Worshop on Cryptographic Hardware and Embedded Systems CHES 2012

Leuven, Belgium
9 - 12 September 2012

Call For Papers

CHES covers new results on all aspects of the design and analysis of cryptographic hardware and software implementations. The workshop builds a bridge between the cryptographic research community and the cryptographic engineering community. With participants from industry, academia, and government organizations, the number of participants has grown to over 300 in recent years.

In addition to a track of high-quality presentations, CHES 2012 will offer invited talks, tutorials, a poster session, and a rump session. CHES 2012 especially encourages submissions on the following two subjects: *design methods to build secure and efficient hardware or software* and *leakage resilient cryptography including new model definitions and analysis and the design of new cryptosystems.* All submitted papers will be reviewed by at least four Program Committee members. **This year, authors will be invited to submit brief rebuttals of the reviews before the final acceptances are made.**

The topics of CHES 2012 include but are not limited to:

Cryptographic implementations

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

Attacks against implementations and countermeasures against these attacks

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

Tools and methodologies

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

Interactions between cryptographic theory and implementation issues

- *New and emerging cryptographic algorithms and protocols targeting embedded devices*
- *Special-purpose hardware for cryptanalysis*
- *Leakage resilient cryptography*

Applications

- *Cryptography in wireless applications (mobile phone, WLANs, etc.)*
- *Cryptography for pervasive computing (RFID, sensor networks, smart devices, etc.)*
- *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*

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. 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 18 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 5, 2012, 23:59 PST**	Acceptance notification:	May 14, 2012
Final version due:	June 18, 2012	Workshop presentations:	September 9 – 12, 2012

Poster Session

The CHES technical sessions will include a slot for a poster session, open to any submitter.
Arrangements for submitting posters will be announced later.

Tutorial Sessions

The program chairs welcome suggestions for half-day tutorials at `ches2012programchairs@iacr.org`.

Program Committee

- D. Bernstein, University of Illinois at Chicago, USA
- P. Barreto, University of São Paulo, Brazil
- G. Bertoni, STMicroelectronics, Italy
- S. Bhunia, Case Western University, USA
- Z. Chen, Certicom - A Subsidiary of RIM, USA
- D. Roy Chowdhury, Indian Institute of Technology Kharagpur, India
- J.-S. Coron, University of Luxembourg, Luxembourg
- R. Dahab, University of Campinas, Brazil
- H. Drexler, Giesecke & Devrient, Germany
- T. Eisenbarth, Florida Atlantic University, USA
- K. Gaj, George Mason University, USA
- C. Gebotys, University of Waterloo, Canada
- B. Gierlichs, K.U. Leuven, Belgium
- C. Giraud, Oberthur Technologies, France
- L. Goubin, University of Versailles, France
- S. Guilley, TELECOM ParisTech, France
- T. Gueneysu, Ruhr University Bochum, Germany
- N. Homma, Tohoku University, Japan
- M. Joye, Technicolor, France
- K. Lemke-Rust, University of Applied Sciences Bonn-Rhein-Sieg, Germany
- Y. Makris,University of Texas at Dallas, USA
- S. Mangard, Infineon Technologies, Germany
- M. Matsui, Mitsubishi Electric, Japan
- B. Ors, Istanbul Technical University, Turkey
- E. Oswald, University of Bristol, UK
- O. Pereira, UCL, Belgium
- K. Pietrzak, IST Austria, Austria
- A. Poschmann, Nanyang Technological University, Singapore
- N. Potlapally, Intel Corporation, USA
- L. Reyzin, Boston University, USA
- M. Rivain, CryptoExperts, France
- M. Robshaw, Orange Labs, France
- T. Roche, ANSSI, France
- P. Rohatgi, Cryptography Research, USA
- A. Satoh, AIST, Japan
- E. Savas, Sabanci University, Turkey
- J.-M. Schmidt, IAIK TU Graz, Austria
- S. Skorobogatov, Cambridge University, UK
- N. Smart, University of Bristol, UK
- A. Tria, CEA-LETI/ENSM-SE SAS, France
- N. Veyrat-Charvillon, UCL, Belgium
- C. Walter, Royal Holloway, UK
- D. Watanabe, Hitachi Ltd, Japan
- D. Yamamoto, Fujitsu Laboratories, Japan and K.U. Leuven, Belgium

Organizational Committee

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

Emmanuel Prouff (Program co-Chair)
Oberthur Technologies (France)
Email: ches2012programchairs@iacr.org

Patrick Schaumont (Program co-Chair)
Virginia Tech (USA)
Email: ches2012programchairs@iacr.org

Lejla Batina (General co-Chair)
Radboud University Nijmegen (Netherlands)
and K.U. Leuven (Belgium)
Email: lejla@cs.ru.nl

Ingrid Verbauwhede (General co-Chair)
K.U. Leuven (Belgium)
Email: Ingrid.Verbauwhede@esat.kuleuven.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.