Preface

The Cryptographers’ Track (CT-RSA) is a research conference within the RSA conference, the largest, regularly staged computer security event. CT-RSA 2004 was the fourth year of the Cryptographers’ Track, and it is now an established venue for presenting practical research results related to cryptography and data security.

The conference received 77 submissions, and the program committee selected 28 of these for presentation. The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryptography. Each paper was reviewed by at least three program committee members. Extended abstracts of the revised versions of these papers are in these proceedings. The program also included two invited lectures by Dan Boneh and Silvio Micali.

I am extremely grateful to the program committee members for their enormous investment of time and effort in the difficult and delicate process of review and selection. Many of them attended the program committee meeting during the Crypto 2003 conference at the University of California, Santa Barbara.


Electronic submissions were made possible by the Web Review system of K.U. Leuven. I would like to thank Bart Preneel for his kind support. Special thanks to Thomas Herlea, who greatly supported us by operating the Web Review system customized for CT-RSA 2004.

In addition, I would like to thank Mami Yamaguchi for her support in the review process and in editing these proceedings.
I am specially grateful to Burt Kaliski and Ari Juels of RSA Laboratories for interfacing with the RSA conference.

I wish to thank all the authors, who by submitting papers made this conference possible, and the authors of accepted papers for their cooperation.

December 2003

Tatsuaki Okamoto
Program Chair
CT-RSA 2004
The RSA Conference 2004 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers’ Track was organized by RSA Laboratories.

**Program Chair**

Tatsuaki Okamoto, NTT Labs, Japan

**Program Committee**

Junhui Chao .................................................Chuo U., Japan
Ronald Cramer ..............................................Aarhus U., Denmark
Alex Dent ..................................................Royal Holloway, UK
Anand Desai ................................................NTT MCL, USA
Rosario Gennaro ...........................................IBM Research, USA
Goichiro Hanaoka ........................................U. of Tokyo, Japan
Martin Hirt ..................................................ETH Zurich, Switzerland
Kwangjo Kim ....................................................ICU, Korea
Mitsuru Matsui ...........................................Mitsubishi Electric, Japan
Phong Nguyen .............................................ENS, France
Kazuo Ohta .........................................................UEC, Japan
Pascal Paillier ................................................Gemplus, France
David Pointcheval .........................................ENS, France
Bart Preneel ................................................K.U. Leuven, Belgium
Jean-Jacques Quisquater ................................UCL, Belgium
Tsuyoshi Takagi ...........................................TU Darmstadt, Germany
Serge Vaudenay ...........................................EPF Lausanne, Switzerland
Chung-Huang Yang ........................................NKNU, Taiwan
Moti Yung ..................................................Columbia U., USA
Yuliang Zheng .............................................UNC Charlotte, USA

**Steering Committee**

Marc Joye ..................................................Gemplus, France
Burt Kaliski ................................................RSA Lab, USA
Bart Preneel ................................................K.U. Leuven, Belgium
Ron Rivest ................................................MIT, USA
Moti Yung ..................................................Columbia U., USA
Topics in Cryptology -- CT-RSA 2004
The Cryptographers' Track at the RSA Conference
Proceedings
Okamoto, T. (Ed.)
2004, XII, 392 p., Softcover
ISBN: 978-3-540-20996-6