

Table of Contents

Digital Rights Management

Efficient Trace and Revoke Schemes	1
<i>Moni Naor and Benny Pinkas</i>	

Efficient Watermark Detection and Collusion Security	21
<i>Francis Zane</i>	

Invited Lecture (I)

Towards More Sensible Anti-circumvention Regulations	33
<i>Pamela Samuelson</i>	

Payment Systems

Self-Escrowed Cash against User Blackmailing	42
<i>Birgit Pfitzmann and Ahmad-Reza Sadeghi</i>	

Blind, Auditable Membership Proofs	53
<i>Tomas Sander, Amnon Ta-Shma, and Moti Yung</i>	

Private Selective Payment Protocols	72
<i>Giovanni Di Crescenzo</i>	

Financial Cryptography Tools (I)

Sharing Decryption in the Context of Voting or Lotteries	90
<i>Pierre-Alain Fouque, Guillaume Poupard, and Jacques Stern</i>	

Electronic Postcards

Postal Revenue Collection in the Digital Age	105
<i>Leon A. Pintsov and Scott A. Vanstone</i>	

Signing on a Postcard	121
<i>David Naccache and Jacques Stern</i>	

Panel (I)

Payment Systems: The Next Generation	136
<i>Moti Yung</i>	

Abuses of Systems

Non-repudiation in SET: Open Issues	140
<i>Els Van Herreweghen</i>	
Statistics and Secret Leakage	157
<i>Jean-Sébastien Coron, Paul Kocher, and David Naccache</i>	
Analysis of Abuse-Free Contract Signing	174
<i>Vitaly Shmatikov and John C. Mitchell</i>	
Asymmetric Currency Rounding	192
<i>David M'Raihi, David Naccache, and Michael Tunstall</i>	

Financial Crypto Policies and Issues

The Encryption Debate in Plaintext: National Security and Encryption in the United States and Israel	202
<i>Barak D. Jolish</i>	
Critical Comments on the European Directive on a Common Framework for Electronic Signatures and Certification Service Providers	225
<i>Apol·lònia Martínez Nadal and Josep Lluís Ferrer Gomila</i>	
A Response to “Can We Eliminate Certificate Revocation Lists?”	245
<i>Patrick McDaniel and Aviel Rubin</i>	

Anonymity

Self-Scrambling Anonymizers	259
<i>David Pointcheval</i>	
Authentic Attributes with Fine-Grained Anonymity Protection	276
<i>Stuart G. Stubblebine and Paul F. Syverson</i>	
Resource-Efficient Anonymous Group Identification	295
<i>Ben Handley</i>	

Financial Cryptography Tools (II)

Secret Key Authentication with Software-Only Verification	313
<i>Jaap-Henk Hoepman</i>	

Panel (II)

Panel: Public Key Infrastructure: PKIX, Signed XML or Something Else?	327
<i>Barbara Fox and Brian LaMacchia</i>	

System Architectures

Financial Cryptography in 7 Layers 332
Ian Grigg

Capability-Based Financial Instruments 349
Mark S. Miller, Chip Morningstar, and Bill Frantz

Author Index 379