

Springer

Berlin

Heidelberg

New York

Hong Kong

London

Milan

Paris

Tokyo

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003
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

| | |
|---|-----|
| E-Voting without ‘Cryptography’ | 1 |
| <i>Dahlia Malkhi, Ofer Margo, Elan Pavlov</i> | |
| An Implementation of a Universally Verifiable Electronic Voting Scheme Based on Shuffling | 16 |
| <i>Jun Furukawa, Hiroshi Miyauchi, Kengo Mori, Satoshi Obana, Kazue Sako</i> | |
| Financial Instruments in Recommendation Mechanisms | 31 |
| <i>Markus Jakobsson</i> | |
| Secure Combinatorial Auctions by Dynamic Programming with Polynomial Secret Sharing | 44 |
| <i>Koutarou Suzuki, Makoto Yokoo</i> | |
| A Second-Price Sealed-Bid Auction with Verifiable Discriminant of p_0 -th Root | 57 |
| <i>Kazumasa Omote, Atsuko Miyaji</i> | |
| A Two-Server, Sealed-Bid Auction Protocol | 72 |
| <i>Ari Juels, Michael Szydło</i> | |
| Secure Vickrey Auctions without Threshold Trust | 87 |
| <i>Helger Lipmaa, N. Asokan, Valtteri Niemi</i> | |
| Almost Optimal Hash Sequence Traversal | 102 |
| <i>Don Coppersmith, Markus Jakobsson</i> | |
| Cryptographic Primitives Enforcing Communication and Storage Complexity | 120 |
| <i>Philippe Golle, Stanislaw Jarecki, Ilya Mironov</i> | |
| CryptoComputing with Rationals | 136 |
| <i>Pierre-Alain Fouque, Jacques Stern, Geert-Jan Wackers</i> | |
| Privacy Tradeoffs: Myth or Reality? | 147 |
| <i>Rebecca N. Wright, L. Jean Camp, Ian Goldberg, Ronald L. Rivest, Graham Wood</i> | |
| An Improved Fast Signature Scheme without Online Multiplication..... | 152 |
| <i>Takeshi Okamoto, Mitsuru Tada, Atsuko Miyaji</i> | |
| Timed Release of Standard Digital Signatures | 168 |
| <i>Juan A. Garay, Markus Jakobsson</i> | |

VIII Table of Contents

| | |
|---|-----|
| Quasi-Efficient Revocation of Group Signatures | 183 |
| <i>Giuseppe Ateniese, Dawn Song, Gene Tsudik</i> | |
| The Dark Side of Threshold Cryptography | 198 |
| <i>Shouhuai Xu and Moti Yung</i> | |
| Split-and-Delegate: Threshold Cryptography for the Masses | 220 |
| <i>Daniel E. Geer, Jr., Moti Yung</i> | |
| Redistribution of Mechanical Secret Shares | 238 |
| <i>Yvo Desmedt, Rei Safavi-Naini, Huaxiong Wang</i> | |
| Reliable MIX Cascade Networks through Reputation | 253 |
| <i>Roger Dingledine, Paul Syverson</i> | |
| Offline Payments with Auditable Tracing | 269 |
| <i>Dennis Kügler, Holger Vogt</i> | |
| Fileteller: Paying and Getting Paid for File Storage | 282 |
| <i>John Ioannidis, Sotiris Ioannidis, Angelos D. Keromytis, Vassilis Prevelakis</i> | |
| Author Index | 301 |