Introduction to the PROOFS 2016 special section

Naofumi Homma¹

© Springer-Verlag GmbH Germany 2017

The goal of the International Workshop on Security Proofs for Embedded Systems (PROOFS) is to promote methodologies that increase the confidence level in the security of embedded systems. Formal methods for verification and safety are used in several related fields, such as software; however, the security of embedded systems, including cryptographic hardware and software, is often challenged by many attacks, particularly at the implementation level. Strategies to secure embedded systems are known, but they need to be implemented with care. The main objective of the PROOFS workshop is to bridge the gap between both topics and thus pave the way to verifiable *security by design* for embedded systems. The workshop is an opportunity for researchers of different fields to exchange on their work and also to present some innovative use-cases and/or proofs of concept.

The fifth edition of the PROOFS workshop was held on Saturday August 20, 2016, at Santa Barbara in USA. As all previous editions, PROOFS workshop was scheduled the day after CHES (*Cryptographic Hardware and Embedded Systems*), the flagship IACR conference on embedded systems security. The PROOFS Workshop 2016 featured two invited talks. Yuval Yarom (from The University of Adelaide and Data61, Australia) gave a talk on the following topic: *Thwarting cache-based side-channel attacks*. Ryan Kastner (from University of California, San Diego, USA) talked about *Moving Hardware from “Security through Obscurity” to “Secure by Design”*.

The rest of the program included six contributed papers selected out of ten submissions. All the papers were finally offered a long slot (30 min each) this year. The accepted papers have been revised after the PROOFS workshop, and improved, notably to reflect the comments made by the audience in the *question and answer* session in addition to the ones made by the reviewers. After a second review process in the *Journal of Cryptographic Engineering*, the papers have all been accepted for publication. They appear in this special issue of the JCEN on PROOFS.

In order to increase social interaction within the PROOFS community, a welcome dinner is customarily organized on the eve of PROOFS. For this year, it took place at a cozy restaurant in the downtown of Santa Barbara city. I am very grateful to Çetin Kaya Koç and Erkan Savaş for their excellent local arrangements of the dinner as well as the workshop.

The PROOFS program committee chair is very indebted to the program committee members for their hard work in reading, evaluating, and commenting the submissions. Each paper was reviewed by at least three program committee members. In total, the program committee produced 30 reviews, which brought some feedback to the authors of the submitted papers.

I would like to sincerely acknowledge the work of the program committee of PROOFS 2016, which was made up of: Alessandro Barengi, Begül Bilgin, Joan Daemen, François Dupressoir, Nadia El Mrabet, Emmanuelle Encrenaz, Sylvain Guilley, Debdeep Mukhopadhyay, Renaud Pacalet, Stjepan Picek, Marie-Laure Potet, Axel York Poschmann, Mehdi Tibouchi, Chao Wang, and Yongbin Zhou. They were helped by nine sub-reviewers. I also thank a lot: Lejla Batina, Jeroen Delvaux, Simon Friedberger, Karine

✉ Naofumi Homma
homma@iec.tohoku.ac.jp

¹ Tohoku University, Sendai, Japan

Heydemann, Bodhisatwa Mazumdar, Durga Prasad Sahoo, Vincent Verneuil, and Hailong Zhang, and I would also like to acknowledge the Steering Committee for giving me the opportunity of serving as the program committee chair of PROOFS 2016. In particular, I thank Sylvain Guilley for his help and guidance throughout the process.

Finally, I thank all the participants, who enjoyed the workshop in a nice conference room with its relaxed atmosphere on the campus of UCSB.

Naofumi Homma
Program Chair of PROOFS 2016