Cryptographic Hardware and Embedded Systems (CHES)

CHES 2019, Atlanta, USA, August 24–28, 2019

IACR Transactions on CHES (TCHES), Volume 2019, Issues 1–4

Call for Papers

Having been established in 1999, the Cryptographic Hardware and Embedded Systems (CHES) conference is the premier venue for research on 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 2019, marks the 20th anniversary of the CHES conference and it will take place in the city of Atlanta, U.S.A., August 24–28, 2019, immediately following CRYPTO 2019. The conference website is accessible at

`https://ches.iacr.org/2019`

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 co-processors
- True and pseudorandom number generators
- Physical unclonable functions (PUFs)
- Efficient software implementations

Attacks against implementations, and countermeasures:

- Side-channel attacks and countermeasures
- Fault attacks and countermeasures
- Hardware tampering and tamper-resistance
- White-box cryptography and code obfuscation
- Hardware and software reverse engineering

Tools and methodologies:

- Computer aided cryptographic engineering
- Verification methods and tools for secure design
- Metrics for the security of embedded systems
- Secure programming techniques
- FPGA design security
- Formal methods for secure hardware and software

Interactions between cryptographic theory and implementation issues:

- New and emerging cryptographic algorithms and protocols targeting embedded devices
- Special-purpose hardware for cryptanalysis
- Leakage resilient cryptography

Applications:

- 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
- Smart card processors, systems and applications
- Security for cyberphysical systems (home automation, medical implants, industrial control, etc.)
- Automotive security
- Secure storage devices (memories, disks, etc.)
- Technologies and hardware for content protection
- Trusted computing platforms

New Publication Model

As of 2018, CHES has moved to an open-access journal/conference hybrid model. Following the success of similar initiatives at analogous events such as FSE, this decision was made (by the CHES steering committee) as a means of improving review and publication quality while retaining the highly successful, community-focused nature of the event. A comprehensive set 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 instances then published by the Ruhr University of Bochum in an issue of the newly established journal IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES). Since it has a Gold Open Access status, all papers published in TCHES will be immediately and freely available.

2. The annual CHES conference will consist of presentations for each paper published in the associated issues of TCHES, plus invited talks and a range of additional and social activities.

3. TCHES has four submission deadlines per year; 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

Upcoming deadlines relating to CHES 2019 are as follows:

- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2019, Issue 1
  - Submission: **15 July 2018**
  - Rebuttal: 20–27 August 2018
  - Notification: 15 September 2018
  - Camera-ready: 14 October 2018
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2019, Issue 2
  - Submission: **15 October 2018**
  - Rebuttal: 20–30 November 2018
  - Notification: 15 December 2018
  - Camera-ready: 14 January 2019
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2019, Issue 3
  - Submission: **15 January 2019**
  - Rebuttal: 20–27 February 2019
  - Notification: 15 March 2019
  - Camera-ready: 14 April 2019
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2019, Issue 4
  - Submission: **15 April 2019**
  - Rebuttal: 20–27 May 2019
  - Notification: 15 June 2019
  - Camera-ready: 14 July 2019

Observe that the camera-ready deadline relates to accepted and conditionally accepted papers, and that *all* deadlines are 23:59:59 Anywhere on Earth (AoE).

Instructions for Authors

1. Submission

To submit a paper to TCHES, follow the instructions available at:

`https://tches.iacr.org/index.php/TCHES/submission`

2. Format

A paper submitted to TCHES must be written in English and be anonymous, with no author names, affiliations, acknowledgements, or any identifying citations. It should begin with a title, a short abstract, and a list of keywords. The introduction should summarise 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/latex`

noting that TCHES only accepts electronic submission in PDF format.

TCHES accepts two forms of paper, termed short and long; the page limit (excluding bibliography) is 20 and 40 pages respectively. In either case, authors are encouraged to include supplementary material needed to validate the content (e.g., test vectors or source code) as an appendix: this material will not be included in the page count. In allowing long papers, the goal is to support cases where extra detail (e.g., proofs, or experimental results) is deemed essential. Authors should highlight long papers by annotating the title with "(Long Paper)", and be aware the review process may take longer: a decision may, at the discretion of the editors-in-chief(s), be deferred to the subsequent volume.

3. Regulations

The review process for TCHES, Volume 2019, Issues 1–4, will be governed by the following regulations:

- Members of the TCHES editorial board may submit one new paper per deadline (co-authored or otherwise); editor(s)-in-chief may not submit papers during their tenure.
- 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.
- TCHES follows IACR policy with respect to conflicts of interest that could prevent impartial review. A conflict of interest is considered to occur 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 authors papers in the past 3 years,
  - are immediate family members,
  - have an current, ongoing research collaboration (e.g., are members of the same research project).

  IACR reserves the right to share information about submissions with other program committees and editorial boards to ensure strict enforcement of the policy.
- At the time of submission, authors are **required** to
  1. make a declaration regarding any conflicts of interest, 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 revise and resubmit their article to one of the following two submission deadlines, otherwise any re-submission will be treated as new.
- To ensure consistency, the reviewers assigned for a revised paper are ideally the same as for the original.

Contacts

1. Program Co-Chairs / Co-Editors-in-Chief

4.1.1 Current (i.e., for CHES 2019)

Pierre-Alain Fouque
Université Rennes 1

Jorge Guajardo
Robert Bosch LLC — RTC

`ches2019programchairs@iacr.org`

2. General Co-Chairs

Vincent J. Mooney III
Georgia Institute of Technology

Patrick Schaumont
Virginia Tech

Yunsi Fei
Northeastern University

`ches2019@iacr.org`

3. Managing Editor

Tim Güneysu
Ruhr University Bochum

`tches-managing-editor@iacr.org`

4. Program Committee/Editorial Board (Preliminary)

Diego Aranha	Aarhus University & University of Campinas	DK
Valentima Banciu	Riscure	NL
Lejla Batina	Radboud University	NL
Sonia Belaïd	CryptoExperts	FR
Daniel J. Bernstein	University of Illinois at Chicago	US
Begü Bilgin	Rambus & KU Leuven	NL
Joppe W. Bos	NXP Semiconductors	BE
Jean-Sebastien Coron	Luxembourg University	LUX
Elke De Mulder	Rambus	US
Fraçois Dupressoir	Surrey University	UK
Thomas Eisenbarth	University of Lübeck & WPI	DE
Sebastian Faust	TU Darmstadt	DE
Wieland Fischer	Infineon Technologies	DE
Christopher W. Fletcher	University of Illinois, Urbana Champaign	US
Pierre-Alain Fouque	Université Rennes 1	FR
Kevin Fu	University of Michigan	US
Benoît Gérard	DGA.MI & IRISA	FR
Daniel Genkin	U. Penn	US
Benedikt Gierlichs	KU Leuven	BE
Hannes Gross	Graz University of Technology	AT
Vincent Grosso	CNRS/Laboratory Hubert Curien	FR
Jorge Guajardo	Robert Bosch LLC — RTC	US
Shay Gueron	University of Haifa & Amazon Web Services	IL
Annelie Heuser	Univ Rennes, Inria, CNRS, IRISA	FR
Dan Holcomb	UMASS Amherst	US
Naofumi Homma	Tohoku University	JP
Kimmo U. Järvinen	University of Helsinki	FI
Marc Joye	OneSpan	BE
Tanja Lange	Technische Universiteit Eindhoven	NL
Gaëtan Leurent	INRIA	FR
Patrick Longa	Microsoft Research	US
Roel Maes	Intrinsic ID	NL
Jonathan McCune	Google AI	US
Nele Mentens	KU Leuven	BE
Atsuko Miyaji	Osaka University/JAIST	JP
Amir Moradi	Ruhr University of Bochum	DE
Colin OFlynn	Dalhousie University	CA
Peter Pessl	Graz University of Technology	AT
Thomas Peyrin	NTU	SG
Thomas Pöppelmann	Infineon Technologies	DE
Thomas Pornin	NCC Group	CA
Axel Poschmann	DarkMatter LLC	UAE
Emmanuel Prouff	ANSSI	FR
Christian Rechberger	TU Graz	AT
Francesco Regazzoni	ALaRI – USI	CH
Matthieu Rivain	CryptoExperts	FR
Francisco Rodríguez-Henríquez	CINVESTAV-IPN	MX
Tobias Schneider	Universite catholique de Louvain	BE
Peter Schwabe	Radboud University	NL
Jean-Pierre Seifert	TU Berlin	DE
Johanna Sepulveda	Technical University of Munich	DE
Sujoy Sinha Roy	University of Birmingham	UK
Martijn Stam	University of Bristol	UK
Shahin Tajik	University of Florida	US
Mehdi Tibouchi	NTT Secure Platform Laboratories	JP
Michael Tunstall	Rambus	US
Srinivas Vivek	IIIT Bangalore	IN
André Weimerskirch	Lear Corp.	US
Yuval Yarom	University of Adelaide & Data61	AU