Workshop on Cryptographic Hardware and Embedded Systems (CHES 2013)

www.chesworkshop.org

Santa Barbara, California, USA
August 20 – 23, 2013

sponsored by IACR

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. CHES 2013 will be co-located with the 33rd Annual International Cryptology Conference, CRYPTO 2013, in Santa Barbara, California, USA. This will provide unique interaction opportunities for the communities of both conferences.

In addition to a track of high-quality presentations, CHES 2013 will offer invited talks, tutorials, a poster session, and a rump session. All submitted papers will be reviewed by at least four Program Committee members. Authors will be invited to submit brief rebuttals of the reviews before the final acceptances are made. The proceedings will be published in the Springer Lecture Notes in Computer Science (LNCS) series in time for distribution at the workshop. Selected papers will be invited to be published in Journal of Cryptology and Journal of Cryptographic Engineering.

The topics of CHES 2013 include but are not limited to:

Cryptographic implementations

- *Hardware architectures for cryptographic primitives*
- *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 1, 2013, 23:59 PST**	Acceptance notification:	May 13, 2013
First round of comments:	April 15, 2013	Final version due:	June 8, 2013
Responses to comments due:	April 18, 2013, 23:59 PST	Workshop presentations:	August 20 – 23, 2013

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 ches2013programchairs@iacr.org. A tutorial suggestion should include a short description of the content, its objectives, and its intended audience. The submission deadline is 1 April 2013. Tutorial proposals will be reviewed by the Program Chairs. Presenters of accepted tutorials will be offered a complimentary registration to CHES 2013 as well as partial reimbursement of travel costs.

Program Committee

- L. Batina, Radboud University Nijmegen, The Netherlands.
- D. Bernstein, University of Illinois at Chicago, USA and Technische Universiteit Eindhoven, Netherlands.
- G. Bertoni, STMicroelectronics, Italy (co-chair).
- A. Biryukov, University of Luxemburg, Luxembourg.
- A. Bogdanov, Technical University of Denmark, Department of Mathematics, Denmark.
- C. Clavier, University of Limoges, France.
- J.-S. Coron, University of Luxembourg, Luxembourg (co-chair).
- J. Fan, KU Leuven, Belgium.
- B. Feix, UL, UK Security Lab.
- W. Fischer, Infineon Technologies, Germany.
- P.-A. Fouque, ENS, France.
- K. Gaj, George Mason University, USA.
- B. Gierlichs, KU Leuven, Belgium.
- L. Goubin, University of Versailles, France.
- J. Groszschaedl, University of Luxembourg, Luxembourg.
- S. Gueron, University of Haifa, Israel and Intel Corporation.
- T. Güneysu, Ruhr-Universität Bochum, Germany.
- H. Handschuh, Cryptography Research, USA and KU Leuven, Belgium.
- M. Joye, Technicolor, France.
- R. Khazan, MIT Lincoln Laboratory, USA.
- I. Kizhvatov, Riscure, Netherlands.
- S. Kwon, Sungkyunkwan University, Korea.
- G. Leander, Technical University of Denmark, Denmark.
- K. Lemke-Rust, Bonn-Rhein-Sieg University of Applied Sciences, Germany.
- S. Moriai, NICT, Japan.
- D. Naccache, ENS, France.
- C. Paar, Ruhr-Universität Bochum, Germany.
- D. Page, University of Bristol, UK.
- A. Poschmann, Nanyang Technological University, Singapore.
- E. Prouff, ANSSI, France.
- F. Regazzoni, TU Delft, The Netherlands and ALaRI, Switzerland.
- M. Rivain, CryptoExperts, France.
- A.-R. Sadeghi, TU Darmstadt, Germany.
- A. Satoh, AIST, Japan.
- P. Schaumont, Virginia Tech, USA.
- D. Suzuki, Mitsubishi Electric, Japan.
- Y. Teglia, STMicroelectronics, France.

- M. Tibouchi, NTT Secure Platform Laboratories, Japan.
- S. Tillich, University of Bristol, UK.
- P. Tuyls, Intrinsic-ID, The Netherlands.
- C. Walter, Royal Holloway, UK.
- D. Yamamoto, Fujitsu Laboratories, Japan.
- B.-Y. Yang, Academia Sinica, Taiwan.

Organizational Committee

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

Guido Bertoni (Program co-Chair)
STMicroelectronics (Italy)
Email: ches2013programchairs@iacr.org

Jean-Sébastien Coron (Program co-Chair)
University of Luxembourg (Luxembourg)
Email: ches2013programchairs@iacr.org

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

Thomas Eisenbarth (General co-Chair)
Worcester Polytechnic Institute (USA)
Email: teisenbarth@wpi.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 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.