Preface

You are holding the first in a hopefully long and successful series of RSA Cryptographers' Track proceedings.

The Cryptographers' Track (CT-RSA) is one of the many parallel tracks of the yearly RSA Conference. Other sessions deal with government projects, law and policy issues, freedom and privacy news, analysts' opinions, standards, ASPs, biotech and healthcare, finance, telecom and wireless security, developers, new products, implementers, threats, RSA products, VPNs, as well as cryptography and enterprise tutorials.

RSA Conference 2001 is expected to continue the tradition and remain the largest computer security event ever staged: 250 vendors, 10,000 visitors and 3,000 class-going attendees are expected in San Francisco next year.

I am very grateful to the 22 members of the program committee for their hard work. The program committee received 65 submissions (one of which was later withdrawn) for which review was conducted electronically; almost all papers had at least two reviews although most had three or more. Eventually, we accepted the 33 papers that appear in these proceedings. Revisions were not checked on their scientific aspects and some authors will write final versions of their papers for publication in refereed journals. As is usual, authors bear full scientific and paternity responsibilities for the contents of their papers.

The program committee is particularly indebted to 37 external experts who greatly helped in the review process: André Amègah, Mihir Bellare, Carine Boursier, Fabienne Cathala, Jean-Sébastien Coron, Nora Dabbous, Jean-François Dhem, Serge Fehr, Gerhard Frey, Pierre Girard, Benoît Gonzalvo, Shai Halevi, Helena Handschuh, Martin Hirt, Markus Jakobsson, Marc Joye, Neal Koblitz, François Koeune, Phil MacKenzie, Keith Martin, Alfred John Menezes, Victor Miller, Fabian Monrose, Mike Mosca, Pascal Paillier, Mireille Pauliac, Béatrice Peirani, David Pointcheval, Florence Quès, Ludovic Rousseau, Doug Schales, Jean-François Schultz, Joseph Silverman, Christophe Tymen, Mathieu Vavassori, Yongge Wang and Robert Zuccherato. Special thanks are due to Julien Brouchier for skillfully maintaining and updating the program committee's website.

It is our sincere hope that our efforts will contribute to reduce the distance between the academic community and the information security industry in the coming years.

November 2000 David Naccache

RSA Conference 2001 April 8-12 Moscone Center San Francisco

RSA Conference 2001 is organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers' Track at RSA Conference 2001 is organized by RSA Laboratories (`http://www.rsasecurity.com`) and sponsored by Compaq Computer Corporation, Hewlett-Packard, IBM, Intel Corporation, Microsoft, nCipher, EDS, RSA Security Inc., NIST and the National Security Agency.

Program Committee

David Naccache (Program Chair)	Gemplus, France
Ross Anderson	Cambridge University, United Kingdom
Josh Benaloh	Microsoft Research, USA
Daniel Bleichenbacher	Bell Labs, Lucent Technologies, USA
Dan Boneh	Stanford University, USA
Mike Burmester	Royal Holloway University, United Kingdom
Don Coppersmith	IBM Research, USA
Rosario Gennaro	IBM Research, USA
Ari Juels	RSA Laboratories, USA
Burt Kaliski	RSA Laboratories, USA
Kwangjo Kim	Information and Communications University, Korea
Arjen K. Lenstra	Citibank, USA Technical University Eindhoven, The Netherlands
Ueli Maurer	ETH Zurich, Switzerland
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater	Université Catholique de Louvain, Belgium
Michael Reiter	Bell Labs, Lucent Technologies, USA
Victor Shoup	IBM Research, Switzerland
Jacques Stern	École Normale Supérieure, France
Scott Vanstone	Certicom Research, Canada University of Waterloo, Canada
Michael Wiener	Entrust Technologies, Canada
Moti Yung	Certco, USA
Yuliang Zheng	Monash University, Australia
Phil Zimmerman	PGP, USA