Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011)

http://www.chesworkshop.org/

Nara, Japan
September 28 – October 1, 2011

sponsored by IACR

Final Call for Papers
(The workshop venue and date have been changed)

Important Dates

Submission deadline:	April 4, 2011, 23:59 JST **(Closed)**
Acceptance notification:	June 6, 2011
Final version due:	July 4, 2011
Workshop presentations (changed):	**September 28 – October 1, 2011**

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.

This will be the thirteenth CHES workshop. Previous editions from 1999 to 2010 were successively held in Worcester (twice), Paris, San Francisco, Cologne, Boston, Edinburgh, Yokohama, Vienna, Washington, Lausanne, and Santa Barbara. The number of participants has grown to more than 300, with attendees coming from industry, academia, and government organizations. The topics of CHES 2011 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 our electronic submission system (`https://secure.iacr.org/websubrev/ches2011/submit/index.php`). 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 16 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 or journals, *will be instantly rejected.* The IACR Policy on Irregular Submissions (`http://www.iacr.org/irregular.html`) will be strictly enforced. The program committees may share information about submitted papers with other conference chairs and journal editors to help ensure the integrity of papers under consideration.

Program Committee

- Toru Akishita, Sony Corporation, Japan
- Paulo Barreto, University of São Paulo, Brazil
- Lejla Batina, Radboud University Nijmegen, The Netherlands and Katholieke Univ. Leuven, Belgium
- Daniel J. Bernstein, Univ. of Illinois at Chicago, USA
- Guido Bertoni, STMicroelectronics, Italy
- Swarup Bhunia, Case Western Reserve Univ., USA
- Chen-Mou Cheng, National Taiwan University, Taiwan
- Jean-Sebastien Coron, Univ. of Luxemb., Luxembourg
- Emmanuelle Dottax, Oberthur Technologies, France
- Hermann Drexler, Giesecke & Devrient, Germany
- Martin Feldhofer, Graz Univ. of Technology, Austria
- Pierre-Alain Fouque, ENS, France
- Kris Gaj, George Mason University, USA
- Benedikt Gierlichs, Katholieke Univ. Leuven, Belgium
- Louis Goubin, Universitaté de Versailles, France
- Jorge Guajardo, Philips Research, The Netherlands
- Dong-Guk Han, Kookmin University, Korea
- Helena Handschuh, Intrinsic-ID, USA and Katholieke Univ. Leuven, Belgium.
- Anwar Hasan, University of Waterloo, Canada
- Naofumi Homma, Tohoku University, Japan
- Marc Joye, Technicolor, France
- Pascal Junod, HEIG-VD, Switzerland
- Shinichi Kawamura, AIST, Japan
- Paris Kitsos, Hellenic Open University, Greece
- Markus Kuhn, Cambridge University, UK
- Kerstin Lemke-Rust, University of Applied Sciences Bonn-Rhein-Sieg, Germany
- Stefan Mangard, Infineon Technologies, Germany
- Mitsuru Matsui, Mitsubishi Electric, Japan
- David Naccache, ENS, France
- Heike Neumann, NXP, Germany
- Elisabeth Oswald, University of Bristol, UK
- Christof Paar, Ruhr University of Bochum, Germany
- Matt Robshaw, Orange Labs, France
- Pankaj Rohatgi, Cryptography Research, USA
- Ahmad-Reza Sadeghi, TU Darmstadt and Fraunhofer SIT, Germany
- Kazuo Sakiyama, University of Electro Communications, Japan
- Erkay Savas, Sabancı University, Turkey
- Patrick Schaumont, Virginia Tech, USA
- Nigel P. Smart, University of Bristol, UK
- Masahiko Takenaka, Fujitsu Laboratories, Japan
- Colin Walter, Royal Holloway, Univ. of London, UK

Organizational Committee

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

Bart Preneel (Program co-Chair)
Katholieke Universiteit Leuven (Belgium)
Email: ches2011programchairsHEREATiacr.org

Tsuyoshi Takagi (Program co-Chair)
Kyushu University (Japan)
Email: ches2011programchairsHEREATiacr.org

Akashi Satoh (General Chair)
National Institute of Advanced Industrial Science and Technology (Japan)
Email: ches2011generalchairHEREATiacr.org

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 sign the IACR Copyright form (`http://www.iacr.org/forms/`) and they must guarantee that their paper will be presented at the conference.

Posters

We plan to invite poster presentations at CHES 2011. More details about poster presentations will be announced in the webpage of CHES 2011.