

Table of Contents

Broadcast Encryption and Traitor Tracing

Multi-service Oriented Broadcast Encryption	1
<i>Shaoquan Jiang, Guang Gong</i>	
Secure and Insecure Modifications of the Subset Difference Broadcast Encryption Scheme	12
<i>Tomoyuki Asano</i>	
Linear Code Implies Public-Key Traitor Tracing With <i>Revocation</i>	24
<i>Vu Dong Tô, Reihaneh Safavi-Naini</i>	
TTS Without Revocation Capability Secure Against CCA2	36
<i>Chong Hee Kim, Yong Ho Hwang, Pil Joong Lee</i>	

Private Information Retrieval and Oblivious Transfer

Single Database Private Information Retrieval With Logarithmic Communication	50
<i>Yan-Cheng Chang</i>	
Information Theoretically Secure Oblivious Polynomial Evaluation: Model, Bounds, and Constructions	62
<i>Goichiro Hanaoka, Hideki Imai, Joern Mueller-Quade, Anderson C.A. Nascimento, Akira Otsuka, Andreas Winter</i>	

Trust and Secret Sharing

Optimistic Fair Exchange Based on Publicly Verifiable Secret Sharing	74
<i>Gildas Avoine, Serge Vaudenay</i>	
NGSCB: A Trusted Open System	86
<i>Marcus Peinado, Yuqun Chen, Paul England, John Manferdelli</i>	

Cryptanalysis (I)

The Biryukov-Demirci Attack on Reduced-Round Versions of IDEA and MESH Ciphers	98
<i>Jorge Nakahara, Jr., Bart Preneel, Joos Vandewalle</i>	

Differential-Linear Type Attacks on Reduced Rounds of SHACAL-2	110
<i>Yongsup Shin, Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee</i>	
The Related-Key Rectangle Attack – Application to SHACAL-1	123
<i>Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee, Dowon Hong</i>	
Related Key Differential Cryptanalysis of Full-Round SPECTR-H64 and CIKS-1	137
<i>Youngdai Ko, Changhoon Lee, Seokhie Hong, Sangjin Lee</i>	
The Security of Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders	149
<i>Michael J. Jacobson, Jr.</i>	

Cryptanalysis (II)

Analysis of a Conference Scheme Under Active and Passive Attacks	157
<i>Feng Bao</i>	
Cryptanalysis of Two Password-Authenticated Key Exchange Protocols	164
<i>Zhiguo Wan, Shuhong Wang</i>	
Analysis and Improvement of Micali's Fair Contract Signing Protocol	176
<i>Feng Bao, Guilin Wang, Jianying Zhou, Huafei Zhu</i>	

Digital Signatures (I)

Digital Signature Schemes With Domain Parameters	188
<i>Serge Vaudenay</i>	
Generic Construction of Certificateless Signature	200
<i>Dae Hyun Yum, Pil Joong Lee</i>	

Cryptosystems (I)

A Generalization of PGV-Hash Functions and Security Analysis in Black-Box Model	212
<i>Wonil Lee, Mridul Nandi, Palash Sarkar, Donghoon Chang, Sangjin Lee, Kouichi Sakurai</i>	
How to Re-use Round Function in Super-Pseudorandom Permutation	224
<i>Tetsu Iwata, Kaoru Kurosawa</i>	
How to Remove MAC from DHIES	236
<i>Kaoru Kurosawa, Toshihiko Matsuo</i>	

Symmetric Key Authentication Services Revisited	248
<i>Bruno Crispo, Bogdan C. Popescu, Andrew S. Tanenbaum</i>	

Fast Computation

Improvements to the Point Halving Algorithm	262
<i>Brian King, Ben Rubin</i>	

Theoretical Analysis of XL over Small Fields	277
<i>Bo-Yin Yang, Jiun-Ming Chen</i>	

A New Method for Securing Elliptic Scalar Multiplication Against Side-Channel Attacks	289
<i>Chae Hoon Lim</i>	

Mobile Agents Security

A Mobile Agent System Providing Offer Privacy	301
<i>Ming Yao, Matt Henricksen, Greg Maitland, Ernest Foo, Ed Dawson</i>	

Digital Signatures (II)

Identity-Based Strong Designated Verifier Signature Schemes	313
<i>Willy Susilo, Fangguo Zhang, Yi Mu</i>	

Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups	325
<i>Joseph K. Liu, Victor K. Wei, Duncan S. Wong</i>	

A Group Signature Scheme With Efficient Membership Revocation for Reasonable Groups	336
<i>Toru Nakanishi, Yuji Sugiyama</i>	

Convertible Nominative Signatures	348
<i>Zhenjie Huang, Yumin Wang</i>	

Protocols

Protocols With Security Proofs for Mobile Applications	358
<i>Yiu Shing Terry Tin, Harikrishna Vasanta, Colin Boyd, Juan Manuel González Nieto</i>	

Secure Bilinear Diffie-Hellman Bits	370
<i>Steven D. Galbraith, Herbie J. Hopkins, Igor E. Shparlinski</i>	

Weak Property of Malleability in NTRUSign	379
<i>SungJun Min, Go Yamamoto, Kwangjo Kim</i>	

Security Management

Information Security Risk Assessment, Aggregation, and Mitigation	391
<i>Arjen Lenstra, Tim Voss</i>	

Access Control and Authorisation

A Weighted Graph Approach to Authorization Delegation and Conflict Resolution	402
<i>Chun Ruan, Vijay Varadharajan</i>	

Authorization Mechanisms for Virtual Organizations in Distributed Computing Systems	414
<i>Xi-Bin Zhao, Kwok-Yan Lam, Siu-Leung Chung, Ming Gu, Jia-Guang Sun</i>	

Cryptosystems (II)

Unconditionally Secure Encryption Under Strong Attacks	427
<i>Luke McAven, Rei Safavi-Naini, Moti Yung</i>	

ManTiCore: Encryption With Joint Cipher-State Authentication	440
<i>Erik Anderson, Cheryl Beaver, Timothy Draelos, Richard Schroepel, Mark Torgerson</i>	

Cryptanalysis (III)

On Security of XTR Public Key Cryptosystems Against Side Channel Attacks	454
<i>Dong-Guk Han, Jongin Lim, Kouichi Sakurai</i>	

On the Exact Flexibility of the Flexible Countermeasure Against Side Channel Attacks	466
<i>Katsuyuki Okeya, Tsuyoshi Takagi, Camille Vuillaume</i>	

Fault Attacks on Signature Schemes	478
<i>Christophe Giraud, Erik W. Knudsen</i>	

Author Index	493
------------------------	-----

Information Security and Privacy

9th Australasian Conference, ACISP 2004, Sydney,
Australia, July 13-15, 2004, Proceedings

Wang, H.; Pieprzyk, J.; Varadharajan, V. (Eds.)

2004, XIV, 498 p., Softcover

ISBN: 978-3-540-22379-5