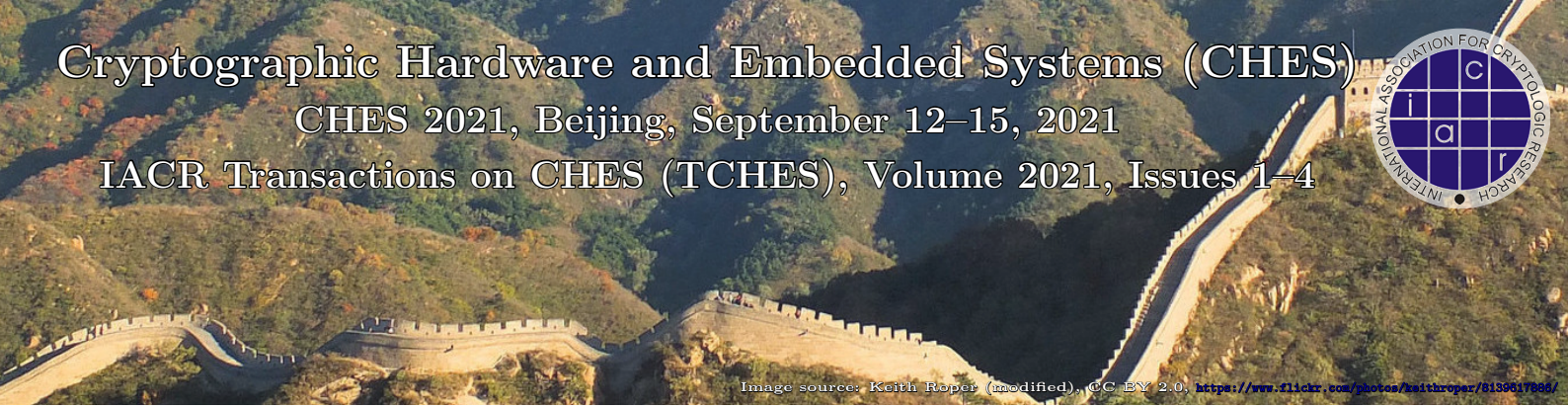

Call for Papers

Having been established in 1999, the Cryptographic Hardware and Embedded Systems (CHES) conference is the premier venue for research on both 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 2021 will take place in Beijing, China, September 12–15, 2021. The conference website is accessible at

https://ches.iacr.org/2021

The scope of CHES is intentionally diverse, meaning 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
- Micro-architectural side-channel attacks
- 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
- High-assurance crypto
- Verification methods and tools for secure design
- Domain-specific languages for cryptographic systems
- Metrics for the security of embedded systems
- Secure programming techniques
- FPGA design security

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
- Smartcard processors, systems, and applications
- Security for cyberphysical systems (home automation, medical implants, industrial-control systems, etc.)
- Automotive security
- Secure storage devices (memories, disks, etc.)
- Technologies for content protection
- Trusted computing platforms

Hybrid 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 event. A comprehensive set of FAQs relating to the model can be found via the TCHES website at

https://tches.iacr.org

In summary:

1. Submitted papers will undergo a journal-style review process, with accepted papers published by Ruhr University Bochum in an issue of the journal IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES). Since it has a Gold Open Access status, all papers published in TCHES 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

Upcoming deadlines relating to CHES 2021 are as follows:

- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2021, Issue 1
  - Submission: **15 July 2020**
  - Rebuttal: 17–21 August 2020
  - Notification: 15 September 2020
  - Camera-ready: 14 October 2020
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2021, Issue 2
  - Submission: **15 October 2020**
  - Rebuttal: 16–20 November 2020
  - Notification: 15 December 2020
  - Camera-ready: 14 January 2021
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2021, Issue 3
  - Submission: **15 January 2021**
  - Rebuttal: 15–19 February 2021
  - Notification: 15 March 2021
  - Camera-ready: 14 April 2021
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2021, Issue 4
  - Submission: **15 April 2021**
  - Rebuttal: 17–21 May 2021
  - Notification: 15 June 2021
  - Camera-ready: 14 July 2021

The camera-ready deadline relates to accepted and conditionally accepted papers. *All* deadlines are 23:59:59 Anywhere on Earth (AoE).

Instructions for Authors

1. Format

A paper submitted to TCHES must be written in English and be anonymous, with no author names, affiliations, acknowledgements, or any identifying citations. It should begin with a title, a short abstract, and a list of keywords. The introduction should summarise 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/submission,

noting that TCHES only accepts electronic submission 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. Long papers need to be marked as such by checking the respective box in the submission system. Authors of long papers should be aware that the review process may take longer: a decision may, at the discretion of the editors-in-chief(s), be deferred to the subsequent volume.

2. Regulations

The review process for TCHES, Volume 2021, Issues 1–4, will be governed by the following regulations:

- There are no longer restrictions on the number of papers members of the TCHES editorial board may submit 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. IACR reserves the right to share information about submissions with other program committees and editorial boards to ensure strict enforcement of the policy.

- TCHES follows IACR policy with respect to conflicts of interest that could prevent impartial review. A conflict of interest is considered to occur automatically 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 authored papers in the past 3 years, or
  - are immediate family members.

  For an interpretation of the above reasons, please refer to the IACR policy on CoIs (https://www.iacr.org/docs/conflicts.pdf). Note that conflicts may also arise for reasons other than those just listed. Examples include closely related technical work, cooperation in the form of joint projects or grant applications, business relationships, close personal friendships, instances of personal enmity.

- Full transparency is of utmost importance, authors and reviewers must disclose to the chairs or editor any circumstances that they think may create bias, even if it does not raise to the level of a CoI. At the time of submission, authors are **required** to

  1. make a declaration regarding any conflicts of interest (including reasons for the conflict), 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 (between the indicated dates) 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 submit a revision of their article to one of the following two submission deadlines; a later re-submission will be treated as a new paper.

- When submitting a major revision, follow the instructions in the submission system to indicate that the paper is a major revision and to provide the ID of the earlier submission.

- To ensure consistency, the reviewers assigned for a revised paper are ideally the same as for the original.

- Resubmission of papers that have previously been rejected from TCHES is only allowed after major modifications and approval by the Editors-in-Chief prior to submission.

- 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 2021)

Elke De Mulder
Rambus Cryptography Research, USA

Peter Schwabe
Radboud University, NL

ches2021programchairs@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

ches2021@iacr.org

3. Managing Editor

Tim Güneysu
Ruhr University Bochum

tches-managing-editor@iacr.org

4. Program Committee/Editorial Board

Diego F. Aranha	Aarhus University, Denmark
Manuel Barbosa	University of Porto (FCUP) & INESC TEC, Portugal
Sonia Belaïd	CryptoExperts, France
Benjamin Beurdouche	Mozilla, France
Begül Bilgin	Rambus Cryptography Research, The Netherlands
Billy Bob Brumley	Tampere University, Finland
Chris Brzuska	Aalto University, Finland
Ileana Buhan	Riscure B.V., The Netherlands
Rajat Subhra Chakraborty	IIT Kharagpur, India
Tung Chou	Academia Sinica, Taiwan
Chitchanok Chuengsatiansup	The University of Adelaide, Australia
Jeroen Delvaux	Open Security Research, China
François Dupressoir	University of Bristol, UK
Stefan Dziembowski	University of Warsaw, Poland
Barış Ege	Riscure B.V., The Netherlands
Fatemeh Ganji	University of Florida, USA
Daniel Genkin	University of Michigan, USA
Benedikt Gierlichs	KU Leuven, Belgium
Dahmun Goudarzi	PQShield, UK
Hannes Gross	SGS Digital Trust Services, Austria
Dong-Guk Han	Kookmin University, South Korea
Annelie Heuser	Université de Rennes, Inria, CNRS, IRISA, France
Xiaolu Hou	Nanyang Technological University, Singapore
Andreas Hülsing	Eindhoven University of Technology, The Netherlands
Elif Bilge Kavun	The University of Sheffield, UK
Boris Köpf	Microsoft Research, UK
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Tancrède Lepoint	Google, USA
Patrick Longa	Microsoft Research, USA
Julio López	University of Campinas, Brazil
Marco Macchetti	Kudelski Group, Switzerland
Stefan Mangard	Graz University of Technology, Austria
Nele Mentens	Leiden University, The Netherlands & KU Leuven, Belgium
Elke De Mulder	Rambus Cryptography Research, USA
Ruben Niederhagen	Fraunhofer SIT, Germany
David Oswald	The University of Birmingham, UK
Colin O'Flynn	Dalhousie University, Canada
Daniel Page	University of Bristol, UK
Peter Pessl	Infineon Technologies, Germany
Stjepan Picek	TU Delft, The Netherlands
Thomas Pornin	NCC Group, Canada
Thomas Pöppelmann	Infineon Technologies, Germany
Francesco Regazzoni	University of Amsterdam, The Netherlands & ALaRI - USI, Switzerland
Francisco Rodríguez-Henríquez	CINVESTAV, Mexico

Kazuo Sakiyama	The University of Electro-Communications, Japan
Pascal Sasdrich	Ruhr University Bochum, Germany
Tobias Schneider	NXP Semiconductors, Austria
Peter Schwabe	Radboud University, The Netherlands
Martijn Stam	Simula UiB, Norway
Marc Stöttinger	Continental AG, Germany
Takeshi Sugawara	The University of Electro-Communications, Japan
Petr Svenda	Masaryk University, Czech Republic
Adrian Thillard	Ledger, France
Mehdi Tibouchi	NTT Corporation, Japan
Yosuke Todo	NTT Corporation, Japan
Gilles Van Assche	STMicroelectronics, Belgium
Srinivas Vivek	IIIT Bangalore, India
Christine van Vredendaal	NXP Semiconductors, The Netherlands
Bo-Yin Yang	Academia Sinica, Taiwan
Bohan Yang	Tsinghua University, China
Yuval Yarom	The University of Adelaide & Data61, Australia