

CONTENTS

Keynote Lecture:

Trusted third parties for secure electronic commerce – Are they needed? 1
Fred Piper

1. Security Models And Access Control

<i>Prospectives for modelling trust in information security</i>	2
A. Jøsang	
<i>Analysis and implementation of a formal authorisation policy design approach</i>	14
Y. Bai and V. Varadharajan	
<i>An approach to dynamic domain and type enforcement</i>	26
J. Tidswell and J. Potter	
<i>Purpose-oriented access control model in object-based systems</i>	38
T. Tachikawa, H. Higaki, and M. Takizawa	
<i>User access domain management system - ADAMS</i>	50
M. Terada and Y. Murayama	

2. Network Security

<i>Revocation of unread email in an untrusted network</i>	62
A. D. Rubin, D. Boneh, and K. Fu	
<i>Security issues in asynchronous transfer mode</i>	76
R. Shankaran, V. Varadharajan, and M. Hitchens	
<i>A method to implement a denial of service protection base</i>	90
J. Leiwo and Y. Zheng	

3. Secure Hardware And Implementation Issues

<i>ProtectOS: Operating system and hardware support for small objects</i>	102
J. Holford and G. Mohay	
<i>Practical memory checkers for stacks, queues and dequeues</i>	114
M. Fischlin	

Panel Session: Cryptographic Policy Guidelines	126
Scott Charney (USA), Stephanie Perrin (Canada), Steve Orlowski (Australia), and Norman Reaburn (Australia), Nigel Hickson (UK), and Philippe Dejean (France)	

4. Cryptographic Functions And Ciphers

<i>Using cyclotomic polynomials to construct efficient discrete logarithm cryptosystems over finite fields</i>	127
A. K. Lenstra	
<i>A new hash function based on block cipher</i>	139
X. Yi and K.-Y. Lam	
<i>New lower bounds on nonlinearity and a class of highly nonlinear functions</i>	147
X.-M. Zhang and Y. Zheng	
<i>On the security of self-synchronous ciphers</i>	159
W. Millan and E. Dawson	
<i>Inefficiency of variant characteristics for substitution-permutation networks with position permutations</i>	171
A. Sadowski	

5. Authentication Codes And Secret Sharing Schemes

<i>Secret sharing with reusable polynomials</i>	183
L. Chen, D. Gollmann, C.J. Mitchell, and P. Wild	
<i>A message authentication code based on Latin squares</i>	194
S. Bakhtiari, R. Safavi-Naini, and J. Pieprzyk	
<i>Characterisation of (k, n) multi-receiver authentication</i>	204
K. Kurosawa and S. Obana	

6. Cryptanalysis

<i>Cryptanalysis of adaptive arithmetic coding encryption schemes</i>	216
J. Lim, C. Boyd, and E. Dawson	
<i>Fast correlation attacks and multiple linear approximations</i>	228
M. Salmasizadeh, L. Simpson, J. D. Golić, and E. Dawson	

7. Key Escrow

<i>Verifiable escrowed signature</i>	240
W. Mao	

<i>Democratic key escrow scheme</i>	249
C. W. Man and R. Safavi-Naini	
<i>Design and analyses of two basic protocols for use in TTP-based key escrow</i>	261
F. Bao, R. Deng, Y. Han, and A. Jeng	
8. Security Protocols And Key Management	
<i>Protection of data and delegated keys in digital distribution</i>	271
M. Mambo, E. Okamoto, and K. Sakurai	
<i>New micropayment schemes based on PayWords</i>	283
Y. Mu, V. Varadharajan, and Y.-X. Lin	
<i>On key agreement and conference key agreement</i>	294
C. Boyd	
<i>Identity-based and self-certified key-exchange protocols</i>	303
S. Saeednia	
9. Applications	
<i>Enabling technology for the trading of MPEG-encoded video</i>	314
J. Dittmann and A. Steinmetz	
<i>Image distribution method with embedded identifier scheme for copyright protection</i>	325
T. Abe, H. Fujii, and K. Kushima	
Author Index	337