Lecture Notes in Computer Science 1318
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Rafael Hirschfeld (Ed.)

Financial Cryptography

First International Conference, FC '97
Anguilla, British West Indies
February 24-28, 1997
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editor

Rafael Hirschfeld
Centrum for Wiskunde en Informatica, Stichting Mathematisch Centrum
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
E-mail: ray@cwi.nl

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Financial cryptography : first international conference ; proceedings / FC '97, Anguilla, British West Indies, February 24 - 28, 1997. Rafael Hirschfeld (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Lecture notes in computer science ; Vol. 1318)
ISBN 3-540-63594-7

CR Subject Classification (1991): E.3, D.4.6, K.6.5, J.1, C.2

ISSN 0302-9743
ISBN 3-540-63594-7 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10545793 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

On the last week of February 1997 a group of cryptographers, security experts, computer hackers, lawyers, bankers, and journalists converged on the small Caribbean island of Anguilla for FC97, the first international conference on Financial Cryptography. The conference aimed to foster cooperation and exchange of ideas among this diverse group. Anguilla's status in the financial world (it's an offshore tax haven) made it an appropriate venue for a conference on this topic.

Financial cryptography is intended to cover all topics related to the security of financial transactions and to digital commerce in general. Thus the conference program runs the gamut from pure cryptosystems to the technology of electronic money to legal and regulatory policy issues. Although security of monetary transactions is an ancient concern, and the use of cryptography for this purpose is not new, the modern study of the area has its roots in the pioneering work of David Chaum in the 1980's on electronic cash, in which cryptographic techniques were developed expressly for payment applications. Chaum's primary concern was anonymity. Although anonymous payments are not popular among many banks and central banks, anonymity remains an important and active area of concern for researchers and privacy advocates. It is thus perhaps fitting that the conference opened with a session on anonymity.

The papers appear in the order in which they were presented at the conference. Although they were mostly grouped into sessions by topic, other scheduling constraints in some cases made this impossible. These are revised versions of the accepted submissions. Revisions were not checked on their scientific aspects, and the authors bear full responsibility for the contents of their papers.

The program also included invited talks by Simon Lelieveld, Ronald Rivest, and Peter Wayner, and a panel discussion on legal issues of digital signatures by Michael Froomkin, Charles Merrill, and Benjamin Wright. All of these speakers have provided summaries of their presentations. In addition to the regular conference program, a rump session chaired by Peter Wayner provided an opportunity for less formal presentations. One of the rump session presentations, by Ronald Rivest on lottery ticket micropayments, has been selected for inclusion in this volume.

Financial Cryptography '97 was the brainchild of Robert Hettinga, who also founded the Digital Commerce Society of Boston. Assembling a group of people most of whom had never or hardly met him, let alone each other, he turned his vision into a reality. Vincent Cate handled all of the local arrangements in Anguilla. Ian Goldberg led the pre-conference tutorial workshop. Julie Rackliffe was responsible for coordinating exhibits and sponsorship. All of them deserve thanks, as do the members of the program committee for their efforts in evaluating the submissions and selecting the program, and of course the authors, without whose submissions there could be no conference. (US president Bill Clinton also played a part in the success of FC97 by ordering a cooling off period, averting a strike at American Airlines that would have made it difficult or impossible for most attendees to reach Anguilla.)

August 1997

Rafael Hirschfeld
FC97 Program Chair

Financial Cryptography '97
Anguilla, BWI
24-28 February 1997

Program Committee:

Matthew Franklin, AT&T Laboratories–Research, Murray Hill, NJ, USA
Michael Froomkin, U. Miami School of Law, Coral Gables, FL, USA
Rafael Hirschfeld (Program Chair), CWI, Amsterdam, The Netherlands
Arjen Lenstra, Citibank, New York, NY, USA
Mark Manasse, Digital Equipment Corporation, Palo Alto, CA, USA
Kevin McCurley, Sandia Laboratories, Albuquerque, NM, USA
Charles Merrill, McCarter & English, Newark, NJ, USA
Clifford Neuman, Information Sciences Institute, Marina del Rey, CA, USA
Sholom Rosen, Citibank, New York, NY, USA
Israel Sendrovic, Federal Reserve Bank of New York, New York, NY, USA

General Chairs:

Robert Hettinga, Shipwright/e$, Boston, MA, USA
Vincent Cate, Offshore Information Services, Anguilla, BWI

Exhibits and Sponsorship Manager:

Julie Rackliffe, Boston, MA, USA

Workshop Leader:

Ian Goldberg, Berkeley, CA, USA

Financial Cryptography '97 was held in cooperation with the International Association for Cryptologic Research and was sponsored by The Journal of Internet Banking and Commerce, Offshore Information Services, e$, and C2NET.

Table of Contents