Lecture Notes in Computer Science 2357

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Matt Blaze
AT&T Labs-Research
Room A275, 180 Park Ave., P.O. Box 971
Florham Park, NJ 07932-0971, USA
E-mail: mab@research.att.com

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): E.3, D.4.6, K.6.5, C.2, J.1, F.2.1-2, K.4.4

ISSN 0302-9743
ISBN 3-540-00646-X Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e. K.
Printed on acid-free paper SPIN: 10870172 06/3142 5 4 3 2 1 0

Preface

The Sixth International Financial Cryptography Conference was held during March 11–14, 2002, in Southampton, Bermuda. As is customary at FC, these proceedings represent "final" versions of the papers presented, revised to take into account comments and discussions from the conference.

Submissions to the conference were strong, with 74 papers submitted and 19 accepted for presentation and publication. (Regrettably, three of the submitted papers had to be summarily rejected after it was discovered that they had been improperly submitted in parallel to other conferences.) The small program committee worked very hard under a tight schedule (working through Christmas day) to select the program. No program chair could ask for a better committee; my thanks to everyone for their hard work and dedication.

In addition to the refereed papers, the program included a welcome from the Minister of Telecommunications and e-Commerce, Renee Webb, a keynote address by Nigel Hickson, and a panel on privacy tradeoffs chaired by Rebecca Wright (with panelists Ian Goldberg, Ron Rivest, and Graham Wood). The traditional Tuesday evening "rump session" was skillfully officiated by Markus Jakobsson.

My job as program chair was made much, much easier by the excellent work of our general chair, Nicko van Someren, who performed the miracle of hiding from me any evidence of the innumerable logistical nightmares associated with conducting this conference. I have no idea how he did it, but it must have involved many sleepless nights.

June 1, 2002 Matt Blaze

Program Committee

Matt Blaze	(AT&T Labs)
Program Chair	
Dan Boneh	(Stanford University)
Stefan Brands	(Zero Knowledge)
Dan Geer	(@stake)
Ian Goldberg	(Zero Knowledge)
Angelos Keromytis	(Columbia University)
Paul Kocher	(Cryptography Research)
Ron Rivest	(MIT)
Tomas Sander	(Intertrust)
Rebecca Wright	(AT&T Labs)

General Chair

Nicko van Someren (nCipher) ll

Table of Contents