

Table of Contents

Micropayments via Efficient Coin-Flipping	1
<i>Richard J. Lipton and Rafail Ostrovsky</i>	
X-Cash: Executable Digital Cash	16
<i>Markus Jakobsson and Ari Juels</i>	
Distributed Trustees and Revocability: A Framework for Internet Payment	28
<i>David M'Raihi and David Pointcheval</i>	
A Platform for Privately Defined Currencies, Loyalty Credits, and Play Money	43
<i>David P. Maher</i>	
Assessment of Threats for Smart Card Based Electronic Cash	58
<i>Kazuo J. Ezawa and Gregory Napiorkowski</i>	
Using a High-Performance, Programmable Secure Coprocessor	73
<i>Sean W. Smith, Elaine R. Palmer, and Steve Weingart</i>	
Secure Group Barter: Multi-party Fair Exchange with Semi-Trusted Neutral Parties	90
<i>Matt Franklin and Gene Tsudik</i>	
A Payment Scheme Using Vouchers	103
<i>Ernest Foo and Colin Boyd</i>	
A Formal Specification of Requirements for Payment Transactions in the SET Protocol	122
<i>Catherine Meadows and Paul Syverson</i>	
On Assurance Structures for WWW Commerce	141
<i>Markus Jakobsson and Moti Yung</i>	
Certificate Revocation: Mechanics and Meaning	158
<i>Barbara Fox and Brian LaMacchia</i>	
Revocation: Options and Challenges	165
<i>Michael Myers</i>	
On Certificate Revocation and Validation	172
<i>Paul C. Kocher</i>	
Can We Eliminate Certificate Revocations Lists?	178
<i>Ronald L. Rivest</i>	

VIII Table of Contents

Group Blind Digital Signatures: A Scalable Solution to Electronic Cash . . .	184
<i>Anna Lysyanskaya and Zulfikar Ramzan</i>	
Curbing Junk E-Mail via Secure Classification	198
<i>Eran Gabber, Markus Jakobsson, Yossi Matias, and Alain Mayer</i>	
Publicly Verifiable Lotteries: Applications of Delaying Functions	214
<i>David M. Goldschlag and Stuart G. Stubblebine</i>	
Robustness and Security of Digital Watermarks	227
<i>Lesley R. Matheson, Stephen G. Mitchell, Talal G. Shamoon, Robert E. Tarjan, and Francis Zane</i>	
Beyond Identity: Warranty-Based Digital Signature Transactions	241
<i>Yair Frankel, David W. Kravitz, Charles T. Montgomery, and Moti Yung</i>	
Compliance Checking in the PolicyMaker Trust Management System	254
<i>Matt Blaze, Joan Feigenbaum, and Martin Strauss</i>	
An Efficient Fair Offline Electronic Cash System with Extensions to Checks and Wallets with Observers	275
<i>Aymeric de Solages and Jacques Traoré</i>	
A More Efficient Untraceable E-Cash System with Partially Blind Signatures Based on the Discrete Logarithm Problem	296
<i>Shingo Miyazaki and Kouichi Sakurai</i>	
Cryptanalysis of SPEED	309
<i>Chris Hall, John Kelsey, Bruce Schneier, and David Wagner</i>	
Author Index	311

Financial Cryptography

Second International Conference, FC'98, Anguilla,

British West Indies, February 23-25, 1998, Proceedings

Hirschfeld, R. (Ed.)

1998, VIII, 320 p., Softcover

ISBN: 978-3-540-64951-9