J Cryptogr Eng (2013) 3:1
DOI 10.1007/s13389-013-0055-5

Introduction to the CHES 2012 special issue

Emmanuel Prouff · Patrick Schaumont

Published online: 27 February 2013

The 14th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2012) was held at the Katholieke Universiteit Leuven, Belgium, during September 9–12, 2012. This special issue presents expanded versions of 5 of the best ranked papers from the CHES Workshop.

The CHES Workshop covers new results on all aspects of the design and analysis of cryptographic hardware and software implementations. The workshop builds a bridge between the cryptographic research community and the cryptographic engineering community. Since its inception in 1999, CHES has grown into the flagship event for the cryptographic engineering community. In this special issue, you will find 5 of the best ranked papers among the 120 submissions received by the workshop. These papers were identified based on the review scores of the CHES review process, and the expanded journal submissions of these papers received an additional, independent peer-review.

The five papers in this special issue reflect the broad spectrum of topics that is typically found in a CHES workshop and include physical hardware security, novel hardware architectures, and novel implementation attacks using faults and side-channel analysis. The first paper, "Simple Photonic Emission Analysis of AES", is by Alexander Schlösser, Dmitry Nedospasov, Juliane Krämer, Susanna Orlic, and Jean-Pierre Seifert. The authors describe how direct optical observation of on-chip transistor switching enables side-channel analysis. The second paper, "On the Use of Physical Unclonable Functions in Oblivious Transfer and Bit Commitment Protocols", is by Ulrich Rührmair and Marten van Dijk. The paper describes a novel attack on two recently proposed PUF protocols, as well as a suitable protocol improvement to thwart it. The third paper, "Code-based Cryptography on Reconfigurable Hardware: Tweaking Niederreiter Encryption for High Performance", is by Stefan Heyse and Tim Güneysu. The authors present new efficient FPGA implementations for the Niederreiter code-based public-key cryptosystem. The fourth paper, "Unified and Optimized Linear Collision Attacks and Their Application in a Non-Profiled Setting", is by Benoît Gérard and François-Xavier Standaert. The authors re-writte the problem of exploiting linear side channel collisions in block ciphers as a *low density parity check* code decoding problem. By combining this re-writing with a Bayesian extension of the collision detection techniques, they succeed in improving the efficiency and error tolerance of previously introduced attacks. The final paper, "Attacking RSA-CRT Signatures with Faults on Montgomery Multiplication", is by Pierre-Alain Fouque, Nicolas Guillermin, Delphine Leresteux, Mehdi Tibouchi, and Jean-Christophe Zapalowicz. The authors propose several new fault attacks against RSA-CRT, including the first fault attacks effective against RSA-PSS.

The guest editors of the special issue would like to thank all submitting authors for their excellent contributions. Furthermore, the guest editors also thank the reviewers of these expanded journal papers. Finally, the guest editors thank the Springer editorial staff and the editor-in-chief for this Journal for their help in the implementation of this special issue. We hope that the papers in this special issue will continue to inspire, guide, and clarify your academic and professional endeavors.

E. Prouff
French Network and Information Security Agency (FNISA), Paris, France
e-mail: e.prouff@gmail.com

P. Schaumont (✉)
Virginia Tech, Blacksburg, USA
e-mail: schaum@vt.edu