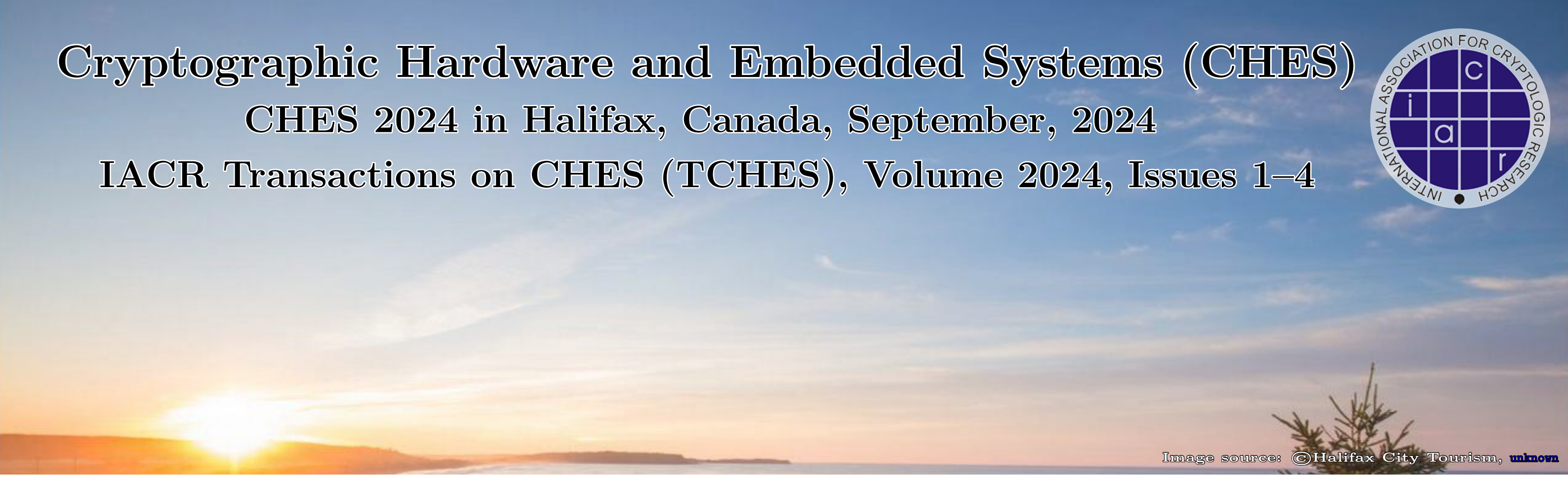

Cryptographic Hardware and Embedded Systems (CHES)

CHES 2024 in Halifax, Canada, September, 2024

IACR Transactions on CHES (TCHES), Volume 2024, Issues 1–4

Image source: ©Halifax City Tourism, unknown

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 2024 takes place in Halifax, Nova Scotia, Canada in September 2024. The conference website is accessible at

https://ches.iacr.org/2024

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

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)

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 cyber-resilience
- Engineering of zero-knowledge proof systems
- Practical privacy-preserving computing (MPC, FHE)

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 2024 are as follows:

- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2024, Issue 1
  - Submission: **15 July 2023**
  - Rebuttal: 21–25 August 2023
  - Notification: 15 September 2023
  - Camera-ready: 14 October 2023
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2024, Issue 2
  - Submission: **15 October 2023**
  - Rebuttal: 20–24 November 2023
  - Notification: 15 December 2023
  - Camera-ready: 14 January 2024
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2024, Issue 3
  - Submission: **15 January 2024**
  - Rebuttal: 19–23 February 2024
  - Notification: 15 March 2024
  - Camera-ready: 14 April 2024
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2024, Issue 4
  - Submission: **15 April 2024**
  - Rebuttal: 20–24 May 2024
  - Notification: 15 June 2024
  - Camera-ready: 14 July 2024

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 2024, 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 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

Bo-Yin Yang
Academia Sinica, TW

Francisco Rodriguez
Technology Innovation Institute, AE

`ches2024programchairs@iacr.org`

2. General Co-Chairs

Colin O'Flynn + Hilary Taylor
NewAE and Dalhousie University, CA
ches2024@iacr.org

3. Artifact Chair

Markku-Juhani O. Saarinen, PQShield, UK
ches2024artifacts@iacr.org

4. Managing Editor

Tim Güneysu
Ruhr University Bochum, DE
tches-managing-editor@iacr.org

5. Program Committee/Editorial Board

Alexandre Venelli	NXP Semiconductors, France
Amir Moradi	RU Bochum, Germany
Aron Gohr	Independent Researcher, New Zealand
Begül Bilgin	Rambus Cryptography Research, USA
Bo-Yin Yang	Academia Sinica, Taiwan
Cécile Dumas	CEA-Leti Université Grenoble Alpes, France
Chen-Mou Cheng	BTQ, Canada
Chester Rebeiro	IIT Madras, India
Chitchanok Chuengsatiansup	University of Melbourne, Australia
Christian Rechberger	TU Graz, Austria
Christoph Dobraunig	Intel Labs, USA
Colin O'Flynn	NewAE Technology Inc., Canada
Cuauhtemoc Mancillas-Lopez	CINVESTAV, Mexico
Daniel Genkin	GeorgiaTech, USA
Elke De Mulder	Google, USA
Erkay Savas	Sabanci University, Turkey
Fan Zhang	Zhejiang University, China
Fatemeh Ganji	Worcester Polytechnic Institute, USA
Francesco Regazzoni	U. of Amsterdam & Università della Svizzera Italiana, Switzerland
Francisco Rodríguez-Henríquez	CINVESTAV & Technology Innovation Institute, United Arab Emirates
François Gérard	University of Luxembourg, Luxembourg
Georg Sigl	TU Munich & Fraunhofer AISEC, Germany
Guilherme Perin	Leiden U, Netherlands
Gustavo Banegas	Qualcomm, France
Ileana Buhan	Radboud University, Netherlands
Jan-Pieter D'Anvers	KULeuven, Belgium
Jean-Luc Beuchat	UAS at HES-SO Valais-Wallis, Switzerland
Jesús-Javier Chi Domínguez	Technology Innovation Institute, United Arab Emirates
Jiun-Peng Chen	Academia Sinica, Taiwan
Johann Heyszl	Google LLC, Germany
Joost Renes	NXP Semiconductors, Netherlands
Junko Takahashi	NTT Corporation, Japan
Kathrin Hövelmanns	Eindhoven University of Technology, Netherlands
Kimmo Järvinen	Xiphera, Finland
Kota Yoshida	Ritsumeikan University, Japan
Leibo Liu	Tsinghua University, China
Lejla Batina	Radboud University, Netherlands
Loïc Masure	UC Louvain, Belgium
Łukasz Chmielewski	Masaryk University, Czech Republic
Matthias J. Kannwischer	Chelpis, Taiwan
Mélissa Rossi	ANSSI, France
Michael Hutter	PQShield, Austria

Ming-Hsien Tsai	National Institute of Cyber Security, Taiwan
Nicolas Thériault	Universidad de Santiago de Chile, Chile
Oscar Reparaz	Cash App at Block Inc., USA
Patrick Longa	Microsoft Research, USA
Petr Svenda	Masaryk University, Czech Republic
Pierrick Méaux	University of Luxembourg, Luxembourg
Raghvendra Singh Rohit	Technology Innovation Institute, United Arab Emirates
Rei Ueno	Tohoku University, Japan
Roel Maes	Intrinsic ID, Netherlands
Romain Poussier	ANSSI, France
Ruben Niederhagen	Academia Sinica and U of Southern Denmark, Taiwan
Sebastian Berndt	University of Lübeck, Germany
Shahin Tajik	Worcester Polytechnic Institute, USA
Shivam Bhasin	Nanyang Technological University, Singapore
Sonia Belaid	CryptoExperts, France
Stefan Mangard	Graz University of Technology, Austria
Sujoy Sinha Roy	TU Graz, Austria
Svetla Nikova	KU Leuven, Belgium
Tanja Lange	TU Eindhoven, Netherlands
Thomas Roche	NinjaLab, France
Thorben Moos	UCLouvain, Belgium
Yu Yu	Shanghai Jiao Tong University, China
Yuval Yarom	Ruhr University Bochum, Germany