Guest Editorial

Claude Carlet · Pierre-Alain Fouque

Accepted: 2 October 2014 / Published online: 15 October 2014
© Springer Science+Business Media New York 2014

Over the last decade, side-channel analysis has emerged as an important research area in cryptography with many theoretical and practical issues. Since the seminal works of Kocher in 1996 and 1999 about timing and differential power analysis, many attacks, countermeasures, provable security proofs have been published. Side channel attacks allow to take into account the security of the implementation by looking at intermediate variables while classical black-box cryptanalyses only consider input/output variables. The main characteristic of these attacks is that they lead to very practical attacks even on very strong cryptographic primitives such as AES.

In light of this, we thought that a special issue on “Side Channel Attacks and their Countermeasures” could be of interest to the cryptology community. This is to harness some important research contributions devoted towards side-channel analysis into a single literary volume with substantial archival value.

For this special issue, we solicited the following in the field of side-channel analysis:

1. novel research contributions;
2. research contributions previously published or presented at conferences and workshops, with substantial revision and new contributions;
3. expository survey articles in relevant topics.

We received 12 submissions and most of them were of publishable quality. After a detailed two round review process (at a similar standard for the invited as well as the contributed papers), we could accept seven papers for this special issue.

C. Carlet (✉)
Universités Paris 8 and 13, 2 rue de la liberté, 93526 Saint-Denis, Cedex, France
e-mail: Claude.Carlet@univ-paris8.fr

P.-A. Fouque
Université Rennes 1 and Institut Universitaire de France, 263 avenue du Général Leclerc,
Campus de Beaulieu, 35042 Rennes Cedex, France
e-mail: Pierre-Alain.Fouque@ens.fr

These 7 papers show the power of side-channel attacks on various implementations of public-key and secret-key cryptography. Two papers present attacks on Elliptic Curve and Pairing cryptography, while the others consider symmetric cryptography. One of these describes some attacks and shows how it is possible to recover some secret parameters of an AES-like cipher. Another one studies two different countermeasures, masking and leakage resilient scheme. Two papers study S-boxes in the framework of side channel attacks and one investigates the output of multiplicative operations.

We would like to thank the authors of all the submitted papers and express our gratitude to the referees for their timely and thorough review work. Finally, we must acknowledge that this special issue would not have been possible without the support of people in the editorial office of the journal.