Journal of Cryptographic Engineering (2018) 8:93–94
https://doi.org/10.1007/s13389-018-0189-6

CHES 2017

Introduction to the CHES 2017 special issue

Wieland Fischer[2] · **Naofumi Homma**[1]

© Springer-Verlag GmbH Germany, part of Springer Nature 2018

This special issue of the Journal of Cryptographic Engineering (JCEN) contains extended versions of three of the papers that were presented at the 19th Conference on Cryptographic Hardware and Embedded Systems (CHES 2017), held in Taipei, Taiwan, September 25–28, 2017. The conference was sponsored by the International Association for Cryptologic Research. 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 2017 received 130 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 240 external reviewers, our 50 Program Committee members wrote an impressive total of 559 reviews. The Program Committee selected 33 papers for publication, corresponding to a 25% 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. The selected papers for this special issues represent a wide range of typical CHES topics, including the state-of-the-art cryptographic implementation, protection schemes against side-channel analysis, and an advanced side-channel analysis technique on FPGA implementation. The authors of these papers were invited to submit extended manuscripts to this special issue of JCEN, and these extended manuscripts went through scientific journal peer review.

The paper *McBits Revisited: Toward a Fast Constant-Time Code-Based KEM* by Tung Chou presents a fast constant-time implementation for a high-security code-based key encapsulation mechanism (KEM). The implementation is based on the "McBits" paper by Bernstein, Chou, and Schwabe in 2013: They use the same FFT algorithms for root finding and syndrome computation, similar algorithms for secret permutation, and bit slicing for low-level operations. As opposed to McBits, where a high decryption throughput is achieved by running many decryption operations in parallel, this paper takes a different approach to exploiting the internal parallelism in one decryption operation for the use of more applications. As a result, a better decryption throughput at a much higher security level than McBits is successfully achieved. This paper also presents a constant-time implementation for encryption and key pair generation, with similar techniques used for decryption.

The paper *A Unified Masking Approach* by Hannes Gross and Stefan Mangard presents a unified masking method that combines existing software and hardware masking schemes in order to provide resistance against side-channel analysis (SCA) at a high level of security. The authors demonstrate how to protect software and hardware implementations using the presented masking algorithm for lower costs of randomness compared to the solitary schemes. An impressive result is that in some cases of hardware implementations these costs of randomness can be halved compared to the state-of-the-art methods. Theoretical considerations as well as practical implementation results are also presented for a comparison with existing schemes from different perspectives and at different levels of security.

The paper *Your Rails Cannot Hide From Localized EM: How Dual-Rail Logic Fails on FPGAs—Extended Version* by Vincent Immler, Robert Specht, and Florian Unterstein shows a new attack using high-resolution electromagnetic analysis. It is able to exploit local characteristics of the placement and routing from DPA-resistant dual-rail logic circuit implemented on FPGAs such that only a marginal security gain remains. It is therefore creating a severe threat while previous works show a significant security gain for power analysis when using such logic on FPGAs. In order to further analyze the properties of both attack and implementation, the authors also develop a custom placer to improve the default placement of the analyzed AES S-box. Different cost functions for the placement are tested and evaluated with regard to the resulting side-channel resistance on a Spartan-6 FPGA.

✉ Naofumi Homma
naofumi.homma.c8@tohoku.ac.jp

[1] Tohoku University, Sendai, Japan

[2] Infineon Technologies AG, Neubiberg, Germany

As a result, they achieved more than double the resistance of the design compared to cases not benefiting from the custom placement.

We hope that this selection of excellent papers from CHES 2017 provides another evidence of the broad coverage and sophistication of research that is part of the CHES community. 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.

Wieland Fischer and Naofumi Homma
Program Co-Chairs of CHES 2017