Table of Contents

Cryptographic Applications

Multi-party Computation from Any Linear Secret Sharing Scheme
Unconditionally Secure against Adaptive Adversary:
The Zero-Error Case .......................................................... 1
  Ventsislav Nikov, Svetla Nikova, Bart Preneel

Optimized \( \chi^2 \)-Attack against RC6 .................................. 16
  Norihisa Isogai, Takashi Matsunaka, Atsuko Miyaji

Anonymity-Enhanced Pseudonym System ............................... 33
  Yuko Tamura, Atsuko Miyaji

Intrusion Detection

Using Feedback to Improve Masquerade Detection .................. 48
  Kwong H. Yung

Efficient Presentation of Multivariate Audit Data for Intrusion
Detection of Web-Based Internet Services ............................. 63
  Zhi Guo, Kwok-Yan Lam, Siu-Leung Chung, Ming Gu, Jia-Guang Sun

An IP Traceback Scheme Integrating DPM and PPM .................. 76
  Fan Min, Jun-yan Zhang, Guo-wie Yang

Cryptographic Algorithms

Improved Scalable Hash Chain Traversal .............................. 86
  Sung-Ryul Kim

Round Optimal Distributed Key Generation of Threshold
Cryptosystem Based on Discrete Logarithm Problem ................ 96
  Rui Zhang, Hideki Imai

On the Security of Two Threshold Signature Schemes with
Traceable Signers ............................................................ 111
  Guilin Wang, Xiaoxi Han, Bo Zhu

Digital Signature

Proxy and Threshold One-Time Signatures ............................ 123
  Mohamed Al-Ibrahim, Anton Cerny
A Threshold GQ Signature Scheme ........................................ 137
  Li-Shan Liu, Cheng-Kang Chu, Wen-Guey Tzeng

Generalized Key-Evolving Signature Schemes or How to Foil an
Armed Adversary .......................................................... 151
  Gene Itkis, Peng Xie

A Ring Signature Scheme Based on the Nyberg-Rueppel
Signature Scheme .......................................................... 169
  Chong-zhi Gao, Zheng-an Yao, Lei Li

Security Modelling

Modelling and Evaluating Trust Relationships in Mobile Agents
Based Systems .............................................................. 176
  Ching Lin, Vijay Varadharajan

An Authorization Model for E-consent Requirement in a Health
Care Application .......................................................... 191
  Chun Ruan, Vijay Varadharajan

PLI: A New Framework to Protect Digital Content for P2P Networks ... 206
  Guofei Gu, Bin B. Zhu, Shipeng Li, Shiyong Zhang

Web Security

Improved Algebraic Traitor Tracing Scheme ................................ 217
  Chunyan Bai, Guiliang Feng

Common Vulnerability Markup Language .................................. 228
  Haitao Tian, Liusheng Huang, Zhi Zhou, Hui Zhang

Trust on Web Browser: Attack vs. Defense ............................... 241
  Tie-Yan Li, Yongdong Wu

Security Protocols

Security Protocols for Biometrics-Based Cardholder Authentication
in Smartcards ............................................................... 254
  Luciano Rila, Chris J. Mitchell

Does It Need Trusted Third Party? Design of Buyer-Seller
Watermarking Protocol without Trusted Third Party .................... 265
  Jae-Gwi Choi, Kowichi Sakurai, Ji-Hwan Park

Using OCSP to Secure Certificate-Using Transactions in M-commerce ... 280
  Jose L. Muñoz, Jordi Forné, Oscar Esparza, Bernabe Miguel Soriano
# Cryptanalysis

**Differential Fault Analysis on A.E.S**  
*Pierre Dusart, Gilles Letourneux, Olivier Vivolo*  
293

**Side-Channel Attack on Substitution Blocks**  
*Roman Novak*  
307

**Timing Attack against Implementation of a Parallel Algorithm for Modular Exponentiation**  
*Yasuyuki Sakai, Kouichi Sakurai*  
319

**A Fast Correlation Attack for LFSR-Based Stream Ciphers**  
*Sarbani Palit, Bimal K. Roy, Arindom De*  
331

# Key Management

**Making the Key Agreement Protocol in Mobile Ad Hoc Network More Efficient**  
*Gang Yao, Kui Ren, Feng Bao, Robert H. Deng, Dengguo Feng*  
343

**An Efficient Tree-Based Group Key Agreement Using Bilinear Map**  
*Sangwon Lee, Yongdae Kim, Kwangjo Kim, Dae-Hyun Ryu*  
357

**A Key Recovery Mechanism for Reliable Group Key Management**  
*Taenam Cho, Sang-Ho Lee*  
372

# Efficient Implementations

**Efficient Software Implementation of LFSR and Boolean Function and Its Application in Nonlinear Combiner Model**  
*Sandeepan Chowdhury, Subhamoy Maitra*  
387

**Efficient Distributed Signcryption Scheme as Group Signcryption**  
*DongJin Kwak, SangJae Moon*  
403

**Architectural Enhancements for Montgomery Multiplication on Embedded RISC Processors**  
*Johann GroßschädI, Guy-Armand Kamendje*  
418

# Author Index

435
Applied Cryptography and Network Security
Zhou, J.; Young, M.; Han, Y. (Eds.)
2003, XII, 440 p., Softcover
ISBN: 978-3-540-20208-0