

Preface

The 17th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2015) was held at the Palais du Grand Large, Saint-Malo, France, September 13–16, 2015. The workshop was sponsored by the *International Association for Cryptologic Research*.

CHES 2015 received 128 submissions from all over the world. Each paper was anonymously reviewed by at least 4 Program Committee members. Papers submitted by Program Committee members were reviewed by at least 5 other Program Committee members. An impressive total of more than 510 reviews were written by the Program Committee members as well as the 210 external reviewers that offered their help to them. This year CHES implemented a new paper submission policy whereby the submissions needed to closely match the final versions in length and format published by Springer. During the review process we received thoroughly positive feedback on this new policy mostly because it allowed the Program Committee members to better anticipate the shape and content of each submission as it would appear in the proceedings. Finally, the Program Committee selected 34 papers for publication in these proceedings.

The program was completed by an excellent invited talk by Matthew Green from Johns Hopkins University on *Secure Protocols in a Hostile World*. In addition several papers were nominated for Best Paper Award and the Program Committee voted to award the Best Paper Award to Patrick Haddad, Viktor Fischer, Florent Bernard, and Jean Nicolai for their work on *A Physical Approach for Stochastic Modeling of TERO-based TRNG*. The other two papers on the podium were *Multi-variate High-Order Attacks of Shuffled Tables Recomputation* by Nicolas Bruneau, Sylvain Guilley, Zakaria Najm, and Yannick Tégli, and *Assessment of Hiding the Higher-Order Leakages in Hardware, What are the Achievements versus Overheads?* by Amir Moradi and Alexander Wild. The authors of these articles were invited to submit an extended version to the *Journal of Cryptology*. In addition, two tutorials were given on the day preceding the workshop by Debdeep Mukhopadhyay and Sikhar Patranabis on *Fault Analysis of Cryptosystems – Attacks, Countermeasures, and Metrics* as well as by David Oswald and Timo Kasper on *RFID and NFC Security in Practice*. As a continued tradition, CHES 2015 also featured two poster sessions on the second and third day of the conference.

Among the numerous people that contributed to the success of CHES 2015, we would first of all like to thank all the authors who submitted their research papers to the conference. Without them, this conference would not exist. The selection of the 34 papers that were eventually presented at the workshop was a challenging and time-consuming task and we sincerely thank the 41 Program Committee members as well as their external reviewers for the hard work and endless hours spent reviewing, assessing, and discussing each of the 128 submissions. This year, for each submitted paper, the authors also received a summary of the discussions that were held in the

Program Committee together with the reviewer comments. This meant that authors could be provided with feedback about the impact of their rebuttals. We would also like to sincerely thank Carolyn Whitnall and Kimmo Järvinen for taking excellent care of all aspects of the poster sessions including collecting and reviewing poster submissions and coordinating the presentation with the authors and local organizers.

We are very much indebted to the General Chairs, Emmanuel Prouff, Guénaél Renault, and Matthieu Rivain, for organizing all aspects of the conference in such a wonderful location; we also extend our thanks to Tancrede Lepoint, the webmaster, for promptly putting online all relevant information for submitters, authors of accepted papers, and conference attendees alike, as well as the local organizers for putting together an entertaining CHES Challenge.

The submission process as well as the review process and the editing of the final proceedings was greatly simplified by the software written by Shai Halevi and we thank him for his kind and immediate support throughout the whole process. Last but not least, we are very grateful for the financial support received from our many generous sponsors, including our Platinum Sponsor Cryptography Research, Gold Sponsors Serma Technologies, Thales, la Région Bretagne, and Pôle D'Excellence Cyber, as well as Sponsors Bosch, Texas Instruments, NXP, Riscure, UL, Orange Labs, Oberthur Technologies, Microsemi, Scytel, Invia, Technicolor, CEA, Infineon, ChaoLogix, SecureIC, and Gemalto.

We hope that the research published in this volume proves valuable to the CHES community and that all attendees enjoyed the event as much as we have enjoyed preparing it over the last few months.

June 2015

Tim Güneysu
Helena Handschuh

Cryptographic Hardware and Embedded Systems --
CHES 2015

17th International Workshop, Saint-Malo, France,

September 13-16, 2015, Proceedings

Güneysu, T.; Handschuh, H. (Eds.)

2015, XIV, 704 p. 204 illus., Softcover

ISBN: 978-3-662-48323-7