Journal of Cryptographic Engineering (2020) 10:287
https://doi.org/10.1007/s13389-020-00248-1

EDITORIAL

PROOFS 2018 Editorial

Lejla Batina[1] · Nele Mentens[2,3]

Accepted: 23 September 2020 / Published online: 20 October 2020

The goal of the PROOFS workshop is to promote methodologies that provably improve the security of embedded systems, especially those which contain cryptographic algorithms. More specifically, the PROOFS workshop seeks contributions in both theory and practice of methods and tools applied to the security of embedded systems. Examples include (semi-)formal methods, simulation-based leakage evaluation and security checks, protocol verification techniques, test and verification of secure embedded systems (software and hardware), and provable security for physical attacks.

This year's PROOFS workshop was held on September 13, 2018, in Amsterdam, the Netherlands. The workshop was held one day after the co-located conference CHES (*Cryptographic Hardware and Embedded Systems*), the flagship IACR conference on embedded systems security.

The morning session of PROOFS 2018 started with a keynote by Professor David Basin of ETH Zurich, who discussed model checking standards for security protocols. The afternoon session started with a keynote by Professor Catuscia Palamidessi of INRIA Saclay and LIX, Ecole Polytechnique, who talked about a machine learning approach to channel leakage estimation.

The presentations of the five contributed papers addressed several topics in the field of hardware and embedded security and evaluation: side-channel analysis, fault analysis, attack trees and the insertion of hardware Trojans. The authors of these papers were invited to submit extended versions to this special issue of *Journal of Cryptographic Engineering* on PROOFS 2018. After a thorough review process, three papers were accepted for publication and are presented in this special issue.

The PROOFS workshop organizers are grateful to the program committee members for their hard work in reading, evaluating and commenting the submissions. We would like to sincerely acknowledge the work of the program committee of PROOFS 2018, which was made up of:

- David Aspinall, University of Edinburgh
- Manuel Barbosa, HASLab—INESC TEC and FCUP
- Shivam Bhasin, Temasek Labs@NTU
- Begül Bilgin, Rambus Cryptography Research and KU Leuven
- Lukasz Chmielewski, Riscure
- Giorgio Di Natale, LIRMM
- François Dupressoir, University of Surrey
- Sebastian Faust, TU Darmstadt
- Tim Güneysu, Ruhr-Universität Bochum & DFKI
- Annelie Heuser, CNRS/IRISA
- Naofumi Homma, Tohoku University
- Ulrich Kühne, Télécom ParisTech
- Kerstin Lemke-Rust, Bonn-Rhein-Sieg University of Applied Sciences
- Debdeep Mukhopadhyay, IIT Kharagpur
- Stjepan Picek, Delft University of Technology
- Ilia Polian, University of Stuttgart
- Erik Poll, Radboud University
- Axel Poschmann, DarkMatter
- Francesco Regazzoni, ALaRI - USI
- Peter Schwabe, Radboud University
- Mehdi Tibouchi, NTT
- Gilles Van Assche, STMicroelectronics

Finally, we also thank all the participants of the workshop, for whom we hope PROOFS 2018 was a source of inspiration and collaboration for future projects in the security of embedded systems.
Lejla Batina, Radboud University
Nele Mentens, Leiden University and KU Leuven
Co-program chairs of PROOFS 2018

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

✉ Lejla Batina
lejla@cs.ru.nl

[1] Radboud University, Nijmegen, The Netherlands

[2] Leiden University, Leiden, The Netherlands

[3] KU Leuven, Leuven, Belgium