

Table of Contents

Two-Server Password-Only Authenticated Key Exchange	1
<i>Jonathan Katz, Philip MacKenzie, Gelareh Taban, and Virgil Gligor</i>	
Strengthening Password-Based Authentication Protocols	
Against Online Dictionary Attacks	17
<i>Peng Wang, Yongdae Kim, Vishal Kher, and Taekyoung Kwon</i>	
Cryptanalysis of an Improved Client-to-Client Password-Authenticated	
Key Exchange (C2C-PAKE) Scheme	33
<i>Raphael C.-W. Phan and Bok-Min Goi</i>	
Efficient Security Mechanisms	
for Overlay Multicast-Based Content Distribution	40
<i>Sencun Zhu, Chao Yao, Donggang Liu, Sanjeev Setia, and Sushil Jajodia</i>	
A Traitor Tracing Scheme Based on RSA for Fast Decryption	56
<i>John Patrick McGregor, Yiqun Lisa Yin, and Ruby B. Lee</i>	
N-Party Encrypted Diffie-Hellman Key Exchange Using Different Passwords	75
<i>Jin Wook Byun and Dong Hoon Lee</i>	
Messin' with Texas Deriving Mother's Maiden Names Using Public Records	91
<i>Virgil Griffith and Markus Jakobsson</i>	
Mitigating Network Denial-of-Service	
Through Diversity-Based Traffic Management	104
<i>Ashraf Matrawy, Paul C. van Oorschot, and Anil Somayaji</i>	
Searching for High-Value Rare Events with Uncheatable Grid Computing	122
<i>Wenliang Du and Michael T. Goodrich</i>	
Digital Signatures Do Not Guarantee Exclusive Ownership	138
<i>Thomas Pornin and Julien P. Stern</i>	
Thompson's Group and Public Key Cryptography	151
<i>Vladimir Shpilrain and Alexander Ushakov</i>	
Rainbow, a New Multivariable Polynomial Signature Scheme	164
<i>Jintai Ding and Dieter Schmidt</i>	
Badger – A Fast and Provably Secure MAC	176
<i>Martin Boesgaard, Thomas Christensen, and Erik Zenner</i>	
IDS False Alarm Reduction Using Continuous and Discontinuous Patterns	192
<i>Abdulrahman Alharby and Hideki Imai</i>	

Indexing Information for Data Forensics	206
<i>Michael T. Goodrich, Mikhail J. Atallah, and Roberto Tamassia</i>	
Model Generalization and Its Implications on Intrusion Detection	222
<i>Zhuowei Li, Amitabha Das, and Jianying Zhou</i>	
Intrusion-Resilient Secure Channels	238
<i>Gene Itkis, Robert McNeerney Jr., and Scott Russell</i>	
Optimal Asymmetric Encryption and Signature Paddings	254
<i>Benoît Chevallier-Mames, Duong Hieu Phan, and David Pointcheval</i>	
Efficient and Leakage-Resilient Authenticated Key Transport Protocol Based on RSA	269
<i>SeongHan Shin, Kazukuni Kobara, and Hideki Imai</i>	
Identity Based Encryption Without Redundancy	285
<i>Benoît Libert and Jean-Jacques Quisquater</i>	
OACerts: Oblivious Attribute Certificates	301
<i>Jiangtao Li and Ninghui Li</i>	
Dynamic k -Times Anonymous Authentication	318
<i>Lan Nguyen and Rei Safavi-Naini</i>	
Efficient Anonymous Roaming and Its Security Analysis	334
<i>Guomin Yang, Duncan S. Wong, and Xiaotie Deng</i>	
Quantifying Security in Hybrid Cellular Networks	350
<i>Markus Jakobsson and Liu Yang</i>	
Off-Line Karma: A Decentralized Currency for Peer-to-peer and Grid Applications	364
<i>Flavio D. Garcia and Jaap-Henk Hoepman</i>	
Building Reliable Mix Networks with Fair Exchange	378
<i>Michael K. Reiter, XiaoFeng Wang, and Matthew Wright</i>	
SCARE of the DES (Side Channel Analysis for Reverse Engineering of the Data Encryption Standard)	393
<i>Rémy Daudigny, Hervé Ledig, Frédéric Muller, and Frédéric Valette</i>	
Robust Key Extraction from Physical Uncloneable Functions	407
<i>B. Škorić, P. Tuyls, and W. Oprey</i>	
Efficient Constructions for One-Way Hash Chains	423
<i>Yih-Chun Hu, Markus Jakobsson, and Adrian Perrig</i>	
Privacy Preserving Keyword Searches on Remote Encrypted Data	442
<i>Yan-Cheng Chang and Michael Mitzenmacher</i>	

An Efficient Solution to the Millionaires' Problem Based on Homomorphic Encryption	456
<i>Hsiao-Ying Lin and Wen-Guey Tzeng</i>	
Non-interactive Zero-Knowledge Arguments for Voting	467
<i>Jens Groth</i>	
Short Signature and Universal Designated Verifier Signature Without Random Oracles	483
<i>Rui Zhang, Jun Furukawa, and Hideki Imai</i>	
Efficient Identity Based Ring Signature	499
<i>Sherman S.M. Chow, Siu-Ming Yiu, and Lucas C.K. Hui</i>	
New Signature Schemes with Coupons and Tight Reduction	513
<i>Benoît Chevallier-Mames</i>	
Author Index	529

Applied Cryptography and Network Security
Third International Conference, ACNS 2005, New York,
NY, USA, June 7-10, 2005, Proceedings
Ioannidis, J.; Keromytis, A.D.; Yung, M. (Eds.)
2005, XII, 530 p., Softcover
ISBN: 978-3-540-26223-7