

Preface

The third Financial Cryptography conference was held in February 1999, once again at Anguilla in the British West Indies. The number of attendees continues to increase from year to year, as do the number and quality of the technical submissions.

The Program Committee did a great job selecting the technical program. I thank them for all of their effort's. We were helped by a number of outside reviewers, including Martín Abadi, Gerrit Bleumer, Drew Dean, Anand Desai, Mariusz Jakubowski, Andrew Odlyzko, David Pointcheval, Guillaume Poupard, Zulfikar Ramzan, Aleta Ricciardi, Dan Simon, Jessica Staddon, Venkie Venkatesan, Avishai Wool, and Francis Zane. I apologize for any omissions.

Adi Shamir gave an excellent invited talk that forecast the future of cryptography and electronic commerce. On-line certificate revocation was the subject of a panel led by Michael Myers, following up on the success of his panel on the same topic at last year's conference. Joan Feigenbaum moderated a lively panel on fair use, intellectual property, and the information economy, and I thank her for pulling together from that discussion a paper for these proceedings. A successful Rump Session allowed participants to present new results in an informal setting, superbly chaired by Avi Rubin.

A pre-proceedings, containing earlier versions of the accepted papers, was distributed at the conference. The pre-proceedings were produced on the Xerox DocuPrint 180 NPS printer, at an amazing 180 pages per minute. Special thanks to Russ Atkinson for teaching me its care and feeding. Final versions were prepared by the authors shortly after the conference, and are included in this volume without further review.

I thank everyone who contributed to the successful organization of the conference. In particular, I would like to thank Vince Cate for another outstanding job with the local arrangements, and Ray Hirschfeld for invaluable advice and support. My colleagues at Xerox PARC also helped in many ways. Lastly, I would like to thank all of the authors for making this conference and these proceedings possible.

May 1999

Matt Franklin
FC99 Program Chair

Financial Cryptography '99
Anguilla, BWI
22–25 February 1999

Program Committee

Joan Feigenbaum, AT&T Labs – Research
Yair Frankel, CertCo
Matt Franklin (Chair), Xerox PARC
David Goldschlag, Divx
Markus Jakobsson, Bell Labs
Ari Juels, RSA Labs
Arjen Lenstra, Citibank
Clifford Neuman, University of Southern California
Berry Schoenmakers, Eindhoven University of Technology
Jacques Stern, ENS
Yacov Yacobi, Microsoft
Bennet Yee, U. C. San Diego

General Chair

Rafael Hirschfeld, Unipay Technologies, Amsterdam, The Netherlands

Local Arrangements Chair

Vincent Cate, Offshore Information Services, Anguilla, BWI

Financial Cryptography '99 was organized by the International Financial Cryptography Association (IFCA), and was sponsored by nCipher Corporation, e-gold Transnational, EURO RSCG Interactive, Hansa Bank & Trust Company, and Offshore Information Services.