

Table of Contents

Practical Security in Public-Key Cryptography	1
<i>David Pointcheval</i>	
A New Cryptanalytic Method Using the Distribution Characteristics of Substitution Distances	18
<i>Beomsik Song, Huaxiong Wang, and Jennifer Seberry</i>	
Truncated Differential Cryptanalysis of Camellia	32
<i>Seonhee Lee, Seokhie Hong, Sangjin Lee, Jongin Lim, and Seonhee Yoon</i>	
Improved Impossible Differential Cryptanalysis of Rijndael and Crypton ..	39
<i>Jung Hee Cheon, MunJu Kim, Kwangjo Kim, Jung-Yeun Lee, and SungWoo Kang</i>	
Cryptanalysis of Nonlinear Filter Generators with $\{0,1\}$ -Metric Viterbi Decoding	50
<i>Sabine Leveiller, Joseph Boutros, Philippe Guillot, and Gilles Zémor</i>	
An IND-CCA2 Public-Key Cryptosystem with Fast Decryption	51
<i>Johannes Buchmann, Kouichi Sakurai, and Tsuyoshi Takagi</i>	
Improvement of Probabilistic Public Key Cryptosystems Using Discrete Logarithm	72
<i>Dug-Hwan Choi, Seungbok Choi, and Dongho Won</i>	
Design and Analysis of Fast Provably Secure Public-Key Cryptosystems Based on a Modular Squaring	81
<i>Mototsugu Nishioka, Hisayoshi Satoh, and Kouichi Sakurai</i>	
Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation	103
<i>Jaechul Sung, Sangjin Lee, Jongin Lim, Wonil Lee, and Okyeon Yi</i>	
Decentralized Event Correlation for Intrusion Detection	114
<i>Christopher Krügel, Thomas Toth, and Clemens Kerer</i>	
Enhancing the Security of Cookies	132
<i>Vorapranee Khu-smith and Chris Mitchell</i>	
A New Stack Buffer Overflow Hacking Defense Technique with Memory Address Confirmation	146
<i>Yang-Seo Choi, Dong-il Seo, and Sung-Won Sohn</i>	

Efficient Revocation Schemes for Secure Multicast	160
<i>Hartono Kurnio, Rei Safavi-Naini, and Huaxiong Wang</i>	
Binary Codes for Collusion-Secure Fingerprinting	178
<i>G��rard Cohen, Simon Litsyn, and Gilles Z��mor</i>	
Copyright Protection of Object-Oriented Software	186
<i>Jarek Pastuszak, Darek Michalek, and Josef Pieprzyk</i>	
Off-Line Authentication Using Watermarks	200
<i>Hyejeoung Yoo, Kwangsoo Lee, Sangjin Lee, and Jongin Lim</i>	
Slide Attacks with a Known-Plaintext Cryptanalysis	214
<i>Soichi Furuya</i>	
Constructions of Cheating Immune Secret Sharing	226
<i>Josef Pieprzyk and Xian-Mo Zhang</i>	
Private Computation with Shared Randomness over Broadcast Channel	244
<i>Clemente Galdi and Pino Persiano</i>	
An Optimistic Multi-party Fair Exchange Protocol with Reduced Trust Requirements	258
<i>Nicol��s Gonz��lez-Deleito and Olivier Markowitch</i>	
Practical Reasoning about Accountability in Electronic Commerce Protocols	268
<i>Supakorn Kungpisdan and Yongyuth Permpoontanalarp</i>	
Content Extraction Signatures	285
<i>Ron Steinfeld, Laurence Bull, and Yuliang Zheng</i>	
New Signcryption Schemes Based on KCDSA	305
<i>Dae Hyun Yum and Pil Joong Lee</i>	
An Efficient and Provably Secure Threshold Blind Signature	318
<i>Jinho Kim, Kwangjo Kim, and Chulsoo Lee</i>	
A Multi-signature Scheme with Signers' Intentions Secure against Active Attacks	328
<i>Kei Kawauchi, Hiroshi Minato, Atsuko Miyaji, and Mitsuru Tada</i>	
A Distributed Light-Weight Authentication Model for Ad-hoc Networks	341
<i>Andr�� Weimerskirch and Gilles Thonet</i>	
Design of an Authentication Protocol for Gsm Javacards	355
<i>Stelvio Cimato</i>	
Secure Authorisation Agent for Cross-Domain Access Control in a Mobile Computing Environment	369
<i>Richard Au, Mark Looi, Paul Ashley, and Loo Tang Seet</i>	
Protecting General Flexible Itineraries of Mobile Agents	382
<i>Joan Mir and Joan Borrell</i>	

RSA Speedup with Residue Number System Immune against Hardware Fault Cryptanalysis	397
<i>Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sangjae Moon</i>	
A Countermeasure against One Physical Cryptanalysis May Benefit Another Attack	414
<i>Sung-Ming Yen, Seungjoo Kim, Seongan Lim, and Sangjae Moon</i>	
A Fast Scalar Multiplication Method with Randomized Projective Coordinates on a Montgomery-Form Elliptic Curve Secure against Side Channel Attacks	428
<i>Katsuyuki Okeya, Kunihiko Miyazaki, and Kouichi Sakurai</i>	
DPA Countermeasure Based on the “Masking Method”	440
<i>Kouichi Itoh, Masahiko Takenaka, and Naoya Torii</i>	
Author Index	457



<http://www.springer.com/978-3-540-43319-4>

Information Security and Cryptology - ICISC 2001
4th International Conference Seoul, Korea, December
6-7, 2001 Proceedings
Kim, K. (Ed.)
2002, XIII, 460 p., Softcover
ISBN: 978-3-540-43319-4