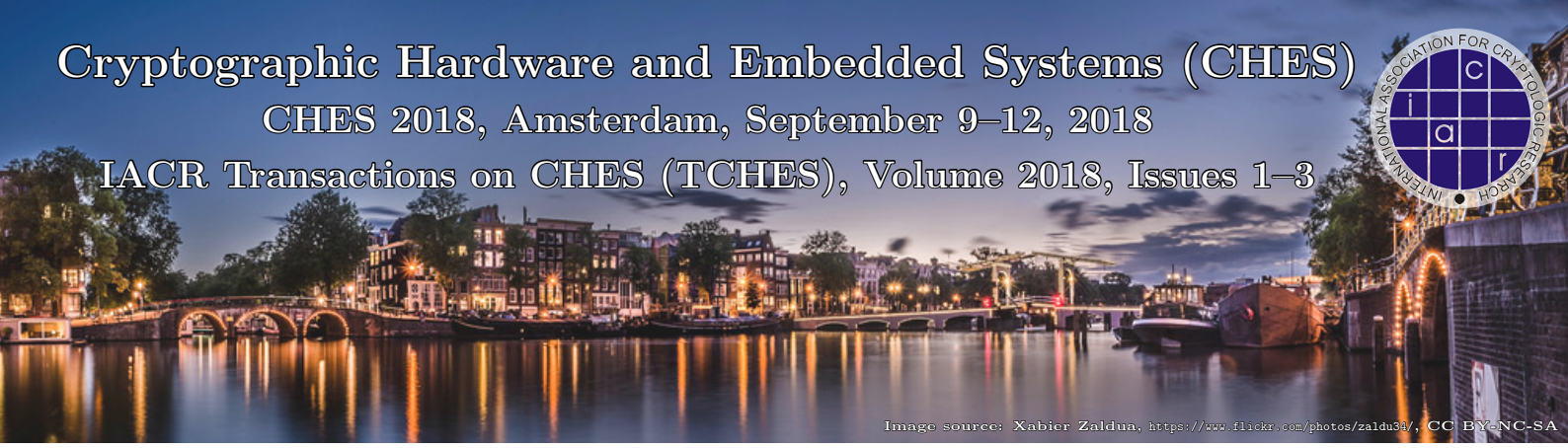

Call for Papers

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 2018 will take place in Amsterdam, The Netherlands, September 9–12, 2018. The conference website is accessible at

`https://ches.iacr.org/2018`

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

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 event. A comprehensive set of FAQs relating to the model can be found via the TCHES website at

`https://tches.iacr.org`

but, 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.

Although this description is the norm, CHES 2018 will be a special case in order to smooth the transition: it will consist of three (vs. four) issues of TCHES only.

Timeline

Upcoming deadlines relating to CHES 2018 are as follows:

- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2018, Issue 1
  - Submission: **15 October 2017**
  - Rebuttal: 20–27 November 2017
  - Notification: 15 December 2017
  - Camera-ready: 14 January 2018
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2018, Issue 2
  - Submission: **15 January 2018**
  - Rebuttal: 20–27 February 2018
  - Notification: 15 March 2018
  - Camera-ready: 14 April 2018
- IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Volume 2018, Issue 3
  - Submission: **15 April 2018**
  - Rebuttal: 20–27 May 2018
  - Notification: 15 June 2018
  - Camera-ready: 14 July 2018

noting 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/pages/view/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/pages/view/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 2018, Issues 1–3, 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

Current (i.e., for CHES 2018)

Daniel Page
University of Bristol

Matthieu Rivain
CryptoExperts

`ches2018programchairs@iacr.org`

Observing (i.e., for CHES 2019)

Pierre-Alain Fouque
Université Rennes 1

Jorge Guajardo
Robert Bosch LLC - RTC

2. General Co-Chairs

Ileana Buhan
Riscure

Peter Schwabe
Radboud University

`ches2018@iacr.org`

3. Managing Editor

Tim Güneysu
Ruhr University Bochum

`tches-managing-editor@iacr.org`

4. Program Committee/Editorial Board

D. Aranha	University of Campinas	BR
R. Avanzi	ARM	DE
L. Batina	Radboud University	NL
S. Belaïd	CryptoExperts	FR
D.J. Bernstein	University of Illinois at Chicago	US
J. Bos	NXP Semiconductors	BE
B. Brumley	Tampere University of Technology	FI
I. Buhan	Riscure	NL
C.-M. Cheng	National Taiwan University	TW
C. Clavier	Université de Limoges	FR
T. Eisenbarth	University of Lübeck & WPI	DE
J. Fan	Open Security Research Inc.	CN
S. Faust	TU Darmstadt	DE
V. Fischer	Jean Monnet University, Saint-Etienne	FR
W. Fischer	Infineon Technologies	DE
P.-A. Fouque	Université Rennes 1	FR
J. Fournier	CEA-Leti	FR
G. Gagnerot	eshard	FR
B. Gierlichs	KU Leuven	BE
A. Gouget	Gemalto	FR
J. Guajardo	Robert Bosch LLC - RTC	US
S. Gueron	Amazon Web Services & University of Haifa	IL
T. Güneysu	Ruhr University Bochum & DFKI	DE
M. Hamburg	Cryptography Research Inc.	US
A. Heuser	CNRS, IRISA	FR
N. Homma	RIEC/Tohoku University	JP
K. Järvinen	University of Helsinki	FI
M. Joye	NXP Semiconductors	BE
E. Käsper	Google	US
K. Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences	DE
T. Lepoint	SRI International	US
P. Longa	Microsoft Research	US
R. Maes	Intrinsic ID	NL
S. Mangard	TU Graz	AT
C. Maurice	CNRS, IRISA	FR
A. Miyaji	Osaka Univirsity/JAIST	JP
A. Moradi	Ruhr University Bochum	DE
D. Mukhopadhyay	Indian Institute of Technology Kharagpur	IN
C. O'Flynn	NewAE Technology Inc.	CA
E. Oswald	University of Bristol	UK
D. Page	University of Bristol	UK
T. Peyrin	Nanyang Technological University	SG
A. Poschmann	DarkMatter LLC	AE
E. Prouff	ANSSI	FR
F. Regazzoni	ALaRI – USI	CH
M. Rivain	CryptoExperts	FR
E. Savaş	Sabanci University	TR
P. Schwabe	Radboud University	NL
S. Skorobogatov	University of Cambridge	UK
F.-X. Standaert	Universite catholique de Louvain	BE
R. Susella	STMicroelectronics	IT
M. Tunstall	Cryptography Research Inc.	US
S. Vivek	IIIT Bangalore	IN
B.-Y. Yang	Academia Sinica, Institute of Information Science (IIS)	TW
Y. Yarom	University of Adelaide & Data61	AU
R. Zeitoun	IDEMIA	FR