Preface

The RSA conference has been a major international event for information security experts since its inception in 1991. It is an annual event that attracts hundreds of vendors and thousands of participants from industry, government, and academia. Since 2001, the RSA conference has included the Cryptographers' Track (CT-RSA), which provides a forum for current research in cryptography. CT-RSA has become a major publication venue in cryptography. It covers a wide variety of topics from public-key to symmetric-key cryptography and from cryptographic protocols to primitives and their implementation security.

This volume represents the proceedings of the 2015 RSA Conference Cryptographers' Track which was held in San Francisco, California, during April 21–24, 2015. A total of 111 full papers were submitted for review out of which 26 papers were selected for presentation. As Chair of the Program Committee, I heartily thank all the authors who contributed the results of their innovative research and all the members of the Program Committee and their designated assistants who carefully reviewed the submissions. In the thorough peer-review process that lasted 2 months, each submission had three independent reviewers. The selection process was completed at a discussion among all members of the Program Committee.

In addition to the contributed talks, the program included a panel discussion moderated by Bart Preneel on *Post-Snowden Cryptography* featuring Paul Kocher, Adi Shamir, and Nigel Smart.

February 2015 Kaisa Nyberg

http://www.springer.com/978-3-319-16714-5

Topics in Cryptology -- CT-RSA 2015
The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings
Nyberg, K. (Ed.)
2015, XIII, 508 p. 79 illus., Softcover
ISBN: 978-3-319-16714-5