Guest Editorial

Christof Paar

Ruhr University of Bochum, Bochum, Germany
Christof.Paar@rub.de

Jean-Jacques Quisquater

Université catholique de Louvain, Louvain-la-Neuve, Belgium

Berk Sunar

WPI, Worcester, MA, USA

Online publication 16 March 2011

Since the beginning of modern cryptology in the early 1970s our field was viewed as being based on computer science and certain sub-disciplines of mathematics, especially number theory and algebra. However, hardware aspects, with their close link to engineering, have always played a role too. To name only two examples, the design of DES was heavily influenced by the desire for a cipher with low hardware costs, and the RSA inventors worked on chip architectures in the early days of their algorithm. With the increase in commercial security applications in the 1990s hardware aspects became more important for industry, and the CHES (Cryptographic Hardware and Embedded Systems) workshop series has become a fixture in the cryptography community.

With the more recent advent of pervasive computing, a host of new devices with security needs—such as smart phones, RFID tags, media players with DRM schemes like the iPod or Kindle, smart power meters, medical implants and many other applications like cars—have arrived. The standard black-box model in which the attacker is assumed to have only access to the I/O channels no longer applies, as the opponent will potentially own the platform. The physical implementation provides an attacker with a wealth of information related to the cryptographic implementation, as she may listen to and tamper with the physical environment of the platform. Even the strongest cryptographic scheme with a rigorous security proof in the classical black-box model may succumb to physical attacks. Specifically, there are information leakages which allows a passive attacker who captures side-channel profiles a means to deduce cryptographic keys. Similarly, active physical attacks aim at extracting secret information by injection faults during the execution of an algorithm. At the same time, the interaction between physical realization and crypto algorithms offers new opportunities for security designers. For instance, subtle variations of the device characteristics can be exploited for key generation or identification. Physical unclonable functions (PUFs) based on manufacturing variations of delays, capacitive load, and on initial memory content are one

example for a constructive use of the interaction between the physical platform and the security function.

This special issue consists of seven articles at the intersection of cryptology and hardware. All papers are original research contributions which advance the state-of-the-art in this fast moving field. Three of the papers address the important area of fault injection attacks and how to protect against them. Two other papers deal with side-channel analysis, where one contribution addresses the theory and the other provides highly efficient ways of protecting symmetric ciphers against such attacks. One article advances PUFs, an emerging and very promising auxiliary function in the cryptographic toolkit. Somewhat related to PUFs are true random-number generators, which are addressed in the final paper; even though TRNGs have been known for a long time their security is still not fully understood. We are extremely happy with this cross-section of applied crypto research and we are confident that the papers in this special issue will be very helpful for researchers in the future.

At this point, we would like to express our gratitude toward all authors for their excellent work and their patients with small delays. We also regret that many good submissions could not be accepted due to space constraints. This issue would not have been possible without the many referees who did an outstanding job reviewing the papers in a timely manner and with great care. Our thanks also go to the Editor-in-Chief, Matt Franklin, and Jennifer Evans from Springer for their support and encouragement.

August 2010