Table of Contents

Managing Payment Transaction Costs
Amortized E-Cash .................................................. 1  
*Moses Liskov, Silvio Micali*
Offline Micropayments without Trusted Hardware ............ 21  
*Matt Blaze, John Ioannidis, Angelos D. Keromytis*

Panel (I)
The Practical Problems of Implementing MicroMint .............. 41  
*Nicko van Someren*
Protecting Digital Rights ....................................... 51  
*Yair Frankel*
*David W. Kravitz*
A Solution to the Napster Phenomenon: Why Value Cannot Be Created Absent the Transfer of Subjective Data ....................... 59  
*Scott Moskowitz*
Golden Times for Digital Rights Management? ................ 64  
*Tomas Sander*
Applicability of Public Key Cryptosystems to Digital Rights Management Applications .................. 75  
*Jeremy Wyant*

Trust and Risk Management
On the Global Content PMI: Improved Copy-Protected Internet Content Distribution ......................... 79  
*Tadayoshi Kohno, Mark McGovern*
Trust: A Collision of Paradigms ................................ 91  
*L. Jean Camp, Helen Nissenbaum, Cathleen McGrath*

Groups and Anonymity
*Éliane Jaulmes, Guillaume Poupard*
Anonymity without ‘Cryptography’ ........................................... 117  
Dahlia Malkhi and Elan Pavlov

Fair Tracing without Trustees ............................................. 136  
Dennis Kügler, Holger Vogt

Invited Talk

Why the War on Money Laundering Should Be Aborted .............. 149  
Richard W. Rahn

Certificates and Authentication

Provably Secure Implicit Certificate Schemes .......................... 156  
Daniel R.L. Brown, Robert Gallant, Scott A. Vanstone

Nonmonotonicity, User Interfaces, and Risk Assessment in Certificate Revocation ................................................................. 166  
Ninghai Li, Joan Feigenbaum

Mutual Authentication for Low-Power Mobile Devices .............. 178  
Markus Jakobsson, David Pointcheval

Credit Card Security

Off-Line Generation of Limited-Use Credit Card Numbers............ 196  
Aviel D. Rubin, Rebecca N. Wright

A Security Framework for Card-Based Systems ....................... 210  
Yiannis Tsiounis

SecureClick: A Web Payment System with Disposable Credit Card Numbers ................................................................. 232  
Adi Shamir

Panel (II)

The Business of Electronic Voting ......................................... 243  
Ed Gerck, C. Andrew Neff, Ronald L. Rivest, Aviel D. Rubin, Moti Yung

Markets and Multiparty Computation

Privacy for the Stock Market ............................................... 269  
Giovanni Di Crescenzo

Secure Distributed Computing in a Commercial Environment .......... 289  
Philippe Golle, Stuart Stubblebine
Signatures in Financial Cryptography

Monotone Signatures .......................................................... 305
    David Naccache, David Pointcheval, Christophe Tymen

The Power of RSA Inversion Oracles and the Security of Chaum’s
RSA-Based Blind Signature Scheme ....................................... 319
    Mihir Bellare, Chanathip Namprempre, David Pointcheval,
    Michael Semanko

Optimistic Fair Exchange with Transparent Signature Recovery ........ 339
    Olivier Markowitch, Shahrokh Saeednia

Auctions

(M + 1)st-Price Auction Protocol ........................................... 351
    Hiroaki Kikuchi

Non-interactive Private Auctions ............................................. 364
    Olivier Baudron, Jacques Stern

Author Index ................................................................. 379
Financial Cryptography
5th International Conference, FC 2001, Grand Cayman,
Syverson, P.F. (Ed.)
2002, IX, 379 p., Softcover
ISBN: 978-3-540-44079-6