

# 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 2016 RSA Conference Cryptographers' Track, which was held in San Francisco, California, from February 29 to March 4, 2016.

A total of 76 full papers were submitted for review, out of which 26 papers were selected for presentation. As chair of the Program Committee, I deeply thank all the authors who contributed the results of their innovative research. My appreciation also goes to all the members of the Program Committee and the designated external reviewers who carefully reviewed the submissions. Each submission had at least three independent reviewers, and those authored/co-authored by a member of the Program Committee had six reviewers. The process of selection was very difficult, as each submission had different aspects in its contribution. It was carried out with enthusiastic discussion among the members of the Program Committee in a transparent manner.

In addition to the contributed talks, the program included a panel discussion moderated by Bart Preneel on "The Future of Bitcoin and Cryptocurrencies."

December 2015

Kazue Sako

Topics in Cryptology - CT-RSA 2016

The Cryptographers' Track at the RSA Conference

2016, San Francisco, CA, USA, February 29 - March 4,

2016, Proceedings

Sako, K. (Ed.)

2016, XI, 465 p. 68 illus. in color., Softcover

ISBN: 978-3-319-29484-1