

Preface

The 18th Conference on Cryptographic Hardware and Embedded Systems (CHES 2016) was held at the University of California at Santa Barbara, California, USA, August 17–19, 2016. The conference was sponsored by the *International Association for Cryptologic Research* and—after 2010 and 2013—it was the third time that CHES was co-located with CRYPTO.

CHES 2016 received a record 148 submissions. Each paper was anonymously reviewed by at least four Program Committee members in a double-blind peer-review process. Submissions co-authored by PC members received at least five reviews. With the help of 210 external reviewers our 47 Program Committee members wrote an impressive total of 623 reviews. This year CHES continued the policy that submissions needed to closely match the final versions published by Springer in length and format. Additionally, we implemented a new paper submission policy whereby authors needed to indicate conflicts of interest with Program Committee members. This mutual indication process led to the upfront identification of roughly five times more conflicts of interest, and, consequently, to a more fair and smooth review process. The Program Committee selected 30 papers for publication in these proceedings, corresponding to a 20% acceptance rate.

Several papers were nominated for the CHES 2016 best paper award. After voting, the Program Committee gave the award to *Differential Computation Analysis: Hiding Your White-Box Designs Is Not Enough* by Joppe W. Bos, Charles Hubain, Wil Michiels, and Philippe Teuwen. The runners-up were *Cache Attacks Enable Bulk Key Recovery on the Cloud* by Mehmet S. Inci, Berk Gulmezoglu, Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar, and *Software Implementation of Koblitz Curves Over Quadratic Fields* by Thomaz Oliveira, Julio López, Francisco Rodríguez-Henríquez. All three were invited to submit extended versions to the *Journal of Cryptology*.

The technical program was completed by a panel discussion that provided valuable feedback to the academic and industrial communities, and by an excellent invited talk (jointly with CRYPTO 2016) by Paul Kocher from Cryptography Research, a Division of Rambus.

As a continued tradition, CHES 2016 also featured a poster session and we are very grateful to Billy Bob Brumley for chairing this aspect of the program. In addition, two tutorials were given on the day preceding the conference: one by Victor Lomné on *Common Criteria Certification of a Smartcard: A Technical Overview* and one by Yuval Yarom on *Micro-Architectural Side-Channel Attacks*. For the second time a CHES challenge was organized. We are very grateful to Ryad Benadjila, Emmanuel Prouff, and Adrian Thillard for chairing the challenge selection process, and to Colin O’Flynn for running the CHES 2016 challenge.

The review process was a challenging and time-consuming task. We sincerely thank the Program Committee members as well as their external reviewers for the hard work and many hours spent reviewing, assessing, and discussing. The submission process,

the review process, and the editing of the final proceedings were greatly simplified by the software written by Shai Halevi and we thank him for his kind and immediate support throughout the whole process.

We would also like to thank the General Chairs, Çetin Kaya Koç and Erkay Savaş, local organizers Sally Vito and Whitney Morris (of UCSB Conference Services), Juan Manuel Escalante, who designed the CHES 2016 memorabilia, and the webmaster, Thomas Eisenbarth. Our thanks also go out to Matt Robshaw and Jonathan Katz, the Program Chairs of CRYPTO 2016, for the successful collaboration and alignment of the programs of CHES and CRYPTO. We are very grateful for the financial support received from our many generous sponsors.

Finally, among the numerous people that contributed to the success of CHES 2016, above all others are the authors who submitted their research papers to the conference. Without them, this conference would not exist. We enjoyed chairing the Program Committee and we hope you will enjoy these proceedings.

June 2016

Benedikt Gierlichs
Axel Y. Poschmann

Cryptographic Hardware and Embedded Systems -
CHES 2016

18th International Conference, Santa Barbara, CA, USA,

August 17-19, 2016, Proceedings

Gierlichs, B.; Poschmann, A.Y. (Eds.)

2016, XIV, 650 p. 159 illus., Softcover

ISBN: 978-3-662-53139-6