Introduction to the CHES 2013 special issue

Guido Bertoni · Jean-Sébastien Coron

Published online: 17 February 2014
© Springer-Verlag Berlin Heidelberg 2014

The 15th edition of the International Workshop on Cryptographic Hardware and Embedded System took place at the University of California, Santa Barbara, during August 20–23, 2013. This special issue hosts five extended versions of selected papers among those presented at the workshop.

CHES is an established event in the landscape of scientific conferences on security; it is considered a reference event that brings together academia and industry focused in the field of applied cryptography. The workshop covers a wide spectrum of subjects, from new implementations of cryptographic algorithms, advances in the field of side channel and fault attacks, countermeasures and secure implementations, protocols and security aspects of device manufacturing. The 15th edition of CHES received 132 submissions. The 43 members of the Program Committee were assisted by more than 190 external reviewers. In total, they delivered 463 reviews. Eventually, the Program Committee selected 27 papers (a 20 % acceptance rate) for publication in the proceedings. Among these 27 accepted papers, we have selected 5 that have received the best reviews in the process. Authors had the chance to extend their manuscripts, and extended manuscripts have been submitted to a second round of peer review.

The first paper, from Thomaz Oliveira, Julio López, Diego F. Aranha, and Francisco Rodríguez-Henríquez, is entitled “Two is the fastest prime: Lambda Coordinates for Binary Elliptic Curves”. In this work it is possible to see the advance-

ment of elliptic curves when implemented on a state of the art CPU. The paper received the CHES 2013 best paper award.

In the paper “Stealthy Dopant-Level Hardware Trojans: Extended Version” by Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson, the authors describe how to modify the behavior of a component in a malicious manufacturing environment while maintaining unchanged the metal layers of the chip. This is the so-called problematic of hardware trojans, where the intended behavior of a chip is changed in the manufacturing process, and these changes are well hidden and hard to detect.

The last three papers are related to the side-channel attacks field. In the paper “Using Bleichenbacher’s Solution to the Hidden Number Problem to Attack Nonce Leaks in 384-Bit ECDSA: Extended Version”, Elke De Mulder, Michael Hutter, Mark E. Marson, and Peter Pearson present a method for recovering the private key of a device executing the Elliptic Curve Digital Signature Algorithm. The Advanced Encryption Standard is the most widely used block cipher, and in “Masking vs. Multiparty Computation: How Large is the Gap for AES?”, Vincent Grosso, François-Xavier Standaert, and Sebastian Faust depict the progress in protecting it. Finally, in “On Measurable Side-Channel Leaks inside ASIC Design Primitives” by Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki, Mitsuru Shiozaki, and Takeshi Fujino, the authors provide an overview of the hardware building blocks and their side-channel leakage.

The guest editors would like to thank the reviewers of the special issue, the Springer editorial staff and the authors of the submissions.

G. Bertoni (✉)
STMicroelectronics, Milan, Italy
e-mail: guido.bertoni@st.com

J.-S. Coron
University of Luxembourg, Luxembourg, Luxembourg
e-mail: jean-sebastien.coron@uni.lu