

# Table of Contents

## Session 1: Electronic Money and Commerce

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| User-Defined Divisibility of Ecash and a Practical Implementation .....    | 1  |
| <i>Eli Biham, Amichai Shulman</i>                                          |    |
| An Operational Model of QuickPay - Extended Abstract .....                 | 19 |
| <i>Pieter H. Hartel, Jake Hill, Matt Sims</i>                              |    |
| Interoperable and Untraceable Debit-Tokens for Electronic Fee Collection . | 29 |
| <i>Cristian Radu, Frederic Klopfert, Jan De Meester</i>                    |    |
| The Banksys Signature Transport (BST) Protocol.....                        | 43 |
| <i>Michel Dawirs, Joan Daemen</i>                                          |    |

## Session 2: The Java Card I

|                                                                 |    |
|-----------------------------------------------------------------|----|
| The OpenCard Framework .....                                    | 52 |
| <i>Reto Hermann, Dirk Husemann, Peter Trommler</i>              |    |
| Smartcards - From Security Tokens to Intelligent Adjuncts ..... | 71 |
| <i>Boris Balacheff, Bruno Van Wilder, David Chan</i>            |    |
| Formal Proof of Smart Card Applets Correctness .....            | 85 |
| <i>Jean-Louis Lanet, Antoine Requet</i>                         |    |

## Session 3: The Java Card II

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Smart Card Payment over Internet with Privacy Protection .....   | 98  |
| <i>Pui-Nang Chan, Samuel T. Chanson, Ricci Jeong, James Pang</i> |     |
| Developing Smart Card-Based Applications Using Java Card .....   | 105 |
| <i>Jean-Jacques Vandewalle, Eric Vétillard</i>                   |     |
| The Performance of Modern Block Ciphers in Java .....            | 125 |
| <i>Rüdiger Weis, Stefan Lucks</i>                                |     |
| Recoverable Persistent Memory for SmartCard .....                | 134 |
| <i>Didier Donsez, Gilles Grimaud, Sylvain Lecomte</i>            |     |

## Session 4: Attacks and Dealing with Specific Threats

|                                              |     |
|----------------------------------------------|-----|
| Pirate Card Rejection .....                  | 141 |
| <i>David M. Goldschlag, David W. Kravitz</i> |     |

Secure Authentication with Multiple Parallel Keys ..... 150  
    *John Kelsey, Bruce Schneier*

Relaxing Tamper-Resistance Requirements for Smart Cards by Using  
(Auto-)Proxy Signatures ..... 157  
    *Marc Girault*

A Practical Implementation of the Timing Attack ..... 167  
    *Jean-François Dhem, François Koeune, Philippe-Alexandre Leroux,  
    Patrick Mestré, Jean-Jacques Quisquater, Jean-Louis Willems*

**Session 5: Authentication**

Techniques for Low Cost Authentication and Message Authentication..... 183  
    *Henri Gilbert*

Enhancing SESAMEV4 with Smart Cards ..... 193  
    *Mark Looi, Paul Ashley, Loo Tang Seet, Richard Au, Gary Gaskell,  
    Mark Vandenwauver*

How to Say "YES" with Smart Cards ..... 203  
    *Yair Frankel, Moti Yung*

**Session 6: Cryptography and Applications**

An Efficient Verifiable Encryption Scheme for Encryption of Discrete  
Logarithms..... 213  
    *Feng Bao*

Efficient Smart-Card Based Anonymous Fingerprinting ..... 221  
    *Josep Domingo-Ferrer, Jordi Herrera-Joancomartí*

Implementation of a Provably Secure, Smartcard-Based Key Distribution  
Protocol ..... 229  
    *Rob Jerdonek, Peter Honeyman, Kevin Coffman, Jim Rees,  
    Kip Wheeler*

The Block Cipher BKSQ ..... 236  
    *Joan Daemen and Vincent Rijmen*

**Session 7: Advanced Encryption Standard**

Serpent and Smartcards ..... 246  
    *Ross Anderson, Eli Biham, Lars Knudsen*

Decorrelated Fast Cipher: An AES Candidate Well Suited for Low Cost  
Smart Cards Applications ..... 254  
    *Guillaume Poupard, Serge Vaudenay*

|                                     |     |
|-------------------------------------|-----|
| Twofish on Smart Cards .....        | 265 |
| <i>Bruce Schneier, Doug Whiting</i> |     |

|                                    |     |
|------------------------------------|-----|
| The Block Cipher Rijndael .....    | 277 |
| <i>Joan Daemen, Vincent Rijmen</i> |     |

## **Session 8: Architectures and Designs**

|                                                           |     |
|-----------------------------------------------------------|-----|
| Secure Log File Download Mechanisms for Smart Cards ..... | 285 |
| <i>Constantinos Markantonakis</i>                         |     |

|                                                                         |     |
|-------------------------------------------------------------------------|-----|
| The Vault, an Architecture for Smartcards to Gain Infinite Memory ..... | 305 |
| <i>Patrick Biget</i>                                                    |     |

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| A Data Driven Model for Designing Applications with Smart Cards ..... | 313 |
| <i>William Caelli, Vincent Cordonnier, Anthony Watson</i>             |     |

|                                                       |     |
|-------------------------------------------------------|-----|
| Secure Personalization Using Proxy Cryptography ..... | 326 |
| <i>Pierre Girard</i>                                  |     |

## **Session 9: Efficient Implementations I**

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| Recent Results on Modular Multiplications for Smart Cards ..... | 336 |
| <i>Jean-François Dhem, Jean-Jacques Quisquater</i>              |     |

|                                                                  |     |
|------------------------------------------------------------------|-----|
| RSA Signature Algorithm for Microcontroller Implementation ..... | 353 |
| <i>Guopei Qiao, Kwok-Yan Lam</i>                                 |     |

## **Session 10: Efficient Implementations II**

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| Efficient Ways to Implement Elliptic Curve Exponentiation on a<br>Smart Card ..... | 357 |
| <i>Alain Durand</i>                                                                |     |

|                                                             |     |
|-------------------------------------------------------------|-----|
| Reducing the Collision Probability of Alleged Comp128 ..... | 366 |
| <i>Helena Handschuh, Pascal Paillier</i>                    |     |

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Smart Card Crypto-Coprocessors for Public-Key Cryptography ..... | 372 |
| <i>Helena Handschuh, Pascal Paillier</i>                         |     |

|                           |     |
|---------------------------|-----|
| <b>Author Index</b> ..... | 381 |
|---------------------------|-----|