

# Preface

The fifth Financial Cryptography conference was held February 19–22, 2001. After half a decade, we moved beyond our Anguillian origins to Grand Cayman, BWI. The venue changed but the focus of the program remained to present the best research in securing electronic financial transactions and electronic commerce. As in the past few years, most of the contributed papers focused on the technical cryptographic and security aspects of financial cryptography, while the financial aspects are reflected primarily in invited talks and panels. (And in the informal discussion.) This year, in addition to the submitted papers, we had a provocative invited talk by Richard Rahn on money laundering as well as panels on digital rights management and the business of electronic voting. There was also a rump session, chaired by Rebecca Wright.

There were many interesting and many technically strong submissions. I thank the program committee (listed on the next page) for their help in the difficult task of choosing those papers that made the strongest contribution to the conference. We had additional reviewing help from Olivier Baudron, Paul Fahn, Juan Garay, Markus Jakobsson, Guenter Karjoth, Phong Nguyen, David Pointcheval, Thomas Pornin, Sholom Rosen, Dawn Song, Susanne Wetzels, and Rebecca Wright. (My apologies if I have overlooked anyone.) I would also like to thank George Davida, the electronic submissions chair, and his student, Dawn Marie Gibson, for setting up and running the submissions process at the University of Wisconsin. An extra big thank you to Yair Frankel, who was always there with his experience and advice that greatly improved the job I did as program chair, as well as making it more enjoyable. Matt Franklin also provided valuable advice. Thanks to all the people who submitted papers, without which there would be no program. Authors were given the opportunity to revise their papers following the conference. These were collected without further review and are included in this volume.

Thanks to general chair Stuart Haber for doing many things that none of the attendees noticed because he did them so nicely. He was ably assisted by Hinde ten Berge. Thanks to Harris McCoy for handling local arrangements and Jason Cronk for maintaining the Web site. Thanks to the IFCA directors for keeping FC thriving, to Adam Shostack for venue arrangements, and to Barb Fox, the sponsorship chair. Thanks to our financial sponsors, who are listed on the next page.

Special thanks to Ray Hirschfeld whose advice to me and to the others mentioned here has been invaluable. Thanks finally to attendees without whom there would be no conference.

## **Program Committee**

Matt Blaze, AT&T Labs - Research  
Yair Frankel, Ecash  
Matt Franklin, UC Davis  
David Kravitz, Wave Systems Corp.  
Arjen Lenstra, Citicorp  
Philip MacKenzie, Lucent Bell Labs  
Avi Rubin, AT&T Labs - Research  
Jacques Stern, Ecole Normale Supérieure  
Kazuo Sako, NEC  
Stuart Stubblebine, CertCo  
Paul Syverson (Chair), Naval Research Lab  
Win Treese, Open Market, Inc.  
Doug Tygar, UC Berkeley  
Michael Waidner, IBM Zurich Research Lab  
Moti Yung, CertCo

## **General Chair**

Stuart Haber, Intertrust

## **Sponsorship Chair**

Barb Fox, Microsoft

Financial Cryptography 2001 was organized by the International Financial Cryptography Association (IFCA), and was sponsored by Bibit Internet Payments, CertCo, Certicom, Hush Communications, IBM, InterTrust STAR Lab, Microsoft, nCipher, RSA Security, and Zero-Knowledge Systems.

Financial Cryptography

5th International Conference, FC 2001, Grand Cayman,  
British West Indies, February 19-22, 2001. Proceedings

Syverson, P.F. (Ed.)

2002, IX, 379 p., Softcover

ISBN: 978-3-540-44079-6