Lecture Notes in Computer Science 1962

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Yair Frankel (Ed.)

Financial Cryptography

4th International Conference, FC 2000
Anguilla, British West Indies, February 20-24, 2000
Proceedings

Springer

Series Editors

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

Volume Editor

Yair Frankel
122 Harrison Ave, Westfield, NJ 07090, USA
E-mail: yfrankel@cryptographers.com

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Financial cryptography : 4th international conference ; proceedings / FC 2000, Anguilla, British West Indies, February 20 - 24, 2000. Yair Frankel (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 1962)
ISBN 3-540-42700-7

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 3-540-42700-7 Springer-Verlag Berlin Heidelberg New York

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

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN 10781056 06/3142 5 4 3 2 1 0

Preface

Financial Cryptography 2000 marked the fourth time the technical, business, legal, and political communities from around the world joined together on the small island of Anguilla, British West Indies to discuss and discover new advances in securing electronic financial transactions. The conference, sponsored by the International Financial Cryptography Association, was held on February 20–24, 2000. The General Chair, Don Beaver, oversaw the local organization and registration.

The program committee considered 68 submissions of which 21 papers were accepted. Each submitted paper was reviewed by a minimum of three referees. These proceedings contain revised versions of the 21 accepted papers. Revisions were not checked and the authors bear full responsibility for the content of their papers.

This year's program also included two invited lectures, two panel sessions, and a rump session. The invited talks were given by Kevin McCurley presenting "In the Search of the Killer App" and Pam Samuelson presenting "Towards a More Sensible Way of Regulating the Circumvention of Technical Protection Systems". For the panel sessions, Barbara Fox and Brian LaMacchia moderated "Public-Key Infrastructure: PKIX, Signed XML, or Something Else" and Moti Yung moderated "Payment Systems: The Next Generation". Stuart Haber organized the informal rump session of short presentations.

This was the first year that the conference accepted submissions electronically as well as by postal mail. Many thanks to George Davida, the electronic submissions chair, for maintaining the electronic submissions server. A majority of the authors preferred electronic submissions with 65 of the 68 submissions provided electronically.

The program committee had a difficult and challenging task in developing the program. Each year both the quantity and quality of submissions has improved and I thank all the authors for their submissions. The committee was assisted by our colleagues: Masayuki Abe, Don Beaver, Josh Benaloh, Daniel Bleichenbacher, Jan Camenisch, George Davida, Giovanni Di Crescenzo, Cynthia Dwork, Stefan Dziembowski, Serge Fehr, Matthias Fitzi, Markus Jakobsson, Ari Juels, Reto Kohlas, CT Montgomery, Satoshi Obana, Bartosz Przydatek, Markus Stadler, Stuart Stubblebine, Avishai Wool, and Moti Yung. I apologize for any inadvertent omissions. The committee also had the benefit of Matt Franklin, the Financial Cryptography '99 program chair, as an invaluable advisor to the committee. My thanks to the program committee and all reviewers.

Many individuals deserve thanks for their contribution to the success of the conference. Leslie Matheson and Bob Tarjan were responsible for exhibitions and sponsorships. Vince Cate and Ray Hirschfeld were responsible for local arrangements. Ben Cutler organized registration and took on many other duties. Organizing the conference this year was especially difficult due to hurricane damage on the island. I am especially grateful to Don Beaver and Ray Hirschfeld for all their advice and assistance.

Many organizations deserve thanks for supporting Financial Cryptography 2000. Financial support for several students was provided by Cryptography Reseach. Other grants of facilities and significant employee time were provided by Hansa Bank and Offshore Information Services. CertCo Incorporated and Hushmail provided financial support and e-Gold, Hansa Bank, Intertrust, nCipher, Telcordia, Xcert, ZeroKnowledge sponsored events. Once again e-Gold sponsored the rump session and provided a $350 e-Gold award for the best presentation at the rump session.

With comments and input from several people, including Moti Yung, Karl Thompson, and Jen Beaver, we saw fit to introduce a logo for this year's conference. The product, executed in final form by Don Beaver, adorned the pre-proceedings and the t-shirts and can be seen below.

Thanks to the people of Anguilla who have shared their island home. Finally I would like to thank my wife, Louise, and my two children, Alex and Erin, for their tremendous support.

September 2000 Yair Frankel

Financial Cryptography 2000

February 21–24, 2000, Anguilla, BWI

Sponsored by the
International Financial Cryptography Association (IFCA)

General Chair

Donald Beaver, CertCo Incorporated

Program Chair

Yair Frankel, CertCo Incorporated

Program Committee

Dan Boneh	Stanford
Joan Feigenbaum	AT&T Labs – Research
Matt Franklin	Xerox
Stuart Haber	InterTrust STAR Lab
Philip MacKenzie	Lucent Bell Labs
Ueli Maurer	ETH Zurich
Clifford Neuman	University of Southern California
Kazue Sako	NEC
Dan Simon	Microsoft
Paul Syverson	Naval Research Laboratory
Win Treese	Open Market, Incorporated
Nicko van Someren	nCipher

Advisory Members

Matt Franklin (FC '99 Program Chair)	Xerox Parc
George Davida (Electronic Submissions)	University of Wisconsin-Milwaukee

Table of Contents

Digital Rights Management

Invited Lecture (I)

Payment Systems

Financial Cryptography Tools (I)

Electronic Postcards

Panel (I)

Abuses of Systems

Financial Crypto Policies and Issues

Anonymity

Financial Cryptography Tools (II)

Panel (II)

System Architectures