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 2023 will take place in Prague, Czech Republic, in September 2023. The conference website is accessible at https://ches.iacr.org/2023

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 2023 highlighted in bold blue):

Cryptographic implementations:
- Hardware architectures
- Cryptographic processors and coprocessors
- True and pseudorandom number generators
- Physical unclonable functions (PUFs)
- Efficient software implementations

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, including quantum circuits
- Leakage resilient cryptography

Attacks against implementations, and countermeasures:
- Remote, micro-architectural and physical side-channel attacks and countermeasures
- Fault attacks and countermeasures
- Hardware tampering and tamper-resistance
- White-box cryptography and code obfuscation
- Reverse engineering of hardware/software

Applications:
- RISC-V security
- Trusted execution environments and trusted computing platforms
- IP protection for hardware/software and technologies for anti-counterfeiting
- Reconfigurable hardware for cryptography
- Secure elements, security subsystems, and applications
- Security for the Internet of Things and cyberphysical systems (RFID, sensor networks, smart meters, medical implants, smart devices for home automation, industrial control, automotive, etc.)
- Secure storage devices (memories, disks, etc.)
- Isolation and monitoring hardware for cyber-resilience
- Engineering of zero-knowledge proof systems
- Privacy-preserving computing in practice (MPC, FHE)

Tools and methodologies:
- Formal methods, techniques and tools for secure design and verification for hardware/software
- Computer aided cryptographic engineering
- Domain-specific languages for cryptographic systems
- Metrics for the security of embedded systems
- FPGA design security

Systematization of Knowledge (SoK)

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 2023 are as follows:

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2023, Issue 1**
  - Submission: **15 July 2022**
  - Rebuttal: 22–26 August 2022
  - Notification: 15 September 2022
  - Camera-ready: 14 October 2022

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2023, Issue 2**
  - Submission: **15 October 2022**
  - Rebuttal: 21–25 November 2022
  - Notification: 15 December 2022
  - Camera-ready: 14 January 2023

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2023, Issue 3**
  - Submission: **15 January 2023**
  - Rebuttal: 20–24 February 2023
  - Notification: 15 March 2023
  - Camera-ready: 14 April 2023

- **IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2023, Issue 4**
  - Submission: **15 April 2023**
  - Rebuttal: 22–26 May 2023
  - Notification: 15 June 2023
  - Camera-ready: 14 July 2023

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,

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 regular 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 2023, 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

Diego F. Aranha  
Aarhus University, DK  
ches2023programchairs@iacr.org

Marcel Medwed  
NXP Semiconductors, AT

2. General Co-Chairs

Hana Kubátová  
Czech Technical University in Prague, CZ

ches2023@iacr.org

3. Artifact Chair

Peter Schwabe  
MPI-SP, DE & Radboud University, NL

ches2023artifacts@iacr.org

4. Managing Editor

Tim Güneysu  
Ruhr University Bochum, DE

tches-managing-editor@iacr.org

5. Program Committee/Editorial Board

Diego F. Aranha  
Aarhus University, Denmark

Aydin Aysu  
North Carolina State University, USA

Gustavo Banegas  
Qualcomm, France

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

Lejla Batina  
Radboud University, The Netherlands

Sebastian Berndt  
University of Lübeck, Germany

Benjamin Beurdouche  
Mozilla, France

Shivam Bhasin  
Nanyang Technological University, Singapore

Nina Bindel  
Sandbox AQ, USA

Estuardo Alpirez Bock  
Xiphera, Finland

Eleonora Cagli  
CEA-Leti, Université Grenoble Alpes, France

Rajat Subhra Chakraborty  
IIT Kharagpur, India

Jesús-Javier Chi-Domínguez  
Technology Innovation Institute, UAE

Marios Omar Choudary  
University Politehnica of Bucharest, Romania

Chitchanok Chuengsatiansup  
University of Adelaide, Australia

Wei Dai  
TikTok, USA

Lauren De Meyer  
Rambus Cryptography Research, The Netherlands

Christoph Dobraunig  
Intel Labs, USA

Cécile Dumas  
CEA-Leti, Université Grenoble Alpes, France

Thomas Espitau  
NTT Corporation, Japan

Fatemeh Ganji  
Worcester Polytechnic Institute, USA

François Gérard  
University of Luxembourg, Luxembourg

Aron Gohr  
Independent Researcher, Germany

Johann Heyszl  
Google LLC, Germany

Xiaolu Hou  
Slovak University of Technology, Slovakia

Andreas Hütting  
Eindhoven University of Technology, The Netherlands

Michael Hutter  
PQShield Ltd., Austria

Matthias Kannwischer  
Academia Sinica, Taiwan

Marcel Keller  
CSIRO Data61, Australia

Elif Bilge Kavun  
University of Passau, Germany

Patrick Longa  
Microsoft Research, USA

Marco Macchetti  
Kudelski Security, Switzerland
<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stefan Mangard</td>
<td>Graz University of Technology, Austria</td>
</tr>
<tr>
<td>Chloe Martindale</td>
<td>University of Bristol, UK</td>
</tr>
<tr>
<td>Pierrick Ménard</td>
<td>University of Luxembourg, Luxembourg</td>
</tr>
<tr>
<td>Marcel Medwed</td>
<td>NXP Semiconductors, Austria</td>
</tr>
<tr>
<td>Daniel Moghimi</td>
<td>UC San Diego &amp; Google, USA</td>
</tr>
<tr>
<td>Veelasha Moonsamy</td>
<td>Ruhr University Bochum, Germany</td>
</tr>
<tr>
<td>Thorben Moos</td>
<td>UCLA, Belgium</td>
</tr>
<tr>
<td>Ruben Niederhagen</td>
<td>Academia Sinica, Taiwan &amp; University of Southern Denmark, Denmark</td>
</tr>
<tr>
<td>Svetla Nikova</td>
<td>KU Leuven, Belgium</td>
</tr>
<tr>
<td>Colin O’Flynn</td>
<td>NewAE Technology Inc, Canada</td>
</tr>
<tr>
<td>Stjepan Picek</td>
<td>Radboud University, The Netherlands</td>
</tr>
<tr>
<td>Romain Poussier</td>
<td>ANSSI, France</td>
</tr>
<tr>
<td>Maria Méndez Real</td>
<td>Polytech Nantes Université, France</td>
</tr>
<tr>
<td>Christian Rechberger</td>
<td>TU Graz, Austria</td>
</tr>
<tr>
<td>Francesco Regazzoni</td>
<td>University of Amsterdam, The Netherlands &amp; USI, Switzerland</td>
</tr>
<tr>
<td>Joost Renes</td>
<td>NXP Semiconductors, The Netherlands</td>
</tr>
<tr>
<td>Oscar Reparaz</td>
<td>Cash App (at Block Inc.), USA</td>
</tr>
<tr>
<td>Peter Rindal</td>
<td>VISA Research, USA</td>
</tr>
<tr>
<td>Thomas Roche</td>
<td>NinjaLab, France</td>
</tr>
<tr>
<td>Francisco Rodríguez-Hénriqué</td>
<td>CINVESTAV-IPN, Mexico &amp; Technology Innovation Institute, UAE</td>
</tr>
<tr>
<td>Mélissa Rossi</td>
<td>ANSSI, France</td>
</tr>
<tr>
<td>Sujoy Sinha Roy</td>
<td>Graz University of Technology, Austria</td>
</tr>
<tr>
<td>Markku-Juhani O. Saarinen</td>
<td>PQShield Ltd., UK</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 &amp; Fraunhofer AISEC, Germany</td>
</tr>
<tr>
<td>Marcos A. Simplício Jr.</td>
<td>University of São Paulo, Brazil</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>Junko Takahashi</td>
<td>NTT Corporation, Japan</td>
</tr>
<tr>
<td>Russell Tessier</td>
<td>University of Massachusetts Amherst, USA</td>
</tr>
<tr>
<td>Nicolas Thériault</td>
<td>Universidad de Santiago de Chile</td>
</tr>
<tr>
<td>Alexandre Venelli</td>
<td>NXP Semiconductors, France</td>
</tr>
<tr>
<td>Wenjie Xiong</td>
<td>Virginia Tech, USA</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>