

# Table of Contents

## Electronic Commerce

Experimenting with Electronic Commerce on the PalmPilot .....	1
<i>Neil Daswani and Dan Boneh</i>	

Blinding of Credit Card Numbers in the SET Protocol .....	17
<i>Hugo Krawczyk</i>	

## Anonymity Control

Trustee Tokens: Simple and Practical Anonymous Digital Coin Tracing ....	29
<i>Ari Juels</i>	

Flow Control: A New Approach for Anonymity Control in Electronic Cash Systems .....	46
<i>Tomas Sander and Amnon Ta-Shma</i>	

## Fraud Management

Risk Management for E-Cash Systems with Partial Real-Time Audit .....	62
<i>Yacov Yacobi</i>	

Assessment of Effectiveness of Counterfeit Transaction Detection Systems for Smart Card Based Electronic Cash .....	72
<i>Kazuo J. Ezawa, Gregory Napierkowski and Mariusz Kossarski</i>	

## Public-Key Certificates

Reasoning about Public-Key Certification: On Bindings between Entities and Public Keys .....	86
<i>Reto Kohlas and Ueli Maurer</i>	

Online Certificate Status Checking in Financial Transactions: The Case for Re-issuance .....	104
<i>Barbara Fox and Brian LaMacchia</i>	

## Steganography

Playing ‘Hide and Seek’ with Stored Keys .....	118
<i>Adi Shamir and Nicko van Someren</i>	

On Channel Capacity and Modulation of Watermarks in Digital Still Images .....	125
<i>Markus Breitbach and Hideki Imai</i>	

## Content Distribution

Towards Making Broadcast Encryption Practical .....	140
<i>Michel Abdalla, Yuval Shavitt and Avishai Wool</i>	

Conditional Access Concepts and Principles .....158  
*David W. Kravitz and David M. Goldschlag*

Fair Use, Intellectual Property, and the Information Economy  
(Panel Session Summary) .....173  
*Jon Callas, Joan Feigenbaum, David Goldschlag and Erin Sawyer*

**Anonymity Mechanisms**

Anonymous Authentication of Membership in Dynamic Groups .....184  
*Stuart Schechter, Todd Parnell and Alexander Hartemink*

Some Open Issues and New Directions in Group Signatures .....196  
*Giuseppe Ateniese and Gene Tsudik*

**Auctions and Markets**

Anonymous Investing: Hiding the Identities of Stockholders .....212  
*Philip MacKenzie and Jeffrey Sorensen*

Fair On-Line Auctions without Special Trusted Parties .....230  
*Stuart G. Stubblebine and Paul F. Syverson*

**Auctions and Markets**

Cryptosystems Robust against “Dynamic Faults” Meet Enterprise  
Needs for Organizational “Change Control” .....241  
*Yair Frankel and Moti Yung*

Improved Magic Ink Signatures Using Hints .....253  
*Markus Jakobsson and Joy Müller*

Author Index .....269