

Table of Contents

Key Handling

A New Distributed Primality Test for Shared RSA Keys Using Quadratic Fields	1
<i>Ingrid Biehl, Tsuyoshi Takagi</i>	
Security Analysis and Improvement of the Global Key Recovery System ..	17
<i>Yanjiang Yang, Feng Bao, Robert H. Deng</i>	
The LILI-II Keystream Generator	25
<i>A. Clark, Ed Dawson, J. Fuller, J. Golić, H-J. Lee, William Millan, S-J. Moon, L. Simpson</i>	
A Secure Re-keying Scheme with Key Recovery Property	40
<i>Hartono Kurnio, Rei Safavi-Naini, Huaxiong Wang</i>	

Trust and Secret Sharing

Modelling Trust Structures for Public Key Infrastructures	56
<i>Marie Henderson, Robert Coulter, Ed Dawson, Eiji Okamoto</i>	
Size of Broadcast in Threshold Schemes with Disenrollment	71
<i>S.G. Barwick, W.-A. Jackson, Keith M. Martin, Peter R. Wild</i>	
Requirements for Group Independent Linear Threshold Secret Sharing Schemes	89
<i>Brian King</i>	
Efficient Sharing of Encrypted Data	107
<i>Krista Bennett, Christian Grothoff, Tzvetan Horozov, Ioana Patrascu</i>	
Cheating Prevention in Linear Secret Sharing	121
<i>Josef Pieprzyk, Xian-Mo Zhang</i>	

Fast Computation

Note on Fast Computation of Secret RSA Exponents	136
<i>Wieland Fischer, Jean-Pierre Seifert</i>	
Better than BiBa: Short One-Time Signatures with Fast Signing and Verifying	144
<i>Leonid Reyzin, Natan Reyzin</i>	

Cryptanalysis I

Cryptanalysis of Stream Cipher COS (2, 128) Mode I	154
<i>Hongjun Wu, Feng Bao</i>	
The Analysis of Zheng-Seberry Scheme	159
<i>David Soldera, Jennifer Seberry, Chengxin Qu</i>	
Cryptanalysis of Stream Cipher Alpha1	169
<i>Hongjun Wu</i>	
A Linear Algebraic Attack on the AAFG1 Braid Group Cryptosystem ...	176
<i>James Hughes</i>	

Elliptic Curves

Isomorphism Classes of Hyperelliptic Curves of Genus 2 over \mathbb{F}_q	190
<i>Y. Choie, D. Yun</i>	
Compact Representation of Domain Parameters of Hyperelliptic Curve Cryptosystems	203
<i>Fangguo Zhang, Shengli Liu, Kwangjo Kim</i>	
A New Elliptic Curve Scalar Multiplication Algorithm to Resist Simple Power Analysis	214
<i>Yvonne Hitchcock, Paul Montague</i>	

AES

Strengthening the Key Schedule of the AES	226
<i>Lauren May, Matt Henricksen, William Millan, Gary Carter, Ed Dawson</i>	
On the Necessity of Strong Assumptions for the Security of a Class of Asymmetric Encryption Schemes	241
<i>Ron Steinfeld, Joonsang Baek, Yuliang Zheng</i>	

Security Management

Security Management: An Information Systems Setting	257
<i>M.J. Warren, L.M. Batten</i>	
Resolving Conflicts in Authorization Delegations	271
<i>Chun Ruan, Vijay Varadharajan</i>	
Policy Administration Domains	286
<i>M. Hitchens, Vijay Varadharajan, G. Saunders</i>	

Authentication

Maintaining the Validity of Digital Signatures in B2B Applications	303
<i>Jianying Zhou</i>	
Short 3-Secure Fingerprinting Codes for Copyright Protection	316
<i>Francesc Sebé, Josep Domingo-Ferrer</i>	
An Order-Specified Multisignature Scheme Secure against Active Insider Attacks	328
<i>Mitsuru Tada</i>	
Authenticated Operation of Open Computing Devices	346
<i>Paul England, Marcus Peinado</i>	
A New Identification Scheme Based on the Bilinear Diffie-Hellman Problem	362
<i>Myungsun Kim, Kwangjo Kim</i>	

Invited Talk

A Brief Outline of Research on Correlation Immune Functions	379
<i>Bimal Roy</i>	

Oblivious Transfer

m out of n Oblivious Transfer	395
<i>Yi Mu, Junqi Zhang, Vijay Varadharajan</i>	

Cryptanalysis II

On the Security of Reduced Versions of 3-Pass HAVAL	406
<i>Sangwoo Park, Soo Hak Sung, Seongtaek Chee, Jongin Lim</i>	
On Insecurity of the Side Channel Attack Countermeasure Using Addition-Subtraction Chains under Distinguishability between Addition and Doubling	420
<i>Katsuyuki Okeya, Kouichi Sakurai</i>	
On the Security of a Modified Paillier Public-Key Primitive	436
<i>Kouichi Sakurai, Tsuyoshi Takagi</i>	

Dealing with Adversaries

How to Play Sherlock Holmes in the World of Mobile Agents	449
<i>Biljana Cubaleska, Weidong Qiu, Markus Schneider</i>	
A Practical Approach Defeating Blackmailing	464
<i>Dong-Guk Han, Hye-Young Park, Young-Ho Park, Sangjin Lee, Dong Hoon Lee, Hyung-Jin Yang</i>	

Privacy against Piracy: Protecting Two-Level Revocable P-K
Traitor Tracing 482
 Hyun-Jeong Kim, Dong Hoon Lee, Moti Yung

Asynchronous Perfectly Secure Computation Tolerating Generalized
Adversaries 497
 M.V.N. Ashwin Kumar, K. Srinathan, C. Pandu Rangan

Author Index 513

Information Security and Privacy
7th Australian Conference, ACISP 2002 Melbourne,
Australia, July 3-5, 2002 Proceedings
Batten, L.; Seberry, J. (Eds.)
2002, XII, 516 p., Softcover
ISBN: 978-3-540-43861-8