Foreword

It is our great pleasure to welcome you to the Theory of Implementation Security (TIS) Workshop 2016, co-located with ACM CCS 2016. In this workshop, we focus on physical attacks and their countermeasures. Considering the limitations of an IoT device, we emphasize on efficiency and applicability. A special topic of interest is advances in theory and practice of Threshold Implementations (TIs). Threshold Implementation is proposed as a countermeasure against side-channel attacks (SCA) in 2006. This masking based method has been extended to higher-order SCA and has attracted a lot of attention due to its efficiency and generality in recent years. In order to celebrate the 10th anniversary of TIs' design, this workshop specially focuses on novel results on TIs.

The program contains 3 technical contributed talks, 3 invited talks and 3 short presentations of recent results related to the topics of TIs - either not published yet or published recently elsewhere. We are pleased to welcome the keynote speakers, who will present the following invited lectures:

- *Masking and MPC: When Crypto Theory Meets Crypto Practice,* Nigel Smart (University of Bristol)
- *Threshold Implementations in Industry: A Case Study on SHA-25,* Mike Hutter (Cryptography Research – Rambus)
- *On Non-uniformity in Threshold Sharings,* Joan Daemen (Radboud University Nijmegen and STMicroelectronics)

Putting together *Theory of Implementation Security Workshop 2016* was a team effort. We first thank the authors for providing the content of the program. We are grateful to the program committee for reviewing the papers and providing feedback to the authors. Finally, we thank our sponsor, ACM SIGSAC; our supporter, NXP; and ACM CCS for providing the local organization.

We hope that you will find this program interesting and thought-provoking and that the symposium will provide you with a valuable opportunity to share ideas with other researchers and practitioners from around the world.

Begül Bilgin
TIS Program Chair
KU Leuven, Belgium

Svetla Nikova
TIS Program Chair
KU Leuven, Belgium

Vincent Rijmen
TIS Program Chair
KU Leuven, Belgium