Workshop on Cryptographic Hardware and Embedded Systems (CHES)

Call for Papers

The annual CHES workshop highlights new results in the design and analysis of cryptographic hardware and software implementations. CHES provides a valuable connection between the research and cryptographic engineering communities and attracts participants from industry, academia, and government organizations. As well as a single track of high-quality presentations, CHES 2014 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 and authors will be invited to submit brief rebuttals to reviews before the final decisions are made. Topics suitable for CHES 2014 include, but are not limited to:

Cryptographic implementations

- *Hardware architectures*
- *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*

Attacks against implementations and countermeasures

- *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 phones, 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

Submissions must be **anonymous** with no author names, affiliations, acknowledgments, or obvious references. Papers should begin with a title, a short abstract, and a list of keywords. Papers should be no more than 12 pages in length, excluding bibliography and clearly marked appendices, with at most 18 pages in total using at least 11-point font and reasonable margins. All submissions will be blind-refereed and submissions which substantially duplicate work published elsewhere, or submitted in parallel to any other conference or workshop with proceedings, *will be instantly rejected*; the IACR Policy on Irregular Submissions is available via `www.iacr.org/docs/`. Details of the electronic submission procedure will be posted on the CHES conference web-page. The final proceedings of CHES 2014 will be published by Springer in the LNCS series and accepted papers must conform to Springer publishing requirements. At least one author of an accepted paper must attend CHES 2014 to present the paper.

- *Submission deadline:* ***March 3, 2014, 23:59 PST***
- *Referee comments to authors: May 2, 2014*
- *Author response to comments: May 12, 2014*
- *Paper notification: May 26, 2014*
- *Final version due: June 13, 2014*
- *Workshop dates: September 23 – 26, 2014*

Poster and Tutorial Sessions

- CHES 2014 will include a poster session; the *Call for Posters* is available via the conference web-page.
- The program co-chairs welcome proposals for half-day tutorials at CHES 2014. The presenter of an accepted proposal will be offered a complimentary registration to CHES 2014 and a fixed stipend towards their travel costs. More details are available via the conference web-page.

Program Committee

O. Aciiçmez, Samsung Research America, US.
L. Batina, Radboud University Nijmegen, NL.
G. Bertoni, STMicroelectronics, IT.
D. Bernstein, University of Illinois at Chicago, US, and Technische Universiteit Eindhoven, NL.
C. Clavier, University of Limoges, FR.
J.-S. Coron, University of Luxembourg, LU.
E. De Mulder, Cryptography Research, US.
T. Eisenbarth, Worcester Polytechnic Institute, US.
J. Fan, Nationz Technologies, CN.
W. Fischer, Infineon Technologies, DE.
P.-A. Fouque, Université Rennes 1 and Institut Universitaire de France, FR.
B. Gierlichs, KU Leuven, BE.
K. Gaj, George Mason University, US.
L. Goubin, University of Versailles, FR.
T. Güneysu, Ruhr-Universitat Bochum, DE.
D.-G. Han, Kookmin University, KR.
H. Handschuh, Cryptography Research, US, and KU Leuven, BE.
M. Hutter, Graz University of Technology, AT.
M. Joye, Technicolor, FR.
H. Kim, Pusan National University, KR.
I. Kizhvatov, Riscure, NL.
F. Koeune, Université Catholique de Louvain, BE.
F. Koushanfar, ECE, Rice University, US.
G. Leander, Ruhr-Universität Bochum, DE.
K. Lemke-Rust, Bonn-Rhein-Sieg University of Applied Sciences, DE.
S. Mangard, Graz University of Technology, AT.
R. Maes, Intrinsic-ID, NL.
M. Medwed, NXP Semiconductors, AT.
C. Paar, Ruhr-Universität Bochum, DE.
D. Page, University of Bristol, UK.
E. Peeters, Texas Instruments, US.
A. Poschmann, Nanyang Technological University, SG.
E. Prouff, ANSSI, FR.
F. Regazzoni, ALaRI, Lugano, CH.
M. Rivain, CryptoExperts, FR.
M. Robshaw, Impinj, Inc., US.
A.-R. Sadeghi, Technische Universität Darmstadt /CASED, DE.
K. Sakiyama, University of Electro-Communications, JP.
A. Satoh, University of Electro-Communications, JP.
P. Schaumont, Virginia Tech, US.
P. Schwabe, Radboud University Nijmegen, NL.
D. Suzuki, Mitsubishi Electric, JP.
M. Tibouchi, NTT Secure Platform Laboratories, JP.
I. Verbauwhede, KU Leuven, BE.
B.-Y. Yang, Academia Sinica, TW.

Any enquiries should be sent to Lejla Batina and Matt Robshaw at `ches2014programchairs@iacr.org`.