

# Preface

The 6th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) was held in Berlin, Germany, during April 13–14, 2015. This workshop each year brings together researchers and experts from academia, industry, and government who are working on cryptographic implementations and secure design.

COSADE 2015 received 48 submissions in the domain of side-channel analysis, fault attacks, and secure design, out of which 17 papers were selected. Each paper was reviewed by at least four independent reviewers. The Program Committee consisted of 33 members from 12 countries in America, Asia, and Europe who were carefully selected to represent a balanced view of both academia and industry. The members of the Program Committee were supported in their challenging task by 82 external reviewers. We would like to thank all committee members and reviewers for their hard work. The submission and reviewing process was done using the EasyChair system.

We were excited that Ross Anderson and Emmanuel Prouff accepted our invitations to give invited talks. Ross Anderson provided an excellent overview on “Why Cryptosystems Still Fail”, while Emmanuel Prouff expounded on “Algorithmic Approaches to Defeat Side Channel Analysis”. Beside the invited talks and the accepted papers, an update of the current state of the DPA Contest v4 was also presented at COSADE 2015. The paper “Side-Channel Security Analysis of Ultra-Low-Power FRAM-based MCUs” by Amir Moradi and Gesine Hinterwaelder received the best paper award.

We would like to thank the local organizers, in particular Claudia Petzsch and Matthias Petschik, as well as the general chair Jean-Pierre Seifert, for their support and for making this great event possible. On behalf of the COSADE community we would also like to thank the COSADE 2015 sponsors. Finally and most importantly, we would like to thank the authors for their excellent contributions.

May 2015

Stefan Mangard  
Axel Y. Poschmann

Constructive Side-Channel Analysis and Secure Design  
6th International Workshop, COSADE 2015, Berlin,  
Germany, April 13-14, 2015. Revised Selected Papers  
Mangard, S.; Poschmann, A.Y. (Eds.)  
2015, X, 271 p. 87 illus., Softcover  
ISBN: 978-3-319-21475-7