# Table of Contents

## Session 1: Electronic Money and Commerce

User-Defined Divisibility of Ecash and a Practical Implementation .......................... 1  
*Eli Biham, Amichai Shulman*

An Operational Model of QuickPay - Extended Abstract .................................... 19  
*Pieter H. Hartel, Jake Hill, Matt Sims*

Interoperable and Untraceable Debit-Tokens for Electronic Fee Collection ................ 29  
*Cristian Radu, Frederic Klopfert, Jan De Meester*

The Banksys Signature Transport (BST) Protocol ........................................... 43  
*Michel Dawirs, Joan Daemen*

## Session 2: The Java Card I

The OpenCard Framework ......................................................................................... 52  
*Reto Hermann, Dirk Husemann, Peter Trommler*

Smartcards - From Security Tokens to Intelligent Adjuncts ................................. 71  
*Boris Balacheff, Bruno Van Wilder, David Chan*

Formal Proof of Smart Card Applets Correctness ............................................. 85  
*Jean-Louis Lanet, Antoine Requet*

## Session 3: The Java Card II

Smart Card Payment over Internet with Privacy Protection ............................... 98  
*Pui-Nang Chan, Samuel T. Chanson, Ricci Ieong, James Pang*

Developing Smart Card-Based Applications Using Java Card ............................ 105  
*Jean-Jacques Vandewalle, Eric Vétillard*

The Performance of Modern Block Ciphers in Java ........................................... 125  
*Rüdiger Weis, Stefan Lucks*

Recoverable Persistent Memory for SmartCard ............................................... 134  
*Didier Donsez, Gilles Grimaud, Sylvain Lecomte*

## Session 4: Attacks and Dealing with Specific Threats

Pirate Card Rejection ............................................................................................. 141  
*David M. Goldschlag, David W. Kravitz*
<table>
<thead>
<tr>
<th>Session 5: Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Techniques for Low Cost Authentication and Message Authentication</td>
</tr>
<tr>
<td>Enhancing SESAMEV4 with Smart Cards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Session 6: Cryptography and Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Efficient Verifiable Encryption Scheme for Encryption of Discrete Logarithms</td>
</tr>
<tr>
<td>Efficient Smart-Card Based Anonymous Fingerprinting</td>
</tr>
<tr>
<td>Implementation of a Provably Secure, Smartcard-Based Key Distribution Protocol</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Session 7: Advanced Encryption Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serpent and Smartcards</td>
</tr>
<tr>
<td>Decorrelated Fast Cipher: An AES Candidate Well Suited for Low Cost Smart Cards Applications</td>
</tr>
</tbody>
</table>
## Table of Contents

### TwoFish on Smart Cards
*Bruce Schneier, Doug Whiting*

### The Block Cipher Rijndael
*Joan Daemen, Vincent Rijmen*

### Session 8: Architectures and Designs

- **Secure Log File Download Mechanisms for Smart Cards**
  *Constantinos Markantonakis*

- **The Vault, an Architecture for Smartcards to Gain Infinite Memory**
  *Patrick Biget*

- **A Data Driven Model for Designing Applications with Smart Cards**
  *William Caelli, Vincent Cordonnier, Anthony Watson*

- **Secure Personalization Using Proxy Cryptography**
  *Pierre Girard*

### Session 9: Efficient Implementations I

- **Recent Results on Modular Multiplications for Smart Cards**
  *Jean-François Dhem, Jean-Jacques Quisquater*

- **RSA Signature Algorithm for Microcontroller Implementation**
  *Guopei Qiao, Kwok-Yan Lam*

### Session 10: Efficient Implementations II

- **Efficient Ways to Implement Elliptic Curve Exponentiation on a Smart Card**
  *Alain Durand*

- **Reducing the Collision Probability of Alleged Comp128**
  *Helena Handschuh, Pascal Paillier*

- **Smart Card Crypto-Coprocessors for Public-Key Cryptography**
  *Helena Handschuh, Pascal Paillier*

### Author Index

*381*