J Cryptogr Eng (2017) 7:97–98
DOI 10.1007/s13389-017-0158-5

Introduction to the CHES 2016 special issue

Benedikt Gierlichs[1] · **Axel Y. Poschmann**[2]

Published online: 29 March 2017

This special issue of the *Journal of Cryptographic Engineering* (JCEN) contains extended versions of four of the papers that were presented at the 18th *Conference on Cryptographic Hardware and Embedded Systems* (CHES 2016), held at the University of California at Santa Barbara, CA, USA, August 17–19, 2016. The conference was sponsored by the *International Association for Cryptologic Research*, and—after 2010 and 2013—it was the third time that CHES was co-located with CRYPTO. CHES is considered to be the leading conference in the domain of embedded security, in particular the implementation and deployment aspects of security and cryptography. It aims at bridging theory and practice by bringing together attendees from industry, government agencies, and academia.

CHES 2016 received a record 148 submissions, and each paper was anonymously reviewed by at least four Program Committee members in a double-blind peer-review process. With the help of 210 external reviewers, our 47 Program Committee members wrote an impressive total of 623 reviews. The Program Committee selected 30 papers for publication, corresponding to a 20% acceptance rate. The authors of the best rated papers received invitations to submit extended manuscripts to the *Journal of Cryptology* or the *Journal of Cryptographic Engineering*. Submissions to this special issue of JCEN went through scientific journal peer review.

✉ Benedikt Gierlichs
benedikt.gierlichs@esat.kuleuven.be

Axel Y. Poschmann
axel.poschmann@gmail.com

[1] KU Leuven, Leuven, Belgium

[2] NXP Semiconductors, Hamburg, Germany

A particularly pressing topic today is to address the security challenges of the *Internet of Things* (IoT), and this is the focus of this special issue of JCEN. Among the many different aspects of IoT security, security-by-design and independent third-party testing and certification are among the most relevant to address the security challenges in the long run. However, before the fruits of these efforts can be harvested, it seems that for the years to come, the adversaries will benefit from a combined attack surface of IoT devices, as they are both deployed in the field and connected to the Internet.

In general, IoT security merges two more or less distinct research domains together and opens many interesting research questions:

1. The *Things* domain (also called embedded security) with mostly offline, embedded, and constrained devices that are deployed "in the field" hence can be attacked with physical, local attacks such as side-channel analysis, fault injection, and tampering attacks;
2. The *Internet* or cloud domain (a.k.a. network security) with mostly remote, software-driven, and noninvasive attacks, that sees more and more research in the direction of applying Artificial Intelligence techniques or big data analysis to solve security challenges.

A by-product of the merger of these two domains is an ever-growing cross-fertilization of attack vectors previously only applied in one domain, which are now applied to the other domain. *CacheBleed: A Timing Attack on OpenSSL Constant Time RSA* is an example for a local attack vector that is used to remotely attack a cloud instance. This can be seen as a modern version of Bleichenbacher's Million Message attack from two decades ago [1].

In a way, applying machine learning to attack a security concept that exploits intrinsic hardware features (like a *Physical Unclonable Function*, PUF) is a cross-fertilization from the Internet or better cloud domain to the Things domain. *Having No Mathematical Model May Not Secure PUFs* introduces a framework for assessing the resistance of a PUF to machine learning attacks, this way providing an important addition to the toolbox of PUF designers.

Independent third-party testing and certification is crucial to have transparent security levels for the user. This is an essential component to achieve IoT security by incentivizing investments in security. An important open challenge is the comparability of evaluation results from different evaluators. *Towards Easy Leakage Certification* proposes a theoretical framework for this open challenge.

Another important aspect is security-by-design. *Strong 8-bit Sboxes with Efficient Masking in Hardware* addresses the challenges posed by IoT constraints (low cost, low power, low gate count, adversaries have physical access) by proposing new Sboxes, which can be used to design new crypto primitives with efficient yet highly secure hardware implementations.

We hope that this selection of excellent papers from CHES 2016 helps to address some of the most pressing topics in IoT security. Finally, the guest editors would like to thank the paper reviewers, the Springer editorial staff, and all the authors for their invaluable support for this special issue of the *Journal of Cryptographic Engineering*.

Reference

1. Bleichenbacher, D.: Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In: Krawczyk, H. (ed.) Advances in Cryptology—CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 23–27, 1998, Proceedings, vol 1462, pp. 1–12. Springer, Lecture Notes in Computer Science (1998)