Cryptographic Hardware and Embedded Systems (CHES)

CHES 2020, Beijing, China, September 14–17, 2020

IACR Transactions on CHES (TCHES), Volume 2020, Issues 1–4

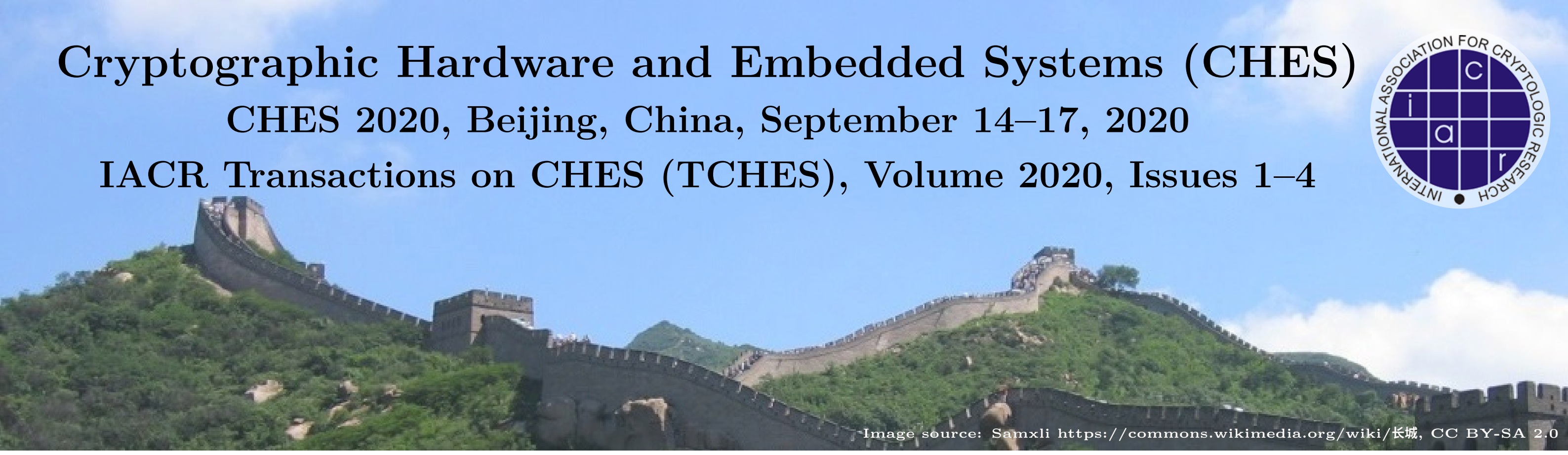

Image source: Samxli https://commons.wikimedia.org/wiki/长城, CC BY-SA 2.0

Call for Papers

Having been established in 1999, the Cryptographic Hardware and Embedded Systems (CHES) conference is the premier venue for research on design and analysis of cryptographic hardware and software implementations. As an area conference of the International Association for Cryptologic Research (IACR), CHES bridges the cryptographic research and engineering communities, and attracts participants from academia, industry, government and beyond.

CHES 2020 will take place in Beijing, China, September 14–17, 2020. The conference website is accessible at

`https://ches.iacr.org/2020`

The scope of CHES is intentionally diverse. We solicit submission of papers on topics including, but not limited to, the following:

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 and software

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

Publication Model

As of 2018, CHES has moved to an open-access journal/conference hybrid model. Following the success of similar initiatives at analogous events such as FSE, this decision was made (by the CHES steering committee) as a means of improving review and publication quality while retaining the highly successful, community-focused nature of the event. A comprehensive set of FAQs relating to the model can be found via the TCHES website at

`https://tches.iacr.org/index.php/TCHES/faq`

In summary:

1. Submitted papers will undergo a journal-style review process, with accepted papers published in the following issue of the *IACR Transactions on Cryptographic Hardware and Embedded Systems* (TCHES), a journal published by Ruhr-University Bochum. TCHES is a Gold Open Access publication, and as such, all TCHES papers are immediately and freely available.

2. The annual CHES conference consists of presentations for each paper published in the associated issues of TCHES, plus invited talks and a range of additional and social activities.

3. TCHES has four submission deadlines per year; all papers accepted for publication in TCHES between 15 July of year $n - 1$ and 15 July of year n will be presented at CHES of year n.

Timeline

The upcoming deadlines of CHES 2020 are as follows:

- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2020, Issue 1
  - Submission: **15 July 2019**
  - Rebuttal: 22–26 August 2019
  - Notification: 15 September 2019
  - Camera-ready: 14 October 2019
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2020, Issue 2
  - Submission: **15 October 2019**
  - Rebuttal: 21–25 November 2019
  - Notification: 15 December 2019
  - Camera-ready: 14 January 2020
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2020, Issue 3
  - Submission: **15 January 2020**
  - Rebuttal: 20–24 February 2020
  - Notification: 15 March 2020
  - Camera-ready: 14 April 2020
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2020, Issue 4
  - Submission: **15 April 2020**
  - Rebuttal: 21–25 May 2020
  - Notification: 15 June 2020
  - Camera-ready: 14 July 2020

Camera-ready deadlines apply to accepted and conditionally accepted papers. Both submission and camera-ready deadlines are set at 23:59 Anywhere on Earth (AoE).

Instructions for Authors

1. Submission

To submit a paper to TCHES, follow the instructions available at:

`https://tches.iacr.org/index.php/TCHES/submission`

2. Format

A paper submitted to TCHES must be written in English and be anonymous, with no author names, affiliations, acknowledgments, or any identifying citations. It should begin with a title, a short abstract, and a list of keywords. The introduction should summarize the contributions of the paper at a level appropriate for a non-specialist reader. Submissions should be typeset in the LaTeX style available at

`https://tches.iacr.org/index.php/TCHES/latex`

In particular, TCHES only accepts electronic submissions in PDF format.

TCHES accepts two forms of paper, termed short and long; the page limit (excluding bibliography) is 20 and 40 pages respectively. In either case, authors are encouraged to include supplementary material needed to validate the content (e.g., test vectors or source code) as an appendix: this material will not be included in the page count. In allowing long papers, the goal is to support cases where extra detail (e.g., proofs, or experimental results) is deemed essential. Authors should highlight long papers by annotating the title with “(Long Paper)”, and be aware the review process may take longer: a decision may, at the discretion of the editors-in-chief(s), be deferred to the subsequent volume.

3. Regulations

The review process for TCHES, Volume 2020, Issues 1–4, will be governed by the following regulations:

- Members of the TCHES editorial board may submit one new paper per deadline (co-authored or otherwise); editor(s)-in-chief may not submit papers during their tenure.
- TCHES follows IACR policy, i.e.,

  `https://www.iacr.org/docs/irregular.pdf`

  with respect to irregular submissions: any submission deemed to be irregular (e.g., which has been submitted, in parallel, to another conference with proceedings), will be instantly rejected.
- TCHES follows IACR policy with respect to conflicts of interest that could prevent impartial review. A conflict of interest is considered to occur whenever one (co-)author of a submitted paper and a TCHES editorial board member
  - were advisee/advisor at any time,
  - have been affiliated to the same institution in the past 2 years,
  - have published 2 or more jointly authors papers in the past 3 years,
  - are immediate family members,
  - have a current, ongoing research collaboration (e.g., are members of the same research project).

  IACR reserves the right to share information about submissions with other program committees and editorial boards to ensure strict enforcement of the policy.
- At the time of submission, authors are **required** to
  1. make a declaration regarding any conflicts of interest, and
  2. guarantee they will deliver a presentation at the associated CHES conference if their submission is accepted for publication in TCHES.
- Each paper will be double-blind reviewed by at least four members of the TCHES editorial board.
- In order to improve the quality of the review process, authors are given the opportunity to submit a rebuttal after receiving the associated reviews.
- The review process outcome is either an outright accept or reject decision, or one of two deferred decision types. Specifically, "minor revision" means the paper is conditionally accepted, and assigned a shepherd to verify the revision is adequate, "major revision" means the authors are invited to revise and resubmit their article to one of the following two submission deadlines, otherwise any re-submission will be treated as new.
- To ensure consistency, the reviewers assigned for a revised paper are ideally the same as for the original.
- Authors of submitted papers are also highly encouraged to check the TCHES FAQ

  `https://tches.iacr.org/index.php/TCHES/faq`

  for answers to questions related to policy and procedures governing CHES

Contacts

1. Program Co-Chairs / Co-Editors-in-Chief

4.1.1 Current (i.e., for CHES 2020)

Amir Moradi
Ruhr University Bochum, DE

Mehdi Tibouchi
NTT Corporation, JP

`ches2020programchairs@iacr.org`

2. General Co-Chairs

Liji Wu
Tsinghua University, CN

Guoqiang Bai
Tsinghua University, CN

Zhe Liu
Nanjing University of Aeronautics & Astronautics, CN

Junfeng Fan
Open Security Research, Inc., CN

`ches2020@iacr.org`

3. Managing Editor

4. Program Committee/Editorial Board

Srinivas Vivek	Institute of Information Technology, Bangalore	IN
Christine van Vredendaal	NXP Semiconductors	NL
Bo-Yin Yang	Academia Sinica	TW
Yuval Yarom	University of Adelaide and Data61	AU