Lecture Notes in Computer Science 3110

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Ari Juels (Ed.)

Financial Cryptography

8th International Conference, FC 2004
Key West, FL, USA, February 9-12, 2004
Revised Papers

Springer

Volume Editor

Ari Juels
RSA Laboratories
174 Middlesex Turnpike, Bedford, MA 01730, USA
E-mail: ajuels@rsasecurity.com

Library of Congress Control Number: 2004108443

CR Subject Classification (1998): E.3, D.4.6, K.6.5, K.4.4, C.2, J.1, F.2.1-2

ISSN 0302-9743
ISBN 3-540-22420-3 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11300311 06/3142 5 4 3 2 1 0

Preface

The 8th Annual Financial Cryptography Conference was held during 9–12 February 2004 in Key West, Florida, USA. The conference was organized by the International Financial Cryptography Association (IFCA).

The program committee, which comprised 25 members, reviewed 78 submissions, of which only 17 were accepted for presentation at the conference. This year's conference differed somewhat from those of previous years in its consideration of papers devoted to implementation, rather than purely conceptual research; one of these submissions was presented at the conference. This represented a movement in the conference toward practical problems and real-world perspectives as a complement to more traditional academic forms of research.

In this spirit, the program included a number of excellent invited speakers. In the opening talk of the conference, Jack Selby threw down the gauntlet, describing some of the achievements of the PayPal system, but also enumerating reasons for the failures of many elegant e-cash schemes in the past. Ron Rivest, in contrast, described an emerging success in the cleverly conceived Peppercoin micropayment system. Jacques Stern enlightened us with his experience in the cryptographic design of banking cards in France. Simon Pugh unveiled some details of a new generation of wireless credit card. Finally, in deference to the many consumers in the world lacking either techno-savvy or technological resources that we often too easily take for granted, Jon Peha described a fielded banking system that avoids reliance on conventional financial infrastructures. Thanks to all of these speakers for rounding out the conference with their expertise and breadth of vision.

The conference also included a panel, moderated by Andrew Patrick, on usability and its impact on security. This was a salutary and engaging reminder of how security means much more than cryptography alone.

I wish to thank the program committee for their diligence and care in reviewing papers, and in some cases for providing highly detailed comments to submitters. I would also like to thank the external referees who lent help in reviewing papers: Danny Bickson, Liad Blumenreich, Julien Brouchier, Dario Catalano, Benoit Chevallier-Mames, Pierre-Alain Fouque, Zvika Guterman, Helena Handschuh, Stanislaw Jarecki, Ofer Margo, Nick Mathewson, Pascal Paillier, Elan Pavlov, Ludovic Rousseau, Yaron Sella, and Jessica Staddon.

Thanks to the IFCA directors and officers for their guidance in conference arrangements. I am grateful to Moti Yung for chairing the rump session, an evening of short, informal presentations on ideas in the making or the breaking. Thomas Herlea of KU Leuven was very helpful as administrator of the conference submission server. Also thanks to Hinde ten Berge, who served as General Chair, overseeing not only the local arrangements for this conference, but also the publication of the preproceedings.

Finally, thanks to all of the contributors of the scientific papers to the conference. As in previous years, participants enjoyed not only mentally stimulating presentations, but also the ample sunshine – a nearly forgotten delight for many delegates from northern countries.

From its beginning, Financial Cryptography has been something of a haven for cryptographic mavericks and a meeting-point for researchers, scientists, financiers, and hands-on implementers. As the conference matures, let us look to see its early spark of originality continue to thrive in the conference hall and on the beaches.

April 2004 Ari Juels

Financial Cryptography 2004

Program Chair

Ari Juels	RSA Laboratories, USA

Program Committee

Masayuki Abe	NTT Laboratories, Japan
David Birch	Consult Hyperion, UK
Roger Dingledine	The Free Haven Project, USA
Niels Ferguson	MacFergus, The Netherlands
Philippe Golle	Stanford University, USA
Tim Jones	Simpay, UK
Marc Joye	Gemplus, France
Kwangjo Kim	ICU, Korea
Arjen Lenstra	Citicorp, USA and Technische Univ. Eindhoven, The Netherlands
Helger Lipmaa	Helsinki Univ. of Tech., Finland
Dahlia Malkhi	Hebrew Univ., Israel
David Naccache	Gemplus, France
Tatsuaki Okamoto	NTT Laboratories, Japan
Benny Pinkas	Hewlett-Packard, USA
Nicole Pohl	Franklin and Marshall College, USA
David Pointcheval	CNRS-École Normale Supérieure, France
Bart Preneel	K.U. Leuven, Belgium
Avi Rubin	Johns Hopkins University, USA
Vitaly Shmatikov	SRI International, USA
Adam Shostack	Informed Security, Canada
Sean Smith	Dartmouth College, USA
Rebecca Wright	Stevens Institute of Technology, USA
Moti Yung	Columbia University, USA

General Chair

Hinde ten Berge

Sponsors

Silver Sponsors	nCipher and NTT DoCoMo USA Labs
Bronze Sponsor	RSA Labs
In-Kind Sponsor	Consult Hyperion

Financial Cryptography 2004 was organized by the International Financial Cryptography Association (IFCA).

Table of Contents

Invited Talks

Analyzing the Success and Failure of Recent e-Payment Schemes (Abstract) 1
Jack R. Selby

Peppercoin Micropayments 2
Ronald L. Rivest

Loyalty and Micropayment Systems

Microcredits for Verifiable Foreign Service Provider Metering 9
Craig Gentry and Zulfikar Ramzan

A Privacy-Friendly Loyalty System Based on Discrete Logarithms over Elliptic Curves 24
Matthias Enzmann, Marc Fischlin, and Markus Schneider

User Authentication

Addressing Online Dictionary Attacks with Login Histories and Humans-in-the-Loop (Extended Abstract) 39
S. Stubblebine and P.C. van Oorschot

Call Center Customer Verification by Query-Directed Passwords 54
Lawrence O'Gorman, Amit Bagga, and Jon Bentley

Invited Talks

Cryptography and the French Banking Cards: Past, Present, Future 68
Jacques Stern

PayPass Security and Risk (Abstract) 70
Simon Pugh

e-Voting

The Vector-Ballot e-Voting Approach 72
Aggelos Kiayias and Moti Yung

Efficient Maximal Privacy in Boardroom Voting and Anonymous Broadcast 90
Jens Groth

Panel Session: Building Usable Security Systems

Usability and Acceptability of Biometric Security Systems 105
Andrew S. Patrick

Mental Models of Computer Security 106
L. Jean Camp

Visualization Tools for Security Administrators 112
William Yurick

Secure Interaction Design 114
Ka-Ping Yee

Invited Talk

Bringing Payment Technology to the Unbanked (Abstract) 116
Jon M. Peha

Auctions and Lotteries

Interleaving Cryptography and Mechanism Design –
The Case of Online Auctions 117
Edith Elkind and Helger Lipmaa

Secure Generalized Vickrey Auction without Third-party Servers 132
Makoto Yokoo and Koutarou Suzuki

Electronic National Lotteries 147
Elisavet Konstantinou, Vasiliki Liagkou, Paul Spirakis, Yannis C. Stamatiou, and Moti Yung

Identity-Based Chameleon Hash and Applications 164
Giuseppe Ateniese and Breno de Medeiros

Game Theoretic and Cryptographic Tools

Selecting Correlated Random Actions 181
Vanessa Teague

An Efficient and Usable Multi-show Non-transferable
Anonymous Credential System 196
Giuseppe Persiano and Ivan Visconti

The Ephemeral Pairing Problem 212
Jaap-Henk Hoepman

Mix Networks and Anonymous Communications

Mixminion: Strong Anonymity for Financial Cryptography 227
Nick Mathewson and Roger Dingledine

Practical Anonymity for the Masses with MorphMix 233
Marc Rennhard and Bernhard Plattner

Timing Attacks in Low-Latency Mix Systems (Extended Abstract) 251
Brian N. Levine, Michael K. Reiter, Chenxi Wang, and Matthew Wright

Provable Unlinkability against Traffic Analysis 266
Ron Berman, Amos Fiat, and Amnon Ta-Shma

Author Index 281