

Table of Contents

Cryptographic Applications

Multi-party Computation from Any Linear Secret Sharing Scheme Unconditionally Secure against Adaptive Adversary: The Zero-Error Case	1
<i>Ventzislav Nikov, Svetla Nikova, Bart Preneel</i>	
Optimized χ^2 -Attack against RC6	16
<i>Norihisa Isogai, Takashi Matsunaka, Atsuko Miyaji</i>	
Anonymity-Enhanced Pseudonym System	33
<i>Yuko Tamura, Atsuko Miyaji</i>	

Intrusion Detection

Using Feedback to Improve Masquerade Detection	48
<i>Kwong H. Yung</i>	
Efficient Presentation of Multivariate Audit Data for Intrusion Detection of Web-Based Internet Services	63
<i>Zhi Guo, Kwok-Yan Lam, Siu-Leung Chung, Ming Gu, Jia-Guang Sun</i>	
An IP Traceback Scheme Integrating DPM and PPM	76
<i>Fan Min, Jun-yan Zhang, Guo-wie Yang</i>	

Cryptographic Algorithms

Improved Scalable Hash Chain Traversal	86
<i>Sung-Ryul Kim</i>	
Round Optimal Distributed Key Generation of Threshold Cryptosystem Based on Discrete Logarithm Problem	96
<i>Rui Zhang, Hideki Imai</i>	
On the Security of Two Threshold Signature Schemes with Traceable Signers	111
<i>Guilin Wang, Xiaoxi Han, Bo Zhu</i>	

Digital Signature

Proxy and Threshold One-Time Signatures	123
<i>Mohamed Al-Ibrahim, Anton Cerny</i>	

A Threshold GQ Signature Scheme	137
<i>Li-Shan Liu, Cheng-Kang Chu, Wen-Guey Tzeng</i>	

Generalized Key-Evolving Signature Schemes or How to Foil an Armed Adversary	151
<i>Gene Itkis, Peng Xie</i>	

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

Security Modelling

Modelling and Evaluating Trust Relationships in Mobile Agents Based Systems	176
<i>Ching Lin, Vijay Varadharajan</i>	

An Authorization Model for E-consent Requirement in a Health Care Application	191
<i>Chun Ruan, Vijay Varadharajan</i>	

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

Web Security

Improved Algebraic Traitor Tracing Scheme	217
<i>Chunyan Bai, Guiliang Feng</i>	

Common Vulnerability Markup Language	228
<i>Haitao Tian, Liusheng Huang, Zhi Zhou, Hui Zhang</i>	

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

Security Protocols

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

Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party	265
<i>Jae-Gwi Choi, Kouichi Sakurai, Ji-Hwan Park</i>	

Using OCSP to Secure Certificate-Using Transactions in M-commerce ...	280
<i>Jose L. Muñoz, Jordi Forné, Oscar Esparza, Bernabe Miguel Soriano</i>	

Cryptanalysis

Differential Fault Analysis on A.E.S	293
<i>Pierre Dusart, Gilles Letourneux, Olivier Vivolo</i>	
Side-Channel Attack on Substitution Blocks	307
<i>Roman Novak</i>	
Timing Attack against Implementation of a Parallel Algorithm for Modular Exponentiation	319
<i>Yasuyuki Sakai, Kouichi Sakurai</i>	
A Fast Correlation Attack for LFSR-Based Stream Ciphers	331
<i>Sarbani Palit, Bimal K. Roy, Arindom De</i>	

Key Management

Making the Key Agreement Protocol in Mobile Ad Hoc Network More Efficient	343
<i>Gang Yao, Kui Ren, Feng Bao, Robert H. Deng, Dengguo Feng</i>	
An Efficient Tree-Based Group Key Agreement Using Bilinear Map	357
<i>Sangwon Lee, Yongdae Kim, Kwangjo Kim, Dae-Hyun Ryu</i>	
A Key Recovery Mechanism for Reliable Group Key Management	372
<i>Taenam Cho, Sang-Ho Lee</i>	

Efficient Implementations

Efficient Software Implementation of LFSR and Boolean Function and Its Application in Nonlinear Combiner Model	387
<i>Sandeepan Chowdhury, Subhamoy Maitra</i>	
Efficient Distributed Signcryption Scheme as Group Signcryption	403
<i>DongJin Kwak, SangJae Moon</i>	
Architectural Enhancements for Montgomery Multiplication on Embedded RISC Processors	418
<i>Johann Großschädl, Guy-Armand Kamendje</i>	

Author Index	435
-------------------------------	------------

Applied Cryptography and Network Security
First International Conference, ACNS 2003. Kunming,
China, October 16-19, 2003, Proceedings
Zhou, J.; Yung, M.; Han, Y. (Eds.)
2003, XII, 440 p., Softcover
ISBN: 978-3-540-20208-0