Workshop on Cryptographic Hardware and Embedded Systems (CHES)

Saint-Malo, France – September 13-16, 2015

Call for Papers

The annual CHES workshop highlights new results in the design and analysis of cryptographic hardware and software implementations. The workshop builds a valuable bridge between the research and cryptographic engineering communities and attracts participants from industry, academia, and government organizations. In addition to a single track of high-quality presentations, CHES 2015 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 of the reviews before the final decisions are made. Topics suitable for CHES 2015 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. *All submissions must follow Springer's LNCS format with a total page limit of 18 pages excluding references.* Supplementary materials may be appended without a page limit, but reviewers are neither required to read them nor will they be printed in the proceedings. Hence papers must be intelligible and self-contained within the 18 page bound. 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; see the IACR Policy on Irregular Submissions (`www.iacr.org/irregular.html`). Note that any submission to CHES 2015 implies the full acknowledgment and commitment of authors to the entire review process; a withdrawal of any paper prior to the notification deadline will be accepted only in exceptional cases (i.e., severe technical flaws discovered after the submission deadline).

Details of the electronic submission procedure will be posted on the conference web-page. The final proceedings of CHES 2015 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 2015 to present the paper.

- *Submission deadline:* ***March 2, 2015, 23:59 PST***
- *Referee comments to authors: April 17, 2015*
- *Author response to comments: April 24, 2015*
- *Paper notification: May 18, 2015*
- *Final version due: June 15, 2015*
- *Workshop dates: September 13 – 16, 2015*

Poster and Tutorial Sessions

CHES 2015 will include a poster session and the *Call for Posters* is available via the conference web-page. The program co-chairs also welcome proposals for half-day tutorials at CHES 2015. The presenter of an accepted proposal will be offered a complimentary registration to CHES 2015 and a fixed stipend towards their travel costs. More details will be available via the CHES 2015 conference web-page.

Program Committee

O. Aciiçmez, Samsung Research America, US.
L. Batina, Radboud University Nijmegen, NL.
D. Bernstein, University of Illinois at Chicago, US, and Technische Universiteit Eindhoven, NL.
G. Bertoni, STMicroelectronics, IT.
C.-M. Cheng, National Taiwan University, TW.
J.-S. Coron, University of Luxembourg, LU.
E. De Mulder, Cryptography Research, FR.
T. Eisenbarth, Worcester Polytechnic Institute, US.
J. Fan, Open Security Research and Neutron Security Inc., CN.
W. Fischer, Infineon Technologies, DE.
P.-A. Fouque, Université Rennes 1 and Institut Universitaire de France, FR.
K. Gaj, George Mason University, US.
B. Gierlichs, KU Leuven, BE.
L. Goubin, University of Versailles, FR.
T. Güneysu, Ruhr-Universität Bochum, DE.
H. Handschuh, Cryptography Research, US, and KU Leuven, BE.
N. Homma, Tohoku University, JP.
M. Hutter, Cryptography Research, US.
M. Joye, Technicolor, US.
I. Kizhvatov, Riscure, NL.
F. Koeune, Université Catholique de Louvain, BE.
K. Lemke-Rust, Bonn-Rhein-Sieg University of Applied Sciences, DE.
R. Maes, Intrinsic-ID, NL.
M. Medwed, NXP Semiconductors, AT.
A. Moradi, Ruhr-Universität Bochum, DE.
C. Paar, Ruhr-Universität Bochum, DE.
D. Page, University of Bristol, UK.
E. Peeters, Texas Instruments, US.
A. Poschmann, NXP Semiconductors, DE.
B. Preneel, KU Leuven, BE.
E. Prouff, ANSSI, FR.
F. Regazzoni, ALaRI-USI, CH.
M. Rivain, CryptoExperts, FR.
M. Robshaw, Impinj, US.
U. Rührmair, Technical University Munich, DE.
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.
A. Tria, CEA-TECH, FR.
M. Tunstall, Cryptography Research, US.
M.-D. Yu, Verayo, US and KU Leuven, BE.

All correspondence and questions should be directed to the program co-chairs Helena Handschuh and Tim Güneysu at `ches2015programchairs@iacr.org`.