, Politecnico di Milano, Italy
- Ernie Brickell, Intel, USA
- Dipanwita Roy Chowdhury, Indian Institute of Technology, Kharagpur, India
- Jean-Sébastien Coron, University of Luxembourg, Luxembourg
- Joan Daemen, STMicroelectronics, Belgium
- Ricardo Dahab, Universidade Estadual de Campinas, Brazil
- Markus Dichtl, Siemens AG, Germany
- Benoît Feix, Inside Contactless, France
- Viktor Fischer, Université de Saint-Étienne, France
- Pierre-Alain Fouque, ENS, France
- Catherine H. Gebotys, University of Waterloo, Canada
- Christophe Giraud, Oberthur Technologies, France
- Louis Goubin, Université de Versailles, France
- Jorge Guajardo, Philips Research Europe, The Netherlands
- Frank K. Gürkaynak, ETH Zurich, Switzerland
- Peter Gutmann, University of Auckland, New Zealand
- Helena Handschuh, Spansion, France
- Naofumi Homma, Tohoku University, Japan
- Josh Jaffe, Cryptography Research, USA
- Marc Joye, Thomson R&D, France

- Jens-Peter Kaps, George Mason University, USA
- Howon Kim, Pusan National University, South Korea
- Çetin Kaya Koç, University of California Santa Barbara, USA
- Markus Kuhn, University of Cambridge, UK
- Soonhak Kwon, Sungkyunkwan University, South Korea
- Kerstin Lemke-Rust, University of Applied Sciences Bonn-Rhein-Sieg, Germany
- Marco Macchetti, Nagracard SA, Switzerland
- Stefan Mangard, Infineon Technologies, Germany
- Liam Marnane, University College Cork, Ireland
- Mitsuru Matsui, Mitsubishi Electric, Japan
- David Naccache, ENS, France
- Dag Arne Osvik, EPFL, Switzerland
- Elisabeth Oswald, University of Bristol, UK
- Christof Paar, Ruhr-Universität Bochum, Germany
- Dan Page, University of Bristol, UK
- Pascal Paillier, Gemalto, France
- Jean-Jacques Quisquater, Université Catholique de Louvain, Belgium
- Francisco Rodríguez-Henríquez, CINVESTAV-IPN, Mexico
- Pankaj Rohatgi, IBM Watson Research Center, USA
- Erkay Savas, Sabanci University, Turkey
- Patrick Schaumont, Virginia Tech, USA
- Rainer Steinwandt, Florida Atlantic University, USA
- Berk Sunar, Worcester Polytechnic Institute, USA
- Elena Trichina, STMicroelectronics, France
- Colin Walter, Salford University, UK
- Michael J. Wiener, Cryptographic Clarity, Canada
- Johannes Wolkerstorfer, IAIK TU Graz, Austria
- Sung-Ming Yen, National Central University, Taiwan

Advisory Members

- François-Xavier Standaert, Université Catholique de Louvain, Belgium

Organizational Committee

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

Christophe Clavier (Program co-Chair)
Université de Limoges (France) &
Institut d'Ingénierie Informatique de Limoges (France)
Email: christophe.clavier@xlim.fr

Kris Gaj (Program co-Chair)
George Mason University (US)
Email: kgaj@gmu.edu

Marcelo Kaihara (General Chair)
École Polytechnique Fédérale de Lausanne (Switzerland)
Email: marcelo.kaihara@epfl.ch

Çetin Kaya Koç (Publicity Chair)
University of California Santa Barbara (US)
Email: koc@cs.ucsb.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.