Preface

The 23rd International Conference on Fast Software Encryption (FSE 2016) was held at Bochum, Germany, during March 20–23, 2016. The conference was organized by Ruhr University Bochum with Gregor Leander serving as the general chair in collaboration with the International Association for Cryptologic Research (IACR). The conference had about 150 registered participants from 28 different countries. FSE 2016 received 91 submissions. The 25 members of the Program Committee were assisted by more than 80 external reviewers. In total, they delivered 304 reviews, with each submission being reviewed by at least three Program Committee members, five in the case of a submission co-authored by members of the Program Committee. The review process was double-blind, and conflicts of interest were handled carefully. It was managed through an online review system that supported discussions among Program Committee members. Eventually, the Program Committee selected 29 papers from 16 countries (a 31.9 % acceptance rate) for publication in the proceedings.

Besides the 29 selected talks, the program included one invited talk by Henri Gilbert from ANSSI, France, on white-box cryptography. The workshop also featured a rump session, chaired by Dan Bernstein and Tanja Lange, with several short informal presentations.

As in previous FSE events, the Program Committee identified the best submissions of the conference for their scientific quality, their originality, and their clarity. The FSE 2016 Best Paper Award went to José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, and François Dupressoir, for their paper "Verifiable Side-Channel Security of Cryptographic Implementations: Constant-Time MEE-CBC." This paper, along with the article "Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression" by Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey received a special invitation for submission to the *Journal of Cryptology*.

Many people contributed to FSE 2016. I would like to thank the authors for contributing their excellent research, but also the Program Committee members and their external reviewers, who spent a lot time and effort reading and analyzing the numerous submissions. I really enjoyed the discussions during the selection phase and I am particularly grateful to Alex Biryukov, Christina Boura, Svetla Nikova, Yu Sasaki, François-Xavier Standaert, and Marc Stevens for accepting to shepherd papers. Finally, I sincerely thank Gregor Leander, the general chair, and his organization team, who worked so hard for the conference to be pleasant for all attendees. Their smooth organization made the event a big success.

I was extremely honored to serve as Program Chair of FSE 2016. The program contained a wide spectrum of the latest research in symmetric cryptography, ranging from cryptanalysis to security proofs, practical implementation aspects to foundations, and considering various primitives such as block ciphers, stream ciphers, hash functions, authenticated encryption, MAC, etc. I hope the selected papers will consolidate

our knowledge in symmetric cryptography, but also open new directions to continue making symmetric cryptography a vibrant research community.

May 2016 Thomas Peyrin

http://www.springer.com/978-3-662-52992-8

Fast Software Encryption
23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers
Peyrin, Th. (Ed.)
2016, XI, 592 p. 105 illus., Softcover
ISBN: 978-3-662-52992-8