



Rafael Hirschfeld (Ed.)

# Financial Cryptography

Second International Conference, FC '98  
Anguilla, British West Indies  
February 23-25, 1998  
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

Unipay Technologies

Prinsengracht 748, 1017 LC Amsterdam, The Netherlands

E-mail: unipay@xs4all.nl

Cataloging-in-Publication data applied for

## Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Financial cryptography** : second international conference ; proceedings / FC '98, Anguilla, British West Indies, February 23 - 25, 1998. Rafael Hirschfeld (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998

(Lecture notes in computer science ; Vol. 1465)

ISBN 3-540-64951-4

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

ISSN 0302-9743

ISBN 3-540-64951-4 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 1998

Printed in Germany

Typesetting: Camera-ready by author

SPIN 10638499 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

## Preface

Following the success of the first Financial Cryptography conference in 1997, a second meeting was held in February 1998, again on the Caribbean island of Anguilla, and drew an even larger group of attendees. The conference struck a chord among participants with a broad range of backgrounds who share a common concern with the security of digital commerce, and it provided a forum for the fertile exchange of ideas among this diverse group.

Submissions to this year's conference, and hence the resulting program, were quite strong. Compared to the previous year, however, they tended to focus more on technical issues and less on policy. Policy issues were covered in panel and roundtable discussions scheduled in separate sessions. One panel discussion, moderated by Barbara Fox on the topic of certificate revocation, was included in the scientific program, and the panelists have provided summaries of their remarks for the printed proceedings.

An informal rump session provided an opportunity for presentation of the latest results and work in progress. One of these was an attack on a cipher presented at FC97. A brief summary of this result is included at the end of this volume; a fuller version has been submitted for presentation elsewhere. With this exception, the papers appear in the order in which they were presented at the conference. 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.

Many people deserve thanks for their contributions to the success of FC98. Robert Hettinga and Vincent Cate were responsible for the general arrangements, and the smooth operation of the conference was due to them. Ian Goldberg led the post-conference workshop, and Blanc Weber was responsible for the exhibition and sponsorship and also took on a variety of other tasks. Thanks are due to the members of the program committee for their efforts in evaluating the submissions and selecting the program, and of course to the authors, without whose contributions there could be no conference. I am especially grateful to Matthew Franklin, whose assistance as Co-Chair, particularly in helping to resolve crises when they arose, was invaluable.

June 1998

Rafael Hirschfeld  
FC98 Program Chair

# Financial Cryptography '98

## Anguilla, BWI

### 23–25 February 1998

#### Program Committee

Matt Blaze, AT&T Laboratories, Florham Park, NJ, USA  
 Antoon Bosselaers, Katholieke Universiteit Leuven, Leuven, Belgium  
 Yves Carlier, Bank for International Settlements, Basel, Switzerland  
 Walter Effross, Washington College of Law, American U., Washington DC, USA  
 Matthew Franklin (Co-Chair), AT&T Laboratories, Florham Park, NJ, USA  
 Michael Froomkin, U. Miami School of Law, Coral Gables, FL, USA  
 Rafael Hirschfeld (Chair), Unipay Technologies, Amsterdam, The Netherlands  
 Alain Mayer, Bell Laboratories/Lucent Technologies, Murray Hill, NJ, USA  
 Moni Naor, Weizmann Institute of Science, Rehovot, Israel  
 Frank Trotter, Mark Twain Ecash/Mercantile Bank, St. Louis, MO, USA  
 Doug Tygar, Carnegie Mellon University, Pittsburgh, PA, USA  
 Moti Yung, CertCo LLC, New York, NY, USA

#### General Chairs

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

#### Exhibits and Sponsorship Manager

Blanc Weber, Seattle, WA, USA

#### Workshop Leader

Ian Goldberg, Berkeley, CA, USA

Financial Cryptography '98 was held in cooperation with the International Association for Cryptologic Research and was sponsored by RSA Data Security, C2NET, Hansa Bank & Trust Company, Sicherheit und Privat- International Bank, Offshore Information Services, and e\$.

# Table of Contents

Micropayments via Efficient Coin-Flipping .....	1
<i>Richard J. Lipton, Rafail Ostrovsky</i>	
X-Cash: Executable Digital Cash .....	16
<i>Markus Jakobsson, Ari Juels</i>	
Distributed Trustees and Revocability: A Framework for Internet Payment .....	28
<i>David M'Raihi, David Pointcheval</i>	
A Platform for Privately Defined Currencies, Loyalty Credits, and Play Money .....	43
<i>David P. Maher</i>	
Assessment of Threats for Smart Card Based Electronic Cash .....	58
<i>Kazuo J. Ezawa, Gregory Napiorkowski</i>	
Using a High-Performance, Programmable Secure Coprocessor .....	73
<i>Sean W. Smith, Elaine R. Palmer, Steve Weingart</i>	
Secure Group Barter: Multi-party Fair Exchange with Semi-Trusted Neutral Parties .....	90
<i>Matt Franklin, Gene Tsudik</i>	
A Payment Scheme Using Vouchers .....	103
<i>Ernest Foo, Colin Boyd</i>	
A Formal Specification of Requirements for Payment Transactions in the SET Protocol .....	122
<i>Catherine Meadows, Paul Syverson</i>	
On Assurance Structures for WWW Commerce .....	141
<i>Markus Jakobsson, Moti Yung</i>	
Certificate Revocation: Mechanics and Meaning .....	158
<i>Barbara Fox, Brian LaMacchia</i>	
Revocation: Options and Challenges .....	165
<i>Michael Myers</i>	
On Certificate Revocation and Validation .....	172
<i>Paul C. Kocher</i>	
Can We Eliminate Certificate Revocations Lists? .....	178
<i>Ronald L. Rivest</i>	

Group Blind Digital Signatures: A Scalable Solution to Electronic Cash . . .	184
<i>Anna Lysyanskaya, Zulfikar Ramzan</i>	
Curbing Junk E-Mail via Secure Classification . . . . .	198
<i>Erin Gabber, Markus Jakobsson, Yossi Matias, Alain Mayer</i>	
Publicly Verifiable Lotteries: Applications of Delaying Functions . . . . .	214
<i>David M. Goldschlag, Stuart G. Stubblebine</i>	
Robustness and Security of Digital Watermarks . . . . .	227
<i>Lesley R. Matheson, Stephen G. Mitchell, Talal G. Shamoon, Robert E. Tarjan, Francis Zane</i>	
Beyond Identity: Warranty-Based Digital Signature Transactions . . . . .	241
<i>Yair Frankel, David W. Kravitz, Charles T. Montgomery, Moti Yung</i>	
Compliance Checking in the PolicyMaker Trust Management System . . . . .	254
<i>Matt Blaze, Joan Feigenbaum, Martin Strauss</i>	
An Efficient Fair Off-Line Electronic Cash System with Extensions to Checks and Wallets with Observers . . . . .	275
<i>Aymeric de Solages, Jacques Traoré</i>	
A More Efficient Untraceable E-Cash System with Partially Blind Signatures Based on the Discrete Logarithm Problem . . . . .	296
<i>Shingo Miyazaki, Kouichi Sakurai</i>	
Cryptanalysis of SPEED . . . . .	309
<i>Chris Hall, John Kelsey, Bruce Schneier, David Wagner</i>	
Author Index . . . . .	311