

# Preface

The 7th International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) was held in Graz, Austria, during April 14–15, 2016. This now well-established workshop brings together researchers from academia, industry, and government who share a common interest in the design and secure implementation of cryptographic primitives. COSADE 2016 received 32 submission; the review process relied on the EasyChair system.

From the pool of submissions, 12 high-quality papers were selected carefully after deliberations of the 30 Program Committee members who were supported by 24 additional reviewers. The composition of the Program Committee was representative of the good mix between academic and industrial researchers as well as the geographic spread of researchers across the globe. We would like to express our sincere gratitude to both the Program Committee members and reviewers.

As it has become custom, the Program Committee members voted on the best paper among the accepted papers. The resulting winner was “Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption” authored by Thomas Unterluggauer and Stefan Mangard. The program also featured three invited talks. Tom Chothia elaborated on advanced statistical tests for detecting information leakage. François Dupressoir spoke about formal and compositional proofs of probing security for masked algorithms. Aurélien Francillon discussed what security problems can be spotted with large-scale static analysis of systems. We would like to thank the invited speakers for joining us in Graz.

Finally, we would like to thank the local organizers, in particular Stefan Mangard (general chair) and Thomas Korak, for their support and for making this great event possible. On behalf of the COSADE community we would also like to thank our GOLD sponsors Infineon Technologies AG, NewAE Technology Inc., NXP Semiconductors, Riscure, and Secure-IC, as well as our SILVER sponsors Rambus Cryptography Research and Oberthur Technologies, for their support.

And most importantly, we would like to thank the authors for their excellent contributions.

May 2016

Elisabeth Oswald  
François-Xavier Standaert

Constructive Side-Channel Analysis and Secure Design  
7th International Workshop, COSADE 2016, Graz,  
Austria, April 14-15, 2016, Revised Selected Papers  
Standaert, F.-X.; Oswald, E. (Eds.)  
2016, X, 219 p. 74 illus., Softcover  
ISBN: 978-3-319-43282-3