# Workshop on Cryptographic Hardware and Embedded Systems (CHES 2010)

www.chesworkshop.org

Santa Barbara, California, USA
August 17 – 20, 2010

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 and other interested parties. 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 aims to bridge the gap between the cryptography research community and the application areas of cryptography. All submitted papers will be reviewed. During the last years, the number of participants of CHES has grown to more than 300, with attendees coming from industry, academia, and government organizations. CHES 2010 will be co-located with the 30th Annual International Cryptology Conference, CRYPTO 2010, in Santa Barbara, California, USA. This will provide unique interaction opportunities for the communities of both conferences. The topics of CHES 2010 include but are not limited to:

***Cryptographic implementations***

- *Hardware architectures for public-key and secret-key cryptographic algorithms*
- *Cryptographic processors and co-processors*
- *Hardware accelerators for security protocols (security processors, network processors, etc.)*
- *True and pseudorandom number generators*
- *Physically unclonable functions (PUFs)*
- *Efficient software implementations of cryptography for embedded processors*

***Attacks against implementations and countermeasures against these attacks***

- *Side channel attacks and countermeasures*
- *Fault attacks and countermeasures*
- *Hardware tamper resistance*
- *Hardware trojans*

***Tools and methodologies***

- *Computer aided cryptographic engineering*
- *Verification methods and tools for secure design*
- *Metrics for the security of embedded systems*
- *Secure programming techniques*

***Applications***

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

***Interactions between cryptographic theory and implementation issues***

- *New and emerging cryptographic algorithms and protocols targeting embedded devices*
- *Non-classical cryptographic technologies*
- *Special-purpose hardware for cryptanalysis*
- *Formal methods for secure hardware*

## 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 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.* The IACR Policy on Irregular Submissions (`http://www.iacr.org/irregular.html`) will be strictly enforced.

## Important Dates

| | | | |
|---|---|---|---|
| Submission deadline: | **March 1, 2010, 23:59 PST** | Acceptance notification: | April 30, 2010 |
| Final version due: | May 26, 2010 | Workshop presentations: | August 18 – 20, 2010 |

## Program Committee

- Lejla Batina, Radboud University Nijmegen, The Netherlands and KU Leuven, Belgium
- Daniel J. Bernstein, University of Illinois, USA
- Guido Bertoni, STMicroelectronics, Italy
- Jean-Luc Beuchat, University of Tsukuba, Japan
- Christophe Clavier, Université de Limoges, France
- Jean-Sébastien Coron, Univ. of Luxemb., Luxembourg
- Josep Domingo-Ferrer, Univ. Rovira i Virgili,Catalonia
- Hermann Drexler, Giesecke & Devrient, Germany
- Viktor Fischer, Université de Saint-Étienne, France
- Wieland Fischer, Infineon Technologies, Germany
- Pierre-Alain Fouque, ENS, France
- Kris Gaj, George Mason University, USA
- Louis Goubin, Université de Versailles, France
- Aline Gouget, Gemalto, France
- Johann Großschädl, Univ. of Luxemb., Luxembourg
- Jorge Guajardo, Philips Research, The Netherlands
- Kouichi Itoh, Fujitsu Laboratories, Japan
- Marc Joye, Thomson R&D, France
- Çetin Kaya Koç, UC Santa Barbara, USA
- François Koeune, UC Louvain, Belgium
- Soonhak Kwon, Sungkyunkwan Univ., South Korea
- Kerstin Lemke-Rust, University of Applied Sciences Bonn-Rhein-Sieg, Germany
- Marco Macchetti, Nagravision SA, Switzerland
- Mitsuru Matsui, Mitsubishi Electric, Japan
- Máire O'Neill (nee McLoone),Queens Univ. Belfast,UK
- Michael Neve, Intel, USA
- Elisabeth Oswald, University of Bristol, UK
- Christof Paar, Ruhr-Universität Bochum, Germany
- Eric Peeters, Texas Instruments, Germany
- Axel Poschmann, NTU, Singapore
- Emmanuel Prouff, Oberthur Technologies, France
- Pankaj Rohatgi, Cryptography Research, USA
- Akashi Satoh, Research Center for Inf. Security, Japan
- Erkay Savas, Sabanci University, Turkey
- Patrick Schaumont, Virginia Tech, USA
- Werner Schindler, BSI, Germany
- Sergei Skorobogatov, University of Cambridge, UK
- Tsuyoshi Takagi, Future University-Hakodate, Japan
- Stefan Tillich, Graz University of Technology, Austria
- Mathias Wagner, NXP Semiconductors, Germany
- Colin Walter, Royal Holloway, UK

## Organizational Committee

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

**Stefan Mangard** (Program co-Chair)
*Infineon Technologies (Germany)*
*Email: stefan.mangard@infineon.com*

**François-Xavier Standaert** (Program co-Chair)
*Université catholique de Louvain (Belgium)*
*Email: fstandae@uclouvain.be*

**Çetin Kaya Koç** (General co-Chair)
*University of California Santa Barbara (USA)*
*Email: koc@cs.ucsb.edu*

**Jean-Jacques Quisquater** (General co-Chair)
*Université catholique de Louvain (Belgium)*
*Email: jjq@uclouvain.be*

## 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 follow the LNCS default author instructions at URL `http://www.springer.de/comp/lncs/authors.html` (see file "`typeinst.pdf`"). In order to be included in the proceedings, the authors of an accepted paper must guarantee to present their contribution at the workshop.