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 2022 will take place in Leuven, Belgium, on September 18-21, 2022. The conference website is accessible at https://ches.iacr.org/2022

The scope of CHES is intentionally diverse, meaning we solicit submission of papers on topics including, but not limited to, the following (with new topics for CHES 2022 highlighted in bold blue):

**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 counter-measures:**
- 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:**
- **Formal methods for secure hardware and software**
- 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:**
- Quantum cryptanalysis
- Algorithm subversion and subversion prevention
- New and emerging cryptographic algorithms and protocols targeting embedded devices
- Special-purpose hardware for cryptanalysis
- Leakage-resilient cryptography

**Applications:**
- RISC-V security
- Trusted execution environments and trusted computing platforms
- 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

**TCHES Publication Model**

CHES has transitioned to an open-access journal/conference hybrid model. A comprehensive list 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. 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

TCHES has four submission deadlines per year; Upcoming deadlines relating to CHES 2022 are as follows:

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2022, Issue 1**
  - Submission: **15 July 2021**
  - Rebuttal: 23–27 August 2021
  - Notification: 15 September 2021
  - Camera-ready: 14 October 2021

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2022, Issue 2**
  - Submission: **15 October 2021**
  - Rebuttal: 22–26 November 2021
  - Notification: 15 December 2021
  - Camera-ready: 14 January 2022

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2022, Issue 3**
  - Submission: **15 January 2022**
  - Rebuttal: 21–25 February 2022
  - Notification: 15 March 2022
  - Camera-ready: 14 April 2022

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2022, Issue 4**
  - Submission: **15 April 2022**
  - Rebuttal: 23–27 May 2022
  - Notification: 15 June 2022
  - Camera-ready: 14 July 2022

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, 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/submission](https://tches.iacr.org/index.php/TCHES/submission), noting that TCHES only accepts electronic submission in PDF format. Please use the submission mode `\documentclass[submission]{iacrtrans}` that displays line numbers to ease the review process.

TCHES accepts two forms of paper, termed short and long; the page limit (excluding bibliography) is 20 and 40 pages respectively. Authors are encouraged to include additional supplementary material needed to validate the content (e.g., test vectors or source code) as separate files. In order to ensure that appendices are also reviewed, they need to be included before the bibliography within the 20 or 40-page limit during submission. 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 and by annotating the title with *Long Paper*. Authors need to justify the need to submit the content as long paper in a justification letter included in the supplementary materials. Long papers submitted without proper justification will be returned without review. Authors of long papers should be aware that the review process may take longer: a decision may, at the discretion of the editor(s)-in-chief, be deferred to the subsequent volume.
TCHES solicits submission of Systematization of Knowledge (SoK) papers, i.e., papers whose goal is to review and contextualize existing literature in a particular area in order to systematize existing knowledge. To be considered for publication, SoK papers must provide significant added value beyond prior work, such as novel insights or reasonably questioning previous assumptions. Authors should highlight SoK papers by annotating the title with “SoK.”

2. Regulations
The review process for TCHES, Volume 2022, Issues 1–4, will be governed by the following regulations:

- 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 submission.

- 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

Sonia Belaïd
CryptoExperts, FR
ches2022programchairs@iacr.org

Thomas Eisenbarth
University of Lübeck, DE

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

ches2022@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

Aydin Aysu
North Carolina State University, USA

Gustavo Banegas
Inria and Institut Polytechnique de Paris, France

Manuel Barbosa
University of Porto (FCUP) & INESC TEC, Portugal

Sonia Belaïd
CryptoExperts, France

Sebastian Berndt
University of Lübeck, Germany

Benjamin Beurdouche
Mozilla, France

Shivam Bhasin
Temasek Labs, Nanyang Technological University, Singapore

Xavier Bonnetain
University of Waterloo, Canada

Billy Bob Brumley
Tampere University, Finland

Chris Brzuska
Aalto University, Finland

Ileana Buhan
Radboud University, The Netherlands

Eleonora Cagli
CEA-Leti, Université Grenoble Alpes, France

Rajat Subhra Chakraborty
IIT Kharagpur, India

Jean-Sébastien Coron
University of Luxembourg, Luxembourg

Lauren De Meyer
Rambus Cryptography Research, The Netherlands

Elke De Mulder
Rambus Cryptography Research, USA

Thomas Eisenbarth
University of Lübeck, Germany

Thomas Espitau
NTT Corporation, Japan

Fatemeh Ganji
Worcester Polytechnic Institute, USA

Benedikt Gierlichs
KU Leuven, Belgium

Aron Gohr
BSI, Germany

Annelie Heuser
University of Rennes, CNRS, IRISA

Xiaolu Hou
Slovak University of Technology, Slovakia

Marc Joye
Zama, France

Elif Bilge Kavun
University of Passau, Germany

Julio López
University of Campinas, Brazil

Stefan Mangard
Graz University of Technology, Austria

Pierrick Méaux
UCLouvain, Belgium

Florian Mendel
Infineon, Germany

Nele Mentens
Leiden University, The Netherlands & KU Leuven, Belgium

Daniel Moghimi
University of California San Diego, USA

Ruben Niederhagen
University of Southern Denmark, Denmark
<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colin O'Flynn</td>
<td>NewAE Technology Inc, Canada</td>
</tr>
<tr>
<td>David Oswald</td>
<td>The University of Birmingham, UK</td>
</tr>
<tr>
<td>Elisabeth Oswald</td>
<td>Alpen-Adria Universität, Austria</td>
</tr>
<tr>
<td>Daniel Page</td>
<td>University of Bristol, UK</td>
</tr>
<tr>
<td>Kenneth Paterson</td>
<td>ETH Zurich, Switzerland</td>
</tr>
<tr>
<td>Stepan Picek</td>
<td>Radboud University and TU Delft, The Netherlands</td>
</tr>
<tr>
<td>Axel Poschmann</td>
<td>xen1thLabs, UAE</td>
</tr>
<tr>
<td>Oscar Reparaz</td>
<td>Cash App (at Square), USA and KU Leuven, Belgium</td>
</tr>
<tr>
<td>Matthieu Rivain</td>
<td>CryptoExperts, France</td>
</tr>
<tr>
<td>Thomas Roche</td>
<td>NinjaLab, France</td>
</tr>
<tr>
<td>Francisco Rodríguez-Henríquez</td>
<td>Technology Innovation Institute and Cinvestav, Mexico</td>
</tr>
<tr>
<td>Mélissa Rossi</td>
<td>ANSSI, France</td>
</tr>
<tr>
<td>Ahmad Sadeghi</td>
<td>TU Darmstadt, Germany</td>
</tr>
<tr>
<td>Kazuo Sakiyama</td>
<td>The University of Electro-Communications, Japan</td>
</tr>
<tr>
<td>Pascal Sasdrich</td>
<td>Ruhr University Bochum, Germany</td>
</tr>
<tr>
<td>Patrick Schaumont</td>
<td>Worcester Polytechnic Institute, USA</td>
</tr>
<tr>
<td>Georg Sigl</td>
<td>Technical University of Munich and Fraunhofer AISEC, Germany</td>
</tr>
<tr>
<td>François-Xavier Standaert</td>
<td>UCLouvain, Belgium</td>
</tr>
<tr>
<td>Rainer Steinwandt</td>
<td>University of Alabama in Huntsville, USA</td>
</tr>
<tr>
<td>Takeshi Sugawara</td>
<td>The University of Electro-Communications, Japan</td>
</tr>
<tr>
<td>Petr Svenda</td>
<td>Masaryk University, Czech Republic</td>
</tr>
<tr>
<td>Jakub Szefer</td>
<td>Yale, USA</td>
</tr>
<tr>
<td>Adrian Thillard</td>
<td>Ledger, France</td>
</tr>
<tr>
<td>Yosuke Todo</td>
<td>NTT Corporation, Japan</td>
</tr>
<tr>
<td>Meltem Sönmez Turan</td>
<td>National Institute of Standards and Technology, USA</td>
</tr>
<tr>
<td>Alexandre Venelli</td>
<td>NXP Semiconductors, France</td>
</tr>
<tr>
<td>Christine van Vredendaal</td>
<td>NXP Semiconductors, The Netherlands</td>
</tr>
<tr>
<td>Junwei Wang</td>
<td></td>
</tr>
<tr>
<td>Wenjie Xion</td>
<td>Virginia Tech, USA</td>
</tr>
<tr>
<td>Bo-Yin Yang</td>
<td>Academia Sinica, Taiwan</td>
</tr>
<tr>
<td>Bohan Yang</td>
<td>Tsinghua University, China</td>
</tr>
<tr>
<td>Yuval Yarom</td>
<td>The University of Adelaide, Australia</td>
</tr>
<tr>
<td>Yu Yu</td>
<td>Shanghai Jiao Tong University, China</td>
</tr>
<tr>
<td>Fan (Terry) Zhang</td>
<td>Zhejiang University, China</td>
</tr>
</tbody>
</table>