Conference on Cryptographic Hardware and Embedded Systems (CHES)

Taipei, Taiwan – September 25-28, 2017

Call for Papers

The annual CHES conference 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 2017 will offer invited talks, tutorials, a poster session, and a rump session. Program committee members are allowed to submit one paper, and a second one if both submissions are co-authored. All submitted papers will be reviewed by at least four Program Committee members. Any Program Committee member submission will be reviewed by at least five Program Committee members. Program chairs are not allowed to submit. Authors will be invited to submit brief rebuttals of the reviews before the final decisions are made. Topics suitable for CHES 2017 include, but are not limited to:

Cryptographic implementations

- *Hardware architectures*
- *Cryptographic processors and co-processors*
- *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*
- *White-box cryptography and code obfuscation*
- *Hardware and software reverse engineering*

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 and security for the Internet of Things (RFID, sensor networks, smart devices, smart meters, etc.)*
- *Hardware IP protection and anti-counterfeiting*
- *Reconfigurable hardware for cryptography*
- *Smart card processors, systems and applications*
- *Security for cyberphysical systems (home automation, medical implants, industrial control, etc.)*
- *Automotive security*
- *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, acknowledgements, or obvious references (this includes metadata hidden in the files). Papers should begin with a title, a short abstract, and a list of keywords. *All submissions must follow Springer's LNCS format* (`http://www.springer.com/computer/lncs/lncs+authors`) *without changing default margins, fonts, etc. The total page limit is 18 pages excluding references.* Supplementary materials that facilitate verification of the results, e.g., source code, proof details, etc., may be appended without a page limit or uploaded as separate files, but reviewers are neither required to read them nor will they be printed in the proceedings. Hence submissions must be complete, intelligible and self-contained within the 18 pages bound. Papers should have page numbers to facilitate their review. In LaTeX, this can be achieved for instance using `\pagestyle{plain}`.

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 (`https://www.iacr.org/docs/irregular.pdf`) and the Guidelines for Authors (`https://www.iacr.org/docs/author.pdf`). Note that any submission to CHES 2017 implies the full acknowledgement 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 website. The final proceedings of CHES 2017 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 2017 to present the paper. Furthermore, with their submission, the authors agree that the presentation will be video taped by IACR. For more information please regard `https://www.iacr.org/docs`.

Conflicts of Interest

The program co-chairs invite authors to help preventing submissions from being evaluated by reviewers who have a conflict of interest. CHES follows the rules and guidelines of IACR with respect to identifying conflicts of interest. During submission to CHES 2017 authors must declare any conflict of interest with Program Committee members that might influence an impartial judgment of their submission. A conflict of interest exists for example if an author and a Program Committee member:

- have a currently ongoing research collaboration
- have been affiliated to the same institution in the last 3 years
- have been in a student-advisor relationship in the last 5 years
- have jointly published more than one paper in the last 3 years
- have personal ties (family, friends, etc.).

For co-authored submissions a conflict of interest exists if at least one co-author has a conflict of interest.

Important Dates

- *Submission deadline:* ***March 17, 2017, 23:59 PST***
- *Referee comments to authors: May 12, 2017*
- *Author response to comments: May 19, 2017*
- *Paper notification: June 06, 2017*
- *Final version due: June 26, 2017*
- *Workshop dates: September 25 – 28, 2017*

Poster and Tutorial Sessions

CHES 2017 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 2017. The presenter of an accepted proposal will be offered a complimentary registration to CHES 2017 and a fixed stipend towards their travel costs. More details will be available via the CHES 2017 conference web-page.

Program Committee

D. Aranha, University of Campinas, BR

J. Balasch, KU Leuven, BE

L. Batina, Radboud University, NL

O. Benoit , Qualcomm Technologies, Inc., US

D. J. Bernstein, University of Illinois at Chicago and Technische Universiteit Eindhoven, US

G. Bertoni, STMicroelectronics, IT

T. Chou, Technische Universiteit Eindhoven, NL

C. Clavier, Universit de Limoges, FR

E. De Mulder, Rambus, Cryptography Research Division, US

H. Drexler, Giesecke & Devrient, DE

Th. Eisenbarth, Worcester Polytechnic Institute, US

J. Fan, Open Security Research, CN

V. Fischer, Hubert Curien Laboratory, University of Lyon, FR

W. Fischer, Infineon Technologies, DE

P.-A. Fouque, Universit de Rennes 1, FR

B. Gammel, Infineon Technologies, DE

B. Gierlichs, KU Leuven, BE

C. Giraud, Oberthur Technologies, FR

J. Guajardo, Robert Bosch LLC, US

S. Guilley, TELECOM-ParisTech and Secure-IC, FR

T. Güneysu, University of Bremen & DFKI, DE

J. Heyszl, Fraunhofer AISEC, DE

N. Homma, Tohoku University, JP

É. Jaulmes, ANSSI, FR

M. Joye, NXP Semiconductors, US

F. Koeune, Université catholique de Louvain, BE

Y. Komano, Toshiba, JP

K. Lemke-Rust, Bonn-Rhein-Sieg University of Applied Sciences, DE

T. Lepoint, SRI International, US

Y. Li, Nanjing University of Aeronautics and Astronautics, CN

V. Lomné, LIRMM/University of Montpellier, FR

P. Maistri, TIMA Laboratory, FR

M. Matsui, Mitsubishi Electric, JP

M. Medwed, NXP Semiconductors Austria GmbH, AT

A. Moradi, Ruhr-Universität Bochum, DE

D. Mukhopadhyay, Indian Institute of Technology Kharagpur, IN

D. Oswald, School of Computer Science, The University of Birmingham, GB

D. Page, University of Bristol, UK

F. Regazzoni, ALaRI - USI, CH

M. Rivain, CryptoExperts, FR

E. Savaş, Sabanci University, TR

P. Schaumont, Virginia Tech, US

J.-M. Schmidt, Secunet, DE

S. Skorobogatov, University of Cambridge, UK

M. Stöttinger, Continental Teves, DE

M. Tibouchi, NTT Secure Platform Laboratories, JP

M. Tunstall, Cryptography Research, GB

A. Weimerskirch, Lear Corporation, US

B. Wyseur, Kudelski Security, CH

D. Yamamoto, Fujitsu Laboratories Ltd., JP

All correspondence and questions should be directed to the program co-chairs Wieland Fischer and Naofumi Homma at `ches2017programchairs@iacr.org`.