

# Preface

The RSA Conference is attended by over 10,000 security professionals each year. The Cryptographers' Track (CT-RSA), one of several parallel tracks at the conference, provides an excellent opportunity for cryptographers to showcase their research to a wide audience. CT-RSA 2005 was the fifth year of the Cryptographers' Track.

The selection process for the CT-RSA program is the same as for other cryptography research conferences. This year, the program committee selected 23 papers from 74 submissions (two of which were later withdrawn) that covered all aspects of cryptography. The program also included two invited talks by Cynthia Dwork and Moti Yung. These proceedings contain the revised versions of the selected papers. The revisions were not checked, and so the authors (and not the committee) bear full responsibility for the contents of their papers.

I am very grateful to the program committee for their very conscientious efforts to review each paper fairly and thoroughly. The initial review stage was followed by a tremendous amount of discussion which contributed to our high confidence in our judgements. Thanks also to the many external reviewers whose names are listed in the following pages. My apologies to those whose names were inadvertently omitted from this list.

Thanks to Eddie Ng for maintaining the submission server and the Web review system. The submission software was written by Chanathip Namprempre, and the Web review software by Wim Moreau and Joris Claessens. Thanks to Alfred Hofmann and his colleagues at Springer for the timely production of these proceedings. Finally, it is my pleasure to acknowledge Ari Juels and Mike Szydlo of RSA Laboratories for their assistance and cooperation during the past seven months.

October 2004

Alfred Menezes

Topics in Cryptology -- CT-RSA 2005

The Cryptographers' Track at the RSA Conference

2005, San Francisco, CA, USA, February 14-18, 2005,

Proceedings

Menezes, A.J. (Ed.)

2005, X, 390 p., Softcover

ISBN: 978-3-540-24399-1