

# 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

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 1997  
Printed in Germany

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 Fromkin, 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

Anonymity Control in E-Cash Systems <i>George Davida, Yair Frankel, Yiannis Tsiounis, Moti Yung</i> .....	1
How to Make Personalized Web Browsing Simple, Secure, and Anonymous <i>Eran Gabber, Phillip B. Gibbons, Yossi Matias, Alain Mayer</i> .....	17
Anonymous Networking and Virtual Intranets: Tools for Anonymous Corporations <i>Jim McCoy</i> .....	33
Unlinkable Serial Transactions <i>Paul F. Syverson, Stuart G. Stubblebine, David M. Goldschlag</i> .....	39
Efficient Electronic Cash with Restricted Privacy <i>Cristian Radu, René Govaerts, Joos Vandewalle</i> .....	57
The SPEED Cipher <i>Yuliang Zheng</i> .....	71
Evaluating the Security of Electronic Money <i>Simon L. Lelieveldt</i> .....	91
Electronic Cash—Technology Will Denationalise Money <i>David G.W. Birch, Neil A. McEvoy</i> .....	95
Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective <i>David P. Maher</i> .....	109
Some Critical Remarks on "Dynamic Data Authentication" as Specified in EMV '96 <i>Louis Claude Guillou</i> .....	123
Single-Chip Implementation of a Cryptosystem for Financial Applications <i>Nikolaus Lange</i> .....	135
Perspectives on Financial Cryptography <i>Ronald L. Rivest</i> .....	145
Auditable Metering with Lightweight Security <i>Matthew K. Franklin, Dahlia Malkhi</i> .....	151

SVP: A Flexible Micropayment Scheme <i>Jacques Stern, Serge Vaudenay</i> .....	161
An Efficient Micropayment System Based on Probabilistic Polling <i>Stanislaw Jarecki, Andrew Odlyzko</i> .....	173
On the Continuum Between On-line and Off-line E-cash Systems - I <i>Yacov Yacobi</i> .....	193
Towards Multiple-Payment Schemes for Digital Money <i>H. Pagnia, R. Jansen</i> .....	203
Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System <i>Markus Jakobsson, Moti Yung</i> .....	217
The Uses and Limits of Financial Cryptography: A Law Professor's Perspective <i>Peter P. Swire</i> .....	239
Legal Issues in Cryptography <i>Edward J. Radlo</i> .....	259
Digital Signatures Today <i>A. Michael Froomkin</i> .....	287
An Attorney's Roadmap to the Digital Signature Guidelines <i>Charles R. Merrill</i> .....	291
Alternative Visions for Legal Signatures and Evidence <i>Benjamin Wright</i> .....	299
Money Laundering: Past, Present and Future <i>Peter C. Wayner</i> .....	301
Electronic Lottery Tickets as Micropayments <i>Ronald L. Rivest</i> .....	307
Strategic Tasks for Government in the Information Age <i>Paul Lampru</i> .....	315
Using Electronic Markets to Achieve Efficient Task Distribution <i>Ian Grigg, Christopher C. Petro</i> .....	329
The Gateway Security Model in the Java Electronic Commerce Framework <i>Theodore Goldstein</i> .....	340



Highly Scalable On-line Payments Via Task Decoupling <i>David W. Kravitz</i> .....	355
GUMP: Grand Unified Meta-Protocols Recipes for Simple, Standards-Based Financial Cryptography <i>Barbara Fox, Brian Beckman, Dan Simon</i> .....	375
Secure Network Communications and Secure Store & Forward Mechanisms with the SAP R/3 System <i>Bernhard Esslinger, Jürgen Schneider</i> .....	395
Author Index.....	409