Cryptographic Hardware and Embedded Systems (CHES)

CHES 2025 in Kuala Lumpur, Malaysia, September, 2025

IACR Transactions on CHES (TCHES), Volume 2025, Issues 1–4

Image source: ©Kuala Lumpur, https://unsplash.com/photos/

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 2025 takes place in Kuala Lumpur, Malaysia in September 2025. The conference website is accessible at

https://ches.iacr.org/2025

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 coprocessors
- True and pseudorandom number generators
- Physical unclonable functions (PUFs)
- Efficient software implementations
- SHARCS (Special-purpose HARdware for Cryptanalysis, quantum included)

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
- Hardware trojans and countermeasures

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
- Physical assurance and analysis of embedded systems

Systematization of Knowledge (SoK)

Interactions between cryptographic theory and implementation issues:
- Quantum cryptanalysis
- Algorithm subversion and subversion prevention
- New and emerging cryptographic algorithms and protocols targeting embedded devices
- Security proofs in established (e.g., leakage and fault) models
- Discussion and improvement of theoretical models

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
- Practical privacy-preserving computing (MPC, FHE)
- Post-quantum security

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 TCHES (Transactions on Cryptographic Hardware and Embedded Systems), which is Gold Open Access, 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 2025 are as follows:

- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2025, Issue 1
  - Submission: **15 July 2024**
  - Rebuttal: 19–23 August 2024
  - Notification: 15 September 2024
  - Camera-ready: 14 October 2024
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2025, Issue 2
  - Submission: **15 October 2024**
  - Rebuttal: 20–25 November 2024
  - Notification: 15 December 2024
  - Camera-ready: 14 January 2025
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2025, Issue 3
  - Submission: **15 January 2025**
  - Rebuttal: 24–28 February 2025
  - Notification: 15 March 2025
  - Camera-ready: 14 April 2025
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2025, Issue 4
  - Submission: **15 April 2025**
  - Rebuttal: 26–30 May 2025
  - Notification: 15 June 2025
  - Camera-ready: 14 July 2025

Camera-ready deadline relates to (conditionally) accepted papers. 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 2025, 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 three 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 major revision paper are ideally the same as for the original submission. The Editor(s)-in-Chief will strive to include new reviewers for a resubmission after a Reject.

- Resubmission of papers that have previously been Rejected from TCHES is only allowed after approval by the Editor(s)-in-Chief prior to submission, presumably with meaningful revisions.

- 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

Michael Hutter
UniBwM & PQShield, Germany

Debdeep Mukhopadhyay
IIT Kharagpur, India

ches2025programchairs@iacr.org

2. General Co-Chairs

Muhammad Reza Z'aba
MIMOS, Malaysia

Muhammad Rezal Kamel Ariffin
Universiti Putra, Malaysia

Norziana Jamil
United Arab Emirates University, UAE
Universiti Tenaga Nasional, Malaysia

ches2025@iacr.org

3. Artifact Chair

Lennert Wouters
KU Leuven

ches2025artifacts@iacr.org

4. Managing Editor

Tim Güneysu
Ruhr University Bochum, DE

tches-managing-editor@iacr.org

5. Program Committee/Editorial Board

Anita Aghaie	Siemens AG, Germany
Diego Aranha	Aarhus University, Denmark
Victor Arribas	Rambus, Netherlands
Aydin Aysu	North Carolina State University, USA
Melissa Azouaoui	NXP Semiconductors, Germany
Sebastian Berndt	Technische Hochschule Lübeck, Germany
Shivam Bhasin	Nanyang Technological University, Singapur
Sarani Bhattacharya	IIT Kharagpur, India
Billy Bob Brumley	Rochester Institute of Technology, USA
Ileana Buhan	Radboud University, Netherlands
Fabio Campos	RheinMain University of Applied Sciences, Germany
Gaëtan Cassiers	UCLouvain, Belgium
Durba Chatterjee	Radboud University, Netherlands
Jesús-Javier Chi-Domínguez	Technology Innovation Institute, United Arab Emirates
Lukasz Chmielewski	Masaryk University, Czech Republic
Marios Omar Choudary	University Politehnica of Bucharest, Romania
Chitchanok Chuengsatiansup	University of Klagenfurt, Austria
Thomas Eisenbarth	University of Lübeck, Germany
Daniel Genkin	Georgia Tech, USA
Ashrujit Ghoshal	Carnegie Mellon University, USA
Benedikt Gierlichs	KU Leuven, Belgium
Qian Guo	Lund University, Schweden
Vedad Hadžić	Graz University of Technology, Austria
Julius Hermelink	Max Planck Institute for Security and Privacy (MPI-SP), Germany
Johann Heyszl	Google, Germany
Xiaolu Hou	Slovak University of Technology, Slovakia
Michael Hutter	UniBwM & PQShield, Germany
Kimmo Järvinen	Xiphera Ltd., Finland
Chenglu Jin	CWI Amsterdam, Netherlands
Marc Joye	Zama, France

Matthias J. Kannwischer	Chelpis Quantum Corp, Taiwan
Elif Bilge Kavun	University of Passau, Germany
Tanja Lange	Eindhoven University of Technology, Netherlands
Leibo Liu	Tsinghua University, China
Patrick Longa	Microsoft Research, USA
Roel Maes	Synopsys, Netherlands
Cuauhtemoc Mancillas-Lopez	Cinvestav-IPN, Mexico
Mihalis Maniatakos	New York University Abu Dhabi, United Arab Emirates
Loïc Masure	LIRMM CNRS, France
Thorben Moos	UCLouvain, Belgium
Amir Moradi	TU Darmstadt, Germany
Debdeep Mukhopadhyay	IIT Kharagpur, India
Svetla Nikova	KU Leuven, Belgium
David Oswald	University of Birmingham, United Kingdom
Daniel Page	University of Bristol, United Kingdom
Sri Parameswaram	University of Sydney, Australia
Sikhar Patranabis	IBM Research India, India
Peter Pessl	Infineon, Germany
Ilia Polian	University of Stuttgart, Germany
Romain Poussier	ANSSI, France
Bart Preneel	KU Leuven, Belgium
Robert Primas	Intel Labs, USA
Chester Rebeiro	IIT Madras, India
Francesco Regazzoni	University of Amsterdam & Università Della Svizzera Italiana, Switzerland
Joost Renes	NXP Semiconductors, Netherlands
Jan Richter-Brockmann	Ruhr University Bochum, Germany
Sujoy Sinha Roy	Graz University of Technology, Austria
Markku-Juhani Saarinen	Tampere University, Finland
Sayandeep Saha	IIT Bombay, India
Kazuo Sakiyama	The University of Electro-Communications, Japan
Simona Samardjiska	Radboud University, Netherlands
Yu Sasaki	NTT Social Informatics Laboratories and NIST Associate, Japan
Pascal Sasdrich	Ruhr University Bochum, Germany
Erkay Savas	Sabanci University, Turkey
Jean-Pierre Seifert	TU Berlin, Germany
Aein Shahmirzadi	PQShield, Germany
Georg Sigl	TU Munich & Fraunhofer AISEC, Germany
François-Xavier Standaert	UCLouvain, Belgium
Rainer Steinwandt	University of Alabama in Huntsville, USA
Marc Stöttinger	RheinMain University of Applied Sciences, Germany
Jakub Szefer	Northwestern University, USA
Shahin Tajik	Worcester Polytechnic Institute, USA
Junko Takahashi	NTT, Japan
Adrian Thillard	PQShield, France
Ming-Hsien Tsai	National Taiwan University of Science and Technology, Taiwan
Michael Tunstall	Google, USA
Aleksei Udovenko	University of Luxembourg, Luxembourg
Rei Ueno	Kyoto University, Japan
Christine Van Vredendaal	NXP Semiconductors, Netherlands
Weijia Wang	Shandong University, China
Bohan Yang	Tsinghua University, China
Bo-Yin Yang	Academia Sinica, Taiwan
Yuval Yarom	Ruhr University Bochum, Germany