Preface to TCHES 2018

Daniel Page[1] and Matthieu Rivain[2]

[1] University of Bristol, Merchant Venturers Building,
Woodland Road, Bristol, BS8 1UB, United Kingdom.
csdsp@bristol.ac.uk
[2] CryptoExperts, 41 Boulevard des Capucines, 75002 Paris, France.
matthieu.rivain@cryptoexperts.com

Having been established in 1999, the Cryptographic Hardware and Embedded Systems (CHES) conference is today 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 was held in Amsterdam, The Netherlands, September 9–12, 2018. It was the twentieth edition of the conference, but the first under a new hybrid (i.e., a mixture of journal and conference), gold open-access (under the Creative Commons CC-BY 4.0 license) publication model: accepted papers constituting the CHES 2018 program were published in the IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) Volume 2018, Issues 1, 2, and 3. The decision to adopt this publication model was made by the CHES Steering Committee in early 2017. Motivated by success of other communities such as FSE, whose program is published under the same model in the IACR Transactions on Symmetric Cryptography (ToSC), it was viewed as a means of improving review and publication quality while retaining the highly successful, community-focused event, plus satisfying modern demand for (and impact of) open-access research.

The change in publication model demanded a new review process. Although the TCHES web-site houses a comprehensive FAQ detailing both, the latter can be summarised by three differences: while retaining a double-blind policy, and following IACR policy on declaration and management of Conflict of Interests (CoI), the process for each TCHES issue involves a) four submission deadlines associated with TCHES issues for a given CHES conference (only three for this first edition), b) reviewers drawn from an Editorial Board who write detailed, careful reviews and c) a richer set of possible decisions, adding journal-like major and minor revision options to outright accept or reject. The decision for each submission is informed by careful discussion between reviewers mediated by the Co-Editors-in-Chief, and a rebuttal phase allowing authors to respond to preliminary reviews. To provide the highest quality feedback to authors, significant effort is made by reviewers to update the preliminary reviews: ideally the final reviews capture discussion points, and justify the resulting decision. We expect both the publication model and review process to evolve over time, to reflect experience, and emerging challenges and opportunities. However, in our view it has already proven successful. The quantity and quality of submissions has been excellent, and, through the review quality and options for revision, we feel it has been possible to further improve both accepted and rejected submissions.

The submission statistics of TCHES Volume 2018 are summarized in Table 1. The three issues have received a total of 181 submissions (164 discounting re-submissions) among which 47 have finally been accepted, making a global acceptance rate of 26%. For the re-submissions following a requested major revision, the acceptance rate soars to 60%,

IACR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925,
Vol. 2018, No. 1, pp. I–IV
DOI:10.13154/tches.v2018.i1.I-IV

Table 1: Submission statistics of TCHES Volume 2018.

	Issue 1	Issue 2	Issue 3
Number of new submissions	45	43	76
Number of re-submissions from previous issues	-	5	12
Number of submissions (total)	45	48	88
Number of accepted submissions	11	13	23
Acceptance rate	24%	29%	26 %

which shows the effectiveness of the new process.

After voting, the Editorial Board conferred the CHES 2018 best paper award to *Cold Boot Attacks on Ring and Module LWE Keys Under the NTT* by Martin Albrecht, Amit Deo, and Kenneth Paterson, who were also afforded a double-length presentation slot as a result. The program included two invited talks: *(Why) Are Microarchitectural Attacks really different than Physical Side-Channel Attacks?* by Daniel Gruss (Graz University of Technology) and *Leveraging deep-learning to perform SCA attacks against AES implementations* by Elie Bursztein (Google). Following their success in previous editions, the conference also held a poster session as well as two pre-conference tutorials: *Counterfeit Integrated Circuits: Threats, Detection, and Avoidance* by Domenic Forte (University of Florida) and Rajat Subhra Chakraborty (Indian Institute of Technology, Kharagpur), and *Formal Verification of Masked Implementations* by Sonia Belaïd (CryptoExperts) and Benjamin Grégoire (INRIA). We feel all these elements reflect both hot-topics for, and the traditional influence of both academia and industry on, CHES as a whole.

Acknowledgments. Both the TCHES journal and CHES conference are the culmination of a huge, and often unseen or under-appreciated, amount of effort by a range of parties. We would like to extend our deep, sincere thanks to all of them. In particular, the conference budget was supported by the generous sponsorship of Rambus, ALPhANOV, eshard, NewAE Technology, NXP, Thales, Infineon Technologies, Robert Bosch LLC, Continental, CryptoExperts, Fox-IT, Idemia, IoTeX, OSR, PQ Shield, Secure-IC, and NSF. The conference logistics were expertly managed by the General Chairs: Ileana Buhan and Peter Schwabe. We are grateful to Sonia Belaïd for chairing the poster session, and to Daniel Genkin and Yuval Yarom for chairing the rump session. We also thank Ileana Buhan, Karim Tobich and Emmanuel Prouff for organising the CHES 2018 CTF. The schedule demanded by multiple TCHES submission deadlines, added to by workload stemming from "long" (i.e., beyond 20 pages) submissions and shepherding of those with minor revisions, has been a significant challenge. The dedication and professionalism of the Editorial Board members, and external reviewers, played a central role in successfully addressing this challenge. Instances of the `websubrev` software, authored and supported by Shai Halevi, enabled the TCHES submission and review processes. The publication of TCHES was supported by Tim Güneysu in the role of Managing Editor; constituent papers all used a LaTeX style originally authored by Gaëtan Leurent. We are indebted to the CHES Steering Committee for advice and support throughout the development of and transision to the new publication model. We capitalised on experience from various members of the FSE/ToSC community, and we are gratefull to the FSE Steering Committee for time and advice. Last but not least, we would like to express our deep gratitude to the authors of all the submissions for their vital contribution to the success of this first edition of the (T)CHES journal/conference hybrid.

July 2018 Daniel Page
Matthieu Rivain

Editorial Board

External Reviewers

Alexandre Adomnicai
Anita Aghaie
Estuardo Alpírez Bock
Pedro G. M. R. Alves
Christopher Ambrose
Florian Bache
Anubhab Baksi
Valentina Banciu
Guillaume Barbu
Alberto Battistello
Pierre Bayon
Emanuele Bellini
Luk Bettale
Shivam Bhasin
Sarani Bhattacharya
Elif Bilge Kavun
Begül Bilgin
Nina Bindel
Manuel Bluhm
Matteo Bocchi
Jakub Breier
Ahmet Can Mert
Anupam Chattopadhyay
Wenjie Che
Yu-Chia Chen
Lukasz Chmielewski
Tung Chou
Jessy Clediere
Brice Colombier
Jean-Sébastien Coron
Joan Daemen
Nilanjan Datta
Elke De Mulder
Nicolas Debande
Thomas Decnudde
Jeroen Delvaux
Markus Dichtl
Cécile Dumas
Baris Ege
Maria Eichlseder
Nadia El Mrabet
Maik Ender
Thomas Espitau
Benoit Feix
Alberto Ferrante
Si Gao
Santosh Ghosh
Gilbert Goodwill
Dahmun Goudarzi
Daniele Grattarola
Aurélien Greuet
Hannes Gross
Vincent Grosso
Berk Gulmezoglu
Patrick Haddad
Carl-Daniel Hailfinger
Sohaib ul Hassan
Matthias Hiller
Kristina Hostakova
Yuan-Che Hsu
Andreas Hülsing
Christopher Huth
Michael Hutter
Gorka Irazoqui
Takanori Isobe
Mustafa Kairallah
Miroslav Knezevic
Lieneke Kusters
Maxime Lecomte
Antoine Loiseau
David Lubicz
Pedro Maat C. Massolino
Houssem Maghrebi
Mark Marson
Dan Martin
Silvia Mella
Vincent Migliore
Ahmad Moghimi
Thorben Moos
Andres Moreno
Ugo Mureddu
Michael Naehrig
Zakaria Najm
Christophe Negre
Ventzi Nikov
Elie Noumon Allini
Tobias Oder
Shinya Okumura
Erdinc Ozturk
Clara Paglialonga
Kostas Papagiannopoulos
Sikhar Patranabis
Florian Pebay Peyroula
Cesar Pereida García
Peter Pessl
Stjepan Picek
Christian Pilato
Jim Plusquellic
Romain Poussier
Robert Primas
Jürgen Pulkus
Thomas Pöppelmann
Shahram Rasoolzadeh
Joost Renes
Oscar Reparaz
Léo Reynaud
Jefferson Ricardini
Bastian Richter
Franck Rondepierre
Debapriya Basu Roy
Sujoy Sinha Roy
Vladimir Rožić
Markku-Juhani O. Saarinen
Simona Samardjiska
Peter Samarin
Falk Schellenberg
Werner Schindler
Tobias Schneider
Okan Seker
Mitsuru Shiozaki
Chunhua Su
Banik Subhadeep
Robert Szerwinski
Yannick Teglia
Hugues Thiebeauld
Adrian Thillard
Karim Tobich
Harshal Tupsamudre
Nicola Tuveri
Rei Ueno
Markus Ullmann
Dan Ungureanu
Thomas Unterluggauer
Praveen Vadnala
Aurelien Vasselle
Vincent Verneuil
Pim Vullers
Junwei Wang
Felix Wegener
Mario Werner
Carolyn Whitnall
Alexander Wild
Antoine Wurcker
Shayan Yassami
Ville Yli-Mäyry
Shih-Chun You
Daniele Zambon