CHES 2026

October 11-15, 2026
Turkey

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 2026 will take place in Turkey in October 11-15, 2026. The conference website is accessible at

https://ches.iacr.org/2026

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 2026 highlighted in **bold blue**):

Cryptographic implementations:

- Hardware architectures
- Cryptographic processors and coprocessors
- True and pseudorandom number generators
- Physical unclonable functions (PUFs)
- Efficient software implementation
- 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
- **New datasets for public use**

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
- Theoretical hardware models that allow proofs

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 cyberresilience
- Engineering of zero-knowledge proof systems
- Privacy-preserving computing in practice (MPC, FHE)
- Post-quantum security

Instructions for Authors

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.

The page limit is up to 20 pages, including all figures, tables, and appendices, but excluding the bibliography. Appendices are also reviewed, and should appear before the bibliography. Authors are encouraged to include additional supplementary material needed to validate the content (e.g., test vectors or source code) as separate files. In exceptional cases, where extra details, such as proofs or experimental results, are deemed essential, long papers of up to 40 pages may be allowed. **Submission of long papers requires pre-approval by the Editors-in-Chief.** Authors need to request pre-approval no later than a week before the submission deadline. The request should specify the number of additional pages required, a justification for a long paper, and a draft of the paper. When submitted, 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 also need to include the justification for long papers in the supplementary material. Long papers submitted without pre-approval 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:*".

⚠ Submissions not meeting these guidelines risk rejection without consideration of their merits.

Regulations

The review process for TCHES, Volume 2026, 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 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.

- Requests for resubmissions of papers that received a “reject & resubmit” or a “reject” decision must be sent to the editors in chief at least one week before the submission deadline and must be accompanied by a document explaining the differences with the original submission plus a draft of the revised paper. Note that, except in extenuating circumstances, such requests will not be granted if the resubmission is within a year after the original submission for rejected papers, or within the subsequent submission cycle in the case of a reject and resubmit decision.
- 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.

Program Committee

Program Co-Chairs

Nele Mentens
KU Leuven, Belgium, and
Leiden University, the Netherlands

Yuval Yarom
Ruhr University Bochum, Germany

ches2026programchairs@iacr.org

General Co-Chairs

TBA

ches2026@iacr.org

Managing Editor

Tim Güneysu
Ruhr University Bochum
Germany

tches-managing-editor@iacr.org

Important Dates (tentative)

All submission deadlines are at 23:59:59 Anywhere on Earth (AoE).

Schedule for TCHES Volume 2026/1

15 July 2025	Submission
28–31 Aug. 2025	Rebuttal period
15 Sept. 2025	Notification
14 Oct. 2025	Camera ready

Schedule for TCHES Volume 2026/2

15 Oct. 2025	Submission
27–30 Nov. 2025	Rebuttal period
15 Dec. 2025	Notification
14 Jan. 2026	Camera ready

Schedule for TCHES Volume 2026/3

15 Jan. 2026	Submission
26 Feb.–1 Mar. 2026	Rebuttal period
15 Mar. 2026	Notification
14 April 2026	Camera ready

Schedule for TCHES Volume 2026/4

15 April 2026	Submission
28–31 May 2026	Rebuttal period
15 June 2026	Notification
14 July 2026	Camera ready

Camera-ready deadline relates to (conditionally) accepted papers.

Further details are available on the paper submission page.