

Table of Contents

Keynote Address: Security Protocols and the Swiss Army Knife <i>Roger Needham</i>	1
Mergers and Principals <i>Dieter Gollmann</i>	5
Discussion	14
Authentication and Naming <i>Michael Roe</i> (Discussion)	20
Users and Trust in Cyberspace <i>Pekka Nikander* and Kristiina Karvonen</i>	24
Discussion	36
Interactive Identification Protocols <i>Peter Landrock</i> (Discussion)	43
Open Questions <i>Peter Ryan</i> (Discussion)	49
Looking on the Bright Side of Black-Box Cryptography <i>Matt Blaze</i> (Discussion)	54
Government Access to Keys – Panel Discussion <i>Michael Roe, Ross Anderson, Bill Harbison, and Mark Lomas</i>	62
Making Sense of Specifications: The Formalization of SET <i>Giampaolo Bella, Fabio Massacci*, Lawrence C. Paulson,</i> <i>and Piero Tramontano</i>	74
Discussion	82
Lack of Explicitness Strikes Back <i>Giampaolo Bella</i>	87
Discussion	94
Review and Revocation of Access Privileges Distributed with PKI Certificates <i>Himanshu Khurana and Virgil D. Gligor*</i>	100
Discussion	113
The Correctness of Crypto Transaction Sets <i>Ross Anderson</i>	125
Discussion	128

Micro-management of Risk in a Trust-Based Billing System <i>John Ioannidis</i> (Discussion)	142
Broadening the Scope of Fault Tolerance within Secure Services <i>Geraint Price</i>	155
Discussion	165
DOS-Resistant Authentication with Client Puzzles <i>Tuomas Aura*</i> , <i>Pekka Nikander</i> , and <i>Jussi Pekka Leiwo</i>	170
Discussion	178
Public-Key Crypto-systems Using Symmetric-Key Crypto-algorithms <i>Bruce Christianson*</i> , <i>Bruno Crispo</i> , and <i>James A. Malcolm</i>	182
Discussion	184
Denial of Service – Panel Discussion <i>Virgil Gligor</i> , <i>Matt Blaze</i> , and <i>John Ioannidis</i>	194
The Resurrecting Duckling – What Next? <i>Frank Stajano</i>	204
Discussion	215
An Anonymous Auction Protocol Using “Money Escrow” <i>George Danezis</i> (Discussion)	223
Short Certification of Secure RSA Modulus <i>Wenbo Mao</i> (Discussion)	234
Authenticating Web-Based Virtual Shops Using Signature-Embedded Marks – A Practical Analysis <i>Hiroshi Yoshiura*</i> , <i>Takaaki Shigematsu</i> , <i>Seiichi Susaki</i> , <i>Tsukasa Saitoh</i> , <i>Hisashi Toyoshima</i> , <i>Chikako Kurita</i> , <i>Satoru Tezuka</i> , and <i>Ryoichi Sasaki</i>	238
Discussion	249
I Cannot Tell a Lie <i>Mark Lomas</i> (Discussion)	253
Afterward	256
Author Index	257

Security Protocols

8th International Workshops Cambridge, UK, April 3-5,
2000 Revised Papers

Christianson, B.; Crispo, B.; Malcolm, J.A.; Roe, M. (Eds.)

2001, VIII, 264 p., Softcover

ISBN: 978-3-540-42566-3