Table of Contents

On the Minimal Assumptions of Group Signature Schemes 1
Michel Abdalla and Bogdan Warinschi

Perfect Concurrent Signature Schemes 14
Willy Susilo, Yi Mu, and Fangguo Zhang

New Identity-Based Ring Signature Schemes 27
Javier Herranz and Germán Sáez

On the Security of a Multi-party Certified Email Protocol 40
Jianying Zhou

Robust Metering Schemes for General Access Structures 53
Ventzislav Nikov, Svetla Nikova, and Bart Preneel

PAYFLUX – Secure Electronic Payment in Mobile Ad Hoc Networks 66
Klaus Herrmann and Michael A. Jaeger

Flexible Verification of MPEG-4 Stream in Peer-to-Peer CDN 79
Tieyan Li, Yongdong Wu, Di Ma, Huafei Zhu, and Robert H. Deng

Provably Secure Authenticated Tree Based Group Key Agreement 92
Ratna Dutta, Rana Barua, and Palash Sarkar

Taxonomic Consideration to OAEP Variants and Their Security 105
Yuichi Komano and Kazuo Ohta

Factorization-Based Fail-Stop Signatures Revisited 118
Katja Schmidt-Samoa

A Qualitative Evaluation of Security Patterns 132
Spyros T. Halkidis, Alexander Chatzigeorgiou, and George Stephanides

Type Inferability and Decidability of the Security Problem
Against Inference Attacks on Object-Oriented Databases 145
Yasunori Ishihara, Yumi Shimakawa, and Toru Fujiwara

Volatile Memory Computer Forensics to Detect Kernel Level Compromise 158
Sandra Ring and Eric Cole

A Secure Workflow Model Based on Distributed Constrained Role
and Task Assignment for the Internet 171
Ilanit Moodahi, Ehud Gudes, Oz Lavee, and Amnon Meisels

Hydan: Hiding Information in Program Binaries 187
Rakan El-Khalil and Angelos D. Keromytis

A Semi-fragile Steganographic Digital Signature for Images 200
Luke Hebbes and Andrew Lenaghan

Identification of Traitors Using a Trellis 211
Marcel Fernandez and Miguel Soriano

Decentralized Publish-Subscribe System to Prevent Coordinated Attacks
via Alert Correlation 223
Joaquin Garcia, Fabien Autrel, Joan Borrell, Sergio Castillo,
Frederic Cuppens, and Guillermo Navarro

Reflector Attack Traceback System with Pushback Based iTrace Mechanism 236
Hyung-Woo Lee, Sung-Hyun Yun, Taekyoung Kwon, Jae-Sung Kim,
Hee-Un Park, and Nam-Ho Oh

Automatic Covert Channel Analysis of a Multilevel Secure Component 249
Ruggero Lanotte, Andrea Maggiolo-Schettini, Simone Tini,
Angelo Troina, and Enrico Tronci

Sound Approximations to Diffie-Hellman Using Rewrite Rules 262
Christopher Lynch and Catherine Meadows

On Randomized Addition-Subtraction Chains
to Counteract Differential Power Attacks 278
Anton Kargl and Götz Wiesend

New Power Analysis on the Ha-Moon Algorithm and the MIST Algorithm 291
Sang Gyoo Sim, Dong Jin Park, and Pil Joong Lee

Modified Power-Analysis Attacks on XTR and an Efficient Countermeasure 305
Dong-Guk Han, Tetsuya Izu, Jongin Lim, and Kouichi Sakurai

Modelling Dependencies Between Classifiers in Mobile Masquerader Detection . . 318
Oleksiy Mazhelis, Seppo Puuronen, and Jari Veijalainen

Threat Analysis on NEtwork MObility (NEMO) 331
Souhwan Jung, Fan Zhao, S. Felix Wu, and HyunGon Kim

Macro-level Attention to Mobile Agent Security:
Introducing the Mobile Agent Secure Hub Infrastructure Concept 343
Michelangelo Giansiracusa, Selwyn Russell, Andrew Clark, and Volker Roth

Securing the Destination-Sequenced Distance Vector Routing Protocol
(S-DSDV) 358
Tao Wan, Evangelos Kranakis, and Paul C. van Oorschot

Secret-Public Storage Trade-Off for Broadcast Encryption Key Management 375
Miodrag J. Mihaljević, Marc P.C. Fossorier, and Hideki Imai

Security Analysis of the Generalized Self-shrinking Generator 388
Bin Zhang, Hongjun Wu, Dengguo Feng, and Feng Bao

On Asymptotic Security Estimates in XL
and Gröbner Bases-Related Algebraic Cryptanalysis 401
Bo-Yin Yang, Jiun-Ming Chen, and Nicolas T. Courtois

On Some Weak Extensions of AES and BES 414
Jean Monnerat and Serge Vaudenay

Clock Control Sequence Reconstruction in the Ciphertext Only Attack Scenario .. 427
Slobodan Petrović and Amparo Fúster-Sabater

Transient Fault Induction Attacks on XTR 440
Mathieu Ciet and Christophe Giraud

Adaptive-CCA on OpenPGP Revisited 452
Hsi-Chung Lin, Sung-Ming Yen, and Guan-Ting Chen

A New Key-Insulated Signature Scheme 465
Nicolás González-Deleito, Olivier Markowitch, and Emmanuel Dall'Olio

Secure Hierarchical Identity Based Signature and Its Application 480
Sherman S.M. Chow, Lucas C.K. Hui, Siu Ming Yiu, and K.P. Chow

Multi-designated Verifiers Signatures 495
Fabien Laguillaumie and Damien Vergnaud

Dynamic Access Control for Multi-privileged Group Communications 508
Di Ma, Robert H. Deng, Yongdong Wu, and Tieyan Li

An Efficient Authentication Scheme Using Recovery Information in Signature ... 520
Kihun Hong and Souhwan Jung

Time-Scoped Searching of Encrypted Audit Logs 532
Darren Davis, Fabian Monrose, and Michael K. Reiter

Rights-Carrying and Self-enforcing Information Objects
for Information Distribution Systems 546
Habtamu Abie, Pål Spilling, and Bent Foyn

Author Index 563