

Table of Contents

Privacy and Anonymity

Grouping Verifiable Content for Selective Disclosure	1
<i>Laurence Bull, David McG. Squire, Jan Newmarch, Yuliang Zheng</i>	
Evaluation of Anonymity of Practical Anonymous Communication Networks	13
<i>Shigeki Kitazawa, Masakazu Soshi, Atsuko Miyaji</i>	
An Anonymous Credential System and a Privacy-Aware PKI	27
<i>Pino Persiano, Ivan Visconti</i>	
Flaws in Some Robust Optimistic Mix-Nets	39
<i>Masayuki Abe, Hideki Imai</i>	

Invited Talk (I)

The Unsolvable Privacy Problem and Its Implications for Security Technologies	51
<i>Andrew Odlyzko</i>	

Elliptic Curves

The Security of Fixed versus Random Elliptic Curves in Cryptography ..	55
<i>Yvonne Hitchcock, Paul Montague, Gary Carter, Ed Dawson</i>	
Cryptanalysis of the Full Version Randomized Addition-Subtraction Chains	67
<i>Dong-Guk Han, Nam Su Chang, Seok Won Jung, Young-Ho Park, Chang Han Kim, Heuisu Ryu</i>	
Generic $GF(2^m)$ Arithmetic in Software and Its Application to ECC	79
<i>André Weimerskirch, Douglas Stebila, Sheueling Chang Shantz</i>	
An Addition Algorithm in Jacobian of C_{34} Curve	93
<i>Seigo Arita</i>	

Cryptanalysis (I)

Amplified Differential Power Cryptanalysis on Rijndael Implementations with Exponentially Fewer Power Traces	106
<i>Sung-Ming Yen</i>	

Differential Fault Analysis on AES Key Schedule and Some Countermeasures	118
<i>Chien-Ning Chen, Sung-Ming Yen</i>	
On the Pseudorandomness of KASUMI Type Permutations	130
<i>Tetsu Iwata, Tohru Yagi, Kaoru Kurosawa</i>	
Theoretical Analysis of χ^2 Attack on RC6	142
<i>Masahiko Takenaka, Takeshi Shimoyama, Takeshi Koshiba</i>	

Mobile and Network Security

A Typed Theory for Access Control and Information Flow Control in Mobile Systems	154
<i>Libin Wang, Kefei Chen</i>	
Provably Secure Mobile Key Exchange: Applying the Canetti-Krawczyk Approach	166
<i>Yiu Shing Terry Tin, Colin Boyd, Juan Manuel González Nieto</i>	
Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications	180
<i>Jabeom Gu, Sehyun Park, Ohyoung Song, Jaeil Lee, Jaehoon Nah, Sungwon Sohn</i>	
Practical Pay TV Schemes	192
<i>Arvind Narayanan, C. Pandu Rangan, Kwangjo Kim</i>	
Cooperative Routers against DoS Attacks	204
<i>Ha Yoon Song, Han-gyoo Kim</i>	
Detecting Distributed Denial of Service Attacks by Sharing Distributed Beliefs	214
<i>Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao</i>	
Malicious ICMP Tunneling: Defense against the Vulnerability.....	226
<i>Abhishek Singh, Ola Nordström, Chenghuai Lu, Andre L.M. dos Santos</i>	
On Fair E-cash Systems Based on Group Signature Schemes	237
<i>Sébastien Canard, Jacques Traoré</i>	

Invited Talk (II)

A Taxonomy of Single Sign-On Systems	249
<i>Andreas Pashalidis, Chris J. Mitchell</i>	

Cryptanalysis (II)

Key Recovery Attacks on the RMAC, TMAC, and IACBC	265
<i>Jaechul Sung, Deukjo Hong, Sangjin Lee</i>	
Key Recovery Attacks on NTRU without Ciphertext Validation Routine	274
<i>Daewan Han, Jin Hong, Jae Woo Han, Daesung Kwon</i>	
Permanent Fault Attack on the Parameters of RSA with CRT	285
<i>Sung-Ming Yen, SangJae Moon, JaeCheol Ha</i>	
Backdoor Attacks on Black-Box Ciphers Exploiting Low-Entropy Plaintexts	297
<i>Adam Young, Moti Yung</i>	

Signature

Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings	312
<i>Fangguo Zhang, Kwangjo Kim</i>	
Digital Signature Schemes with Restriction on Signing Capability	324
<i>Jung Yeon Hwang, Hyun-Jeong Kim, Dong Hoon Lee, JongIn Lim</i>	
On the Exact Security of Multi-signature Schemes Based on RSA	336
<i>Kei Kawauchi, Mitsuru Tada</i>	

Cryptosystems (I)

A Length-Flexible Threshold Cryptosystem with Applications	350
<i>Ivan Damgård, Mads Jurik</i>	
Separating Encryption and Key Issuance in Digital Rights Management Systems	365
<i>Goichiro Hanaoka, Kazuto Ogawa, Itsuro Murota, Go Ohtake, Keigo Majima, Kimiyuki Oyamada, Seiichi Gohshi, Seiichi Namba, Hideki Imai</i>	
An Efficient Revocation Scheme with Minimal Message Length for Stateless Receivers	377
<i>Yong Ho Hwang, Chong Hee Kim, Pil Joong Lee</i>	
Parallel Authentication and Public-Key Encryption	387
<i>Josef Pieprzyk, David Pointcheval</i>	

Invited Talk (III)

Is Cross-Platform Security Possible?	402
<i>Li Gong</i>	

Cryptosystems (II)

A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems	403
<i>Jason Reid, Ian Cheong, Matthew Henricksen, Jason Smith</i>	
Cryptanalysis of a New Cellular Automata Cryptosystem	416
<i>Feng Bao</i>	
A CCA2 Secure Key Encapsulation Scheme Based on 3rd Order Shift Registers	428
<i>Chik How Tan, Xun Yi, Chee Kheong Siew</i>	
Clock-Controlled Shrinking Generator of Feedback Shift Registers	443
<i>Ali Kanso</i>	

Key Management

EPA: An Efficient Password-Based Protocol for Authenticated Key Exchange	452
<i>Yong Ho Hwang, Dae Hyun Yum, Pil Joong Lee</i>	
Constructing General Dynamic Group Key Distribution Schemes with Decentralized User Join	464
<i>Vanesa Daza, Javier Herranz, Germán Sáez</i>	
Robust Software Tokens – Yet Another Method for Securing User’s Digital Identity	476
<i>Taekyoung Kwon</i>	

Theory and Hash Functions

Public-Key Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders	488
<i>Hwankoo Kim, SangJae Moon</i>	
New Constructions for Resilient and Highly Nonlinear Boolean Functions	498
<i>Khoongming Khoo, Guang Gong</i>	
On Parallel Hash Functions Based on Block-Cipher	510
<i>Toshihiko Matsuo, Kaoru Kurosawa</i>	
Square Hash with a Small Key Size	522
<i>Swee-Huay Heng, Kaoru Kurosawa</i>	

Author Index	533
--------------------	-----