J Cryptogr Eng (2016) 6:83–84
DOI 10.1007/s13389-016-0130-9

CrossMark

CHES 2015

Introduction to the CHES 2015 special issue

Tim Güneysu[1] · **Helena Handschuh**[2]

Published online: 20 April 2016

This Special Issue of the *Journal of Cryptographic Engineering* (JCEN) presents extended versions of selected works presented at the 17th International Workshop on Cryptographic Hardware and Embedded Systems that was held in Saint-Malo, France from September 13 to 16, 2015. The workshop was sponsored by the International Association for Cryptologic Research. With more than 430 participants, CHES is one of the best-attended events among all the scientific conferences on security. One of its major goals is to bridge theory and practice in academic research on cryptography with a strong focus on secure implementations and deployment. In this sense, the conference brings together experts from academia and industry to explore the field of applied cryptography in the broader context of embedded systems. The workshop covers a wide spectrum of subjects, from new implementations of cryptographic algorithms, to advances in the field of side channel and fault attacks, to countermeasures and secure implementations, and protocols and security aspects of device manufacturing. CHES 2015 received 128 submissions from all parts of the globe. Each paper was reviewed by at least four independent reviewers, with papers from program committee members receiving at least five reviews. The 44 members of the program committee were aided in this complex and time-consuming task by a further 210 external reviewers, resulting in a total of more than 510 reviews written during the paper selection process. From the 128 submissions, 34 were chosen for presentation at the workshop. They represented all areas of research including constructive and destructive topics reflecting a mix of theoretical and practical results that make CHES such an appealing and successful workshop. Focusing our attention even further, from these 34 accepted papers we have selected five that were particularly well-received during the review process. Furthermore, they represent a wide range of typical CHES topics, including leakage assessment techniques, timing attacks on protected implementations, key generation techniques from physically unclonable functions (PUF), side-channel countermeasures for modern cryptographic implementation and a cryptanalytic improvement on a widely practically used cipher. The authors of these papers were invited to submit extended manuscripts to JCEN and these extended manuscripts underwent a second round of peer review. The papers that successfully passed this process are the following.

The paper *Leakage Assessment Methodology—extended version*—was authored by Tobias Schneider and Amir Moradi. This paper aims at studying the theoretical background of the different flavors of statistical tests used in side-channel analysis. It focuses particularly on Welch's t test which is particularly capable to avoid the undesired dependency between the evaluations and the device's underlying architecture. The authors present a roadmap which is designed to be followed by the evaluation labs to efficiently and correctly conduct these test procedures. Besides general considerations, the paper also proposes a robust approach to perform the tests at higher orders and includes two case studies to provide evidence for its practical feasibility.

The paper *Exclusive Exponent Blinding is Not Enough to Prevent Any Timing Attack on RSA* is an extended version of the work by Werner Schindler presented at CHES 2015. This work presents a timing attack on RSA implementations that apply the Chinese Remainder Theorem (CRT)

✉ Tim Güneysu
gueneysu@informatik.uni-bremen.de

Helena Handschuh
Helena.Handschuh@cryptography.com

[1] University of Bremen and DFKI, Bremen, Germany

[2] Cryptography Research Inc., San Francisco, USA

and Montgomery's multiplication algorithm, even when protected by the common countermeasure of exponent blinding. The attack is applicable both to square and multiply exponentiation and to table-based exponentiation algorithms, and extends previous work on timing attacks on unprotected implementations. In fact, the attack can be avoided when additional implementation constraints are enforced, such as avoiding extra-reductions in the modular exponentiation procedure when using an enlarged radix ensuring that $R > 4p$. Alternatively, the combination of exponent blinding with further countermeasures (such as base blinding) can also help to prevent this attack.

Further, we included an extended version of the paper *Secure Key Generation from Biased PUFs* authored by Roel Maes, Vincent van der Leest, Erik van der Sluis, and Frans M. J. Willems. In this paper, the authors show how to solve the open problem of generating keys from less-then-full entropy PUFs. The authors present a proposal that efficiently debiases PUFs which have biased output bits using code-offset-based constructions for error correction. Arbitrary levels of bias can be addressed while maintaining reliability and reusability of the key generator. As an example, the authors present a use-case that derives a secure 128-bit key from a 15 %-noisy and 25 %-biased PUF demanding for only 4890 PUF bits and 7392 PUF bits for the non-reusable and reusable variant, respectively. To date, we found no other reports on suitable methods that are capable to securely derive a key from such heavily biased PUF instance.

The article *Masking ring-LWE* is a joint work by Oscar Reparaz, Sujoy Sinha Roy, Ruan de Clercq, Frederik Vercauteren, and Ingrid Verbauwhede. In this article, the authors propose a first-order side-channel resistant implementation for the lattice-based ring-LWE encryption scheme. It is the first time to date that a masking technique for lattice-based cryptography is reported. In the respective cryptosystem, the authors identified the decoding step of the decryption process as a crucial component for side-channel leakage so that they put particular emphasis on the efficient design for a correspondingly masked decoder. They implement the fully masked architecture in hardware with only 20 % overhead and a factor 2.6 in execution time compared to an unprotected implementation. We believe that this work is a first step towards the development of physical protection techniques for the emerging field of lattice-based cryptosystems that can inspire further research projects on open topics, such as the efficient CCA2-security conversion or countermeasures against fault-injection attacks.

Finally, we include the paper *Improved Cryptanalysis of the DECT Standard Cipher* that was authored by Iwen Coisel and Ignacio Sanchez. The DECT Standard Cipher (DSC) is a non-public and proprietary stream-cipher used in a wide range of cordless phones to protect the privacy of the personal voice communications worldwide and thus of high interest for the CHES community. This work presents improved cryptanalysis over the previously published attacks by Nohl–Tews–Weinmann that requires substantially less plaintext material compared to the original attack. The article in this issue extends the original CHES paper by an analysis of scenarios where the knowledge of the plaintext is not 100 % accurate. More precisely, the best results require less than 3 min of only 90 % accurately recorded communication and break the key with practical key search capabilities. This suggests the key should be changed as frequently as every 30 s in real-life systems or the newer version of the algorithm should be used.

We hope that this selection of excellent papers from CHES 2015 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*.