J Cryptogr Eng (2015) 5:71–72
DOI 10.1007/s13389-015-0098-x

CHES 2014

Introduction to the CHES 2014 special issue

Lejla Batina[1] · **M. J. B. Robshaw**[2]

Published online: 1 May 2015

The 16th International Workshop on Cryptographic Hardware and Embedded Systems was held in Busan, Korea from September 23–26, 2014. The workshop was sponsored by the International Association for Cryptologic Research. This special issue of the Journal for Cryptographic Engineering (JCEN) contains extended versions of three of the papers that were presented at this workshop.

Each year CHES is one of the best-attended events among all the scientific conferences on security. It is considered by many to be the best leading indicator of the health and relevance of academic research on cryptography, its implementation, and most importantly, its deployment. The conference brings together experts from academia and industry and provides a narrow and focused insight into 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, and protocols and security aspects of device manufacturing.

CHES 2014 received 127 submissions from all parts of the globe. Each paper was reviewed by at least four independent reviewers, with papers from program committee members receiving at least five. The 43 members of the program committee were aided in this complex and time-consuming task by a further 203 external reviewers, providing striking testament to the size and robust health of the CHES community.

From among the 127 submissions, 33 were chosen for presentation at the workshop. They represented all areas of research that are considered to sit under the CHES umbrella, and they reflected the particular blend of the theoretical and practical that makes CHES such an appealing (and successful) workshop. Focusing our attention even further, from among these 33 accepted papers we have selected three that were particularly well-received during the review process. The authors of these papers were invited to submit extended manuscripts to JCEN and these extended manuscripts have been submitted to a second round of peer review. In order of submission to CHES 2014, these three papers are the following.

The paper *Fast Evaluation of Polynomials over Binary Finite Fields and Application to Side-channel Countermeasures* was authored by Jean-Sébastien Coron, Arnab Roy, and Srinivas Vivek. This paper can lead to performance improvements in the secure implementation of cryptographic S-boxes. More specifically, the paper considers the application of masking as a security countermeasure in the implementation of an S-box and the paper shows how to derive more efficient implementations for many of the S-boxes and S-box dimensions commonly found in the literature.

The paper *Reversing Stealthy Dopant-Level Circuits* was authored by Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, and Takeshi Fujino. This paper can be viewed, in part, as a response to a paper that was included in last years' special issue of JCEN that was devoted to CHES 2013. Sugawara et al. consider this earlier paper, among others, and show that the mechanisms by which it was suggested a malicious semiconductor foundry might hide a trap-door or trojan is, in fact, detectable. However, as the paper reveals, there are some trade-offs.

Finally, we include the paper *Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs* that was authored by Daniel Genkin, Itamar Pipman,

✉ M. J. B. Robshaw
mrobshaw@impinj.com

1 Radboud University, Nijmegen, The Netherlands

2 Impinj, Seattle, WA, USA

and Eran Tromer. This paper extends the art of side-channel cryptanalysis in yet another direction. Just by touching a laptop, the authors describe (and have implemented) attacks that can recover RSA and ElGamal secret keys when used in a widely available and widely used software implementation.

We hope that this selection of excellent papers from CHES 2014 helps the reader appreciate the range and sophistication of the topics that are covered by the CHES workshops. The guest editors would like to thank the paper reviewers, the Springer editorial staff, and all the authors for this special issue of the Journal of Cryptographic Engineering.