

Table of Contents

A Few Thoughts on E-Commerce	1
<i>Yacov Yacobi</i>	
New CBC-MAC Forgery Attacks	3
<i>Karl Brincat, Chris J. Mitchell</i>	
Cryptanalysis of a Public Key Cryptosystem Proposed at ACISP 2000	15
<i>Amr Youssef, Guang Gong</i>	
Improved Cryptanalysis of the Self-Shrinking Generator	21
<i>Erik Zenner, Matthias Krause, Stefan Lucks</i>	
Attacks Based on Small Factors in Various Group Structures	36
<i>Chris Pavlovski, Colin Boyd</i>	
On Classifying Conference Key Distribution Protocols	51
<i>Shahrokh Saeednia, Rei Safavi-Naini, Willy Susilo</i>	
Pseudorandomness of MISTY-Type Transformations and the Block Cipher KASUMI	60
<i>Ju-Sung Kang, Okyeon Yi, Dowon Hong, Hyunsook Cho</i>	
New Public-Key Cryptosystem Using Divisor Class Groups	74
<i>Hwankoo Kim, SangJae Moon</i>	
First Implementation of Cryptographic Protocols Based on Algebraic Number Fields	84
<i>Andreas Meyer, Stefan Neis, Thomas Pfahler</i>	
Practical Key Recovery Schemes	104
<i>Sung-Ming Yen</i>	
Non-deterministic Processors	115
<i>David May, Henk L. Muller, Nigel P. Smart</i>	
Personal Secure Booting	130
<i>Naomaru Itoi, William A. Arbaugh, Samuela J. Pollack, Daniel M. Reeves</i>	
Evaluation of Tamper-Resistant Software Deviating from Structured Programming Rules	145
<i>Hideaki Goto, Masahiro Mambo, Hiroki Shizuya, Yasuyoshi Watanabe</i>	
A Strategy for MLS Workflow	159
<i>Vlad Ingar Wietrzyk, Makoto Takizawa, Vijay Varadharajan</i>	

Condition-Driven Integration of Security Services	176
<i>Clifford Neumann</i>	
SKETHIC: Secure Kernel Extension against Trojan Horses with Information-Carrying Codes	177
<i>Eun-Sun Cho, Sunho Hong, Sechang Oh, Hong-Jin Yeh, Manpyo Hong, Cheol-Won Lee, Hyundong Park, Chun-Sik Park</i>	
Secure and Private Distribution of Online Video and Some Related Cryptographic Issues	190
<i>Feng Bao, Robert Deng, Peirong Feng, Yan Guo, Hongjun Wu</i>	
Private Information Retrieval Based on the Subgroup Membership Problem	206
<i>Akihiro Yamamura, Taiichi Saito</i>	
A Practical English Auction with One-Time Registration	221
<i>Kazumasa Omote, Atsuko Miyaji</i>	
A User Authentication Scheme with Identity and Location Privacy	235
<i>Shouichi Hirose, Susumu Yoshida</i>	
An End-to-End Authentication Protocol in Wireless Application Protocol .	247
<i>Jong-Phil Yang, Weon Shin, Kyung-Hyune Rhee</i>	
Error Detection and Authentication in Quantum Key Distribution	260
<i>Akihiro Yamamura, Hirokazu Ishizuka</i>	
An Axiomatic Basis for Reasoning about Trust in PKIs	274
<i>Chuchang Liu, Maris Ozols, Tony Cant</i>	
A Knowledge-Based Approach to Internet Authorizations	292
<i>Along Lin</i>	
Applications of Trusted Review to Information Security	305
<i>John Yesberg, Marie Henderson</i>	
Network Security Modeling and Cyber Attack Simulation Methodology ...	320
<i>Sung-Do Chi, Jong Sou Park, Ki-Chan Jung, Jang-Se Lee</i>	
Cryptographic Salt: A Countermeasure against Denial-of-Service Attacks..	334
<i>DongGook Park, JungJoon Kim, Colin Boyd, Ed Dawson</i>	
Enhanced Modes of Operation for the Encryption in High-Speed Networks and Their Impact on QoS	344
<i>Oliver Jung, Sven Kuhn, Christoph Ruland, Kai Wollenweber</i>	
Improving the Availability of Time-Stamping Services	360
<i>Arne Ansper, Ahto Buldas, Märt Saarepera, Jan Willemsen</i>	

Randomness Required for Linear Threshold Sharing Schemes Defined over Any Finite Abelian Group	376
<i>Brian King</i>	
Democratic Systems	392
<i>Hossein Ghodosi, Josef Pieprzyk</i>	
Efficient and Unconditionally Secure Verifiable Threshold Changeable Scheme	403
<i>Ayako Maeda, Atsuko Miyaji, Mitsuru Tada</i>	
Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold Scheme for Implicit Certificates	417
<i>Douglas R. Stinson, Reto Stroh</i>	
How to Construct Fail-Stop Confirmer Signature Schemes	435
<i>Rei Safavi-Naini, Willy Susilo, Huaxiong Wang</i>	
Signature Schemes Based on 3rd Order Shift Registers	445
<i>Chik How Tan, Xun Yi, Chee Kheong Siew</i>	
Anonymous Statistical Survey of Attributes	460
<i>Toru Nakanishi, Yuji Sugiyama</i>	
Secure Mobile Agent Using Strong Non-designated Proxy Signature	474
<i>Byoungcheon Lee, Heesun Kim, Kwangjo Kim</i>	
Elliptic Curve Based Password Authenticated Key Exchange Protocols ...	487
<i>Colin Boyd, Paul Montague, Khanh Nguyen</i>	
Elliptic Curve Cryptography on a Palm OS Device	502
<i>André Weimerskirch, Christof Paar, Sheueling Chang Shantz</i>	
Reducing Certain Elliptic Curve Discrete Logarithms to Logarithms in a Finite Field	514
<i>Kyungah Shim</i>	
Author Index	521

Information Security and Privacy
6th Australasian Conference, ACISP 2001, Sydney,
Australia, July 11-13, 2001. Proceedings
Varadharajan, V.; Mu, Y. (Eds.)
2001, XI, 522 p., Softcover
ISBN: 978-3-540-42300-3