

Table of Contents

| | |
|--|-----|
| A Fast Square Root Computation Using the Frobenius Mapping | 1 |
| <i>Wang Feng, Yasuyuki Nogami, Yoshitaka Morikawa</i> | |
| A Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption | 11 |
| <i>Dang Nguyen Duc, Jung Hee Cheon, Kwangjo Kim</i> | |
| Secure Route Structures for the Fast Dispatch of Large-Scale Mobile Agents | 22 |
| <i>Yan Wang, Chi-Hung Chi, Tieyan Li</i> | |
| On the RS-Code Construction of Ring Signature Schemes and a Threshold Setting of RST | 34 |
| <i>Duncan S. Wong, Karyin Fung, Joseph K. Liu, Victor K. Wei</i> | |
| A Policy Based Framework for Access Control | 47 |
| <i>Ricardo Nabhen, Edgard Jamhour, Carlos Maziero</i> | |
| Trading-Off Type-Inference Memory Complexity against Communication | 60 |
| <i>Konstantin Hyppönen, David Naccache, Elena Trichina, Alexei Tchoulkine</i> | |
| Security Remarks on a Group Signature Scheme with Member Deletion | 72 |
| <i>Guilin Wang, Feng Bao, Jianying Zhou, Robert H. Deng</i> | |
| An Efficient Known Plaintext Attack on FEA-M | 84 |
| <i>Hongjun Wu, Feng Bao, Robert H. Deng</i> | |
| An Efficient Public-Key Framework | 88 |
| <i>Jianying Zhou, Feng Bao, Robert Deng</i> | |
| ROCEM: Robust Certified E-mail System Based on Server-Supported Signature | 100 |
| <i>Jong-Phil Yang, Chul Sur, Kyung Hyune Rhee</i> | |
| Practical Service Charge for P2P Content Distribution | 112 |
| <i>Jose Antonio Onieva, Jianying Zhou, Javier Lopez</i> | |
| ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback | 124 |
| <i>Henry C.J. Lee, Vrizlynn L.L. Thing, Yi Xu, Miao Ma</i> | |

| | |
|---|-----|
| A Lattice Based General Blind Watermark Scheme | 136 |
| <i>Yongliang Liu, Wen Gao, Zhao Wang, Shaohui Liu</i> | |
| Role-Based Access Control and the Access Control Matrix | 145 |
| <i>Gregory Saunders, Michael Hitchens, Vijay Varadharajan</i> | |
| Broadcast Encryption Schemes Based on the Sectioned Key Tree..... | 158 |
| <i>Miodrag J. Mihaljević</i> | |
| Research on the Collusion Estimation | 170 |
| <i>Gang Li, Jie Yang</i> | |
| Multiple Description Coding for Image Data Hiding Jointly in the Spatial and DCT Domains | 179 |
| <i>Mohsen Ashourian, Yo-Sung Ho</i> | |
| Protocols for Malicious Host Revocation | 191 |
| <i>Oscar Esparza, Miguel Soriano, Jose L. Muñoz, Jordi Forné</i> | |
| A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code | 202 |
| <i>Pik-Wah Chan, Michael R. Lyu</i> | |
| A Novel Two-Level Trust Model for Grid | 214 |
| <i>Tie-Yan Li, HuaFei Zhu, Kwok-Yan Lam</i> | |
| Practical t-out-n Oblivious Transfer and Its Applications..... | 226 |
| <i>Qian-Hong Wu, Jian-Hong Zhang, Yu-Min Wang</i> | |
| Adaptive Collusion Attack to a Block Oriented Watermarking Scheme | 238 |
| <i>Yongdong Wu, Robert Deng</i> | |
| ID-Based Distributed “Magic Ink” Signature from Pairings..... | 249 |
| <i>Yan Xie, Fangguo Zhang, Xiaofeng Chen, Kwangjo Kim</i> | |
| A Simple Anonymous Fingerprinting Scheme Based on Blind Signature | 260 |
| <i>Yan Wang, Shuwang Lü, Zhenhua Liu</i> | |
| Compact Conversion Schemes for the Probabilistic OW-PCA Primitives | 269 |
| <i>Yang Cui, Kazukuni Kobara, Hideki Imai</i> | |
| A Security Verification Method for Information Flow Security Policies Implemented in Operating Systems | 280 |
| <i>Xiao-dong Yi, Xue-jun Yang</i> | |

| | |
|---|------------|
| A Novel Efficient Group Signature Scheme with Forward Security | 292 |
| <i>Jianhong Zhang, Qianhong Wu, Yumin Wang</i> | |
| Variations of Diffie-Hellman Problem | 301 |
| <i>Feng Bao, Robert H. Deng, HuaFei Zhu</i> | |
| A Study on the Covert Channel Detection of TCP/IP Header Using Support Vector Machine | 313 |
| <i>Taeshik Sohn, JungTaek Seo, Jongsub Moon</i> | |
| A Research on Intrusion Detection Based on Unsupervised Clustering and Support Vector Machine | 325 |
| <i>Min Luo, Lina Wang, Huanguo Zhang, Jin Chen</i> | |
| UC-RBAC: A Usage Constrained Role-Based Access Control Model | 337 |
| <i>Zhen Xu, Dengguo Feng, Lan Li, Hua Chen</i> | |
| (Virtually) Free Randomization Techniques for Elliptic Curve Cryptography | 348 |
| <i>Mathieu Ciet, Marc Joye</i> | |
| An Optimized Multi-bits Blind Watermarking Scheme | 360 |
| <i>Xiaoqiang Li, Xiangyang Xue, Wei Li</i> | |
| A Compound Intrusion Detection Model | 370 |
| <i>Jianhua Sun, Hai Jin, Hao Chen, Qian Zhang, Zongfen Han</i> | |
| An Efficient Convertible Authenticated Encryption Scheme and Its Variant | 382 |
| <i>Hui-Feng Huang, Chin-Chen Chang</i> | |
| Space-Economical Reassembly for Intrusion Detection System | 393 |
| <i>Meng Zhang, Jiu-bin Ju</i> | |
| A Functional Decomposition of Virus and Worm Programs | 405 |
| <i>J. Krishna Murthy</i> | |
| Author Index | 415 |

Information and Communications Security
5th International Conference, ICICS 2003, Huhehaote,
China, October 10-13, 2003, Proceedings
Perner, P.; Gollmann, D.; Zhou, J. (Eds.)
2003, X, 418 p., Softcover
ISBN: 978-3-540-20150-2