

Contents

On Cryptographic Techniques for On-line Bankcard Payment Transactions Using Open Networks <i>Wenbo Mao</i>	1
A Certification Scheme for Electronic Commerce <i>Bruno Crispo, Mark Lomas</i>	19
Practical Escrow Cash System <i>Eiichiro Fujisaki, Tatsuaki Okamoto</i>	33
NetCard - A Practical Electronic-Cash System <i>Ross Anderson, Charalampos Maniavas and Chris Sutherland</i>	49
Electronic Payments of Small Amounts <i>Torben P. Pedersen</i>	59
PayWord and MicroMint: Two Simple Micropayment Schemes <i>Ronald L. Rivest, Adi Shamir</i>	69
Transactions Using Bets <i>David Wheeler</i>	89
Protocol Failures for RSA-Like Functions Using Lucas Sequences and Elliptic Curves <i>Marc Joye, Jean-Jacques Quisquater</i>	93
Efficient and Provable Secure Amplifications <i>Ronald Cramer, Ivan Damgård and Torben P. Pedersen</i>	101
A Comparison of RSA and the Naccache-Stern Public-Key Cryptosystem <i>Thomas W. Cusick</i>	111
IEEE P1363: A Standard for RSA, Diffie-Hellman and Elliptic-Curve Cryptography [Abstract] <i>Burton S. Kaliski Jr.</i>	117
Efficient and Secure Conference-Key Distribution <i>Mike Burmester, Yvo G. Desmedt</i>	119
Directed Signatures and Application to Threshold Cryptosystems <i>Chae Hoon Lim, Pil Joong Lee</i>	131

Key Escrow in Mutually Mistrusting Domains <i>Liqun Chen, Dieter Gollmann and Chris J. Mitchell</i>	139
Automatic Event-Stream Notarization Using Digital Signatures <i>Bruce Schneier, John Kelsey</i>	155
Why Isn't Trust Transitive? <i>Bruce Christianson, William S. Harbison</i>	171
Securing Residential Asynchronous Transfer Mode Networks <i>Shaw-Cheng Chuang, David Greaves</i>	177
Visual Cryptography II: Improving the Contrast Via the Cover Base <i>Moni Naori, Adi Shamir</i>	197
Author Index	203