

# Table of Contents

## Managing Payment Transaction Costs

Amortized E-Cash .....	1
<i>Moses Liskov, Silvio Micali</i>	
Offline Micropayments without Trusted Hardware .....	21
<i>Matt Blaze, John Ioannidis, Angelos D. Keromytis</i>	

## Panel (I)

The Practical Problems of Implementing MicroMint .....	41
<i>Nicko van Someren</i>	
Protecting Digital Rights .....	51
<i>Yair Frankel</i>	
Aspects of Digital Rights Management and the Use of Hardware Security Devices .....	54
<i>David W. Kravitz</i>	
A Solution to the Napster Phenomenon: Why Value Cannot Be Created Absent the Transfer of Subjective Data .....	59
<i>Scott Moskowitz</i>	
Golden Times for Digital Rights Management? .....	64
<i>Tomas Sander</i>	
Applicability of Public Key Cryptosystems to Digital Rights Management Applications .....	75
<i>Jeremy Wyant</i>	

## Trust and Risk Management

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

## Groups and Anonymity

On the Security of <i>Homage</i> Group Authentication Protocol .....	106
<i>Éliane Jaulmes, Guillaume Poupard</i>	

Anonymity without ‘Cryptography’ .....	117
<i>Dahlia Malkhi and Elan Pavlov</i>	

Fair Tracing without Trustees .....	136
<i>Dennis K�gler, Holger Vogt</i>	

## Invited Talk

Why the War on Money Laundering Should Be Aborted .....	149
<i>Richard W. Rahn</i>	

## Certificates and Authentication

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

Nonmonotonicity, User Interfaces, and Risk Assessment in Certificate Revocation .....	166
<i>Ninghui Li, Joan Feigenbaum</i>	

Mutual Authentication for Low-Power Mobile Devices .....	178
<i>Markus Jakobsson, David Pointcheval</i>	

## Credit Card Security

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

A Security Framework for Card-Based Systems .....	210
<i>Yiannis Tsionis</i>	

SecureClick: A Web Payment System with Disposable Credit Card Numbers .....	232
<i>Adi Shamir</i>	

## Panel (II)

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

## Markets and Multiparty Computation

Privacy for the Stock Market .....	269
<i>Giovanni Di Crescenzo</i>	

Secure Distributed Computing in a Commercial Environment .....	289
<i>Philippe Golle, Stuart Stubblebine</i>	

## Signatures in Financial Cryptography

Monotone Signatures .....	305
<i>David Naccache, David Pointcheval, Christophe Tymen</i>	
The Power of RSA Inversion Oracles and the Security of Chaum's	
RSA-Based Blind Signature Scheme .....	319
<i>Mihir Bellare, Chanathip Namprempre, David Pointcheval, Michael Semanko</i>	
Optimistic Fair Exchange with Transparent Signature Recovery .....	339
<i>Olivier Markowitch, Shahrokh Saeednia</i>	

## Auctions

$(M + 1)$ st-Price Auction Protocol .....	351
<i>Hiroaki Kikuchi</i>	
Non-interactive Private Auctions .....	364
<i>Olivier Baudron, Jacques Stern</i>	

Author Index .....	379
--------------------	-----

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