

Table of Contents

On the Minimal Assumptions of Group Signature Schemes	1
<i>Michel Abdalla and Bogdan Warinschi</i>	
Perfect Concurrent Signature Schemes	14
<i>Willy Susilo, Yi Mu, and Fangguo Zhang</i>	
New Identity-Based Ring Signature Schemes	27
<i>Javier Herranz and Germán Sáez</i>	
On the Security of a Multi-party Certified Email Protocol	40
<i>Jianying Zhou</i>	
Robust Metering Schemes for General Access Structures	53
<i>Ventzislav Nikov, Svetla Nikova, and Bart Preneel</i>	
PAYFLUX – Secure Electronic Payment in Mobile Ad Hoc Networks	66
<i>Klaus Herrmann and Michael A. Jaeger</i>	
Flexible Verification of MPEG-4 Stream in Peer-to-Peer CDN	79
<i>Tieyan Li, Yongdong Wu, Di Ma, Huafei Zhu, and Robert H. Deng</i>	
Provably Secure Authenticated Tree Based Group Key Agreement	92
<i>Ratna Dutta, Rana Barua, and Palash Sarkar</i>	
Taxonomic Consideration to OAEP Variants and Their Security	105
<i>Yuichi Komano and Kazuo Ohta</i>	
Factorization-Based Fail-Stop Signatures Revisited	118
<i>Katja Schmidt-Samoa</i>	
A Qualitative Evaluation of Security Patterns	132
<i>Spyros T. Halkidis, Alexander Chatzigeorgiou, and George Stephanides</i>	
Type Inferability and Decidability of the Security Problem Against Inference Attacks on Object-Oriented Databases	145
<i>Yasunori Ishihara, Yumi Shimakawa, and Toru Fujiwara</i>	
Volatile Memory Computer Forensics to Detect Kernel Level Compromise	158
<i>Sandra Ring and Eric Cole</i>	
A Secure Workflow Model Based on Distributed Constrained Role and Task Assignment for the Internet	171
<i>Itanit Moodahi, Ehud Gudes, Oz Lavee, and Amnon Meisels</i>	

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
*Joaquín García, 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
<i>Miodrag J. Mihaljević, Marc P.C. Fossorier, and Hideki Imai</i>	
Security Analysis of the Generalized Self-shrinking Generator	388
<i>Bin Zhang, Hongjun Wu, Dengguo Feng, and Feng Bao</i>	
On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis	401
<i>Bo-Yin Yang, Jiun-Ming Chen, and Nicolas T. Courtois</i>	
On Some Weak Extensions of AES and BES	414
<i>Jean Monnerat and Serge Vaudenay</i>	
Clock Control Sequence Reconstruction in the Ciphertext Only Attack Scenario . .	427
<i>Slobodan Petrović and Amparo Fúster-Sabater</i>	
Transient Fault Induction Attacks on XTR	440
<i>Mathieu Ciet and Christophe Giraud</i>	
Adaptive-CCA on OpenPGP Revisited	452
<i>Hsi-Chung Lin, Sung-Ming Yen, and Guan-Ting Chen</i>	
A New Key-Insulated Signature Scheme	465
<i>Nicolás González-Deleito, Olivier Markowitch, and Emmanuel Dall’Olio</i>	
Secure Hierarchical Identity Based Signature and Its Application	480
<i>Sherman S.M. Chow, Lucas C.K. Hui, Siu Ming Yiu, and K.P. Chow</i>	
Multi-designated Verifiers Signatures	495
<i>Fabien Laguillaumie and Damien Vergnaud</i>	
Dynamic Access Control for Multi-privileged Group Communications	508
<i>Di Ma, Robert H. Deng, Yongdong Wu, and Tiejun Li</i>	
An Efficient Authentication Scheme Using Recovery Information in Signature . . .	520
<i>Kihun Hong and Souhwan Jung</i>	
Time-Scoped Searching of Encrypted Audit Logs	532
<i>Darren Davis, Fabian Monrose, and Michael K. Reiter</i>	
Rights-Carrying and Self-enforcing Information Objects for Information Distribution Systems	546
<i>Habtamu Abie, Pål Spilling, and Bent Foyen</i>	
Author Index	563



<http://www.springer.com/978-3-540-23563-7>

Information and Communications Security
6th International Conference, ICICS 2004, Malaga,
Spain, October 27-29, 2004. Proceedings
López, J.; Okamoto, E. (Eds.)
2004, XII, 572 p., Softcover
ISBN: 978-3-540-23563-7