

CONTENTS

Session 1: Theoretical Foundations of Security

<i>Minimizing the use of random oracles in authenticated encryption schemes</i>	<i>1</i>
Mihir Bellare and Phillip Rogaway	

<i>Zero-knowledge proofs of decision power: new protocols and optimal round-complexity</i>	<i>17</i>
Giovanni Di Crescenzo, Kouichi Sakurai and Moti Yung	

<i>Computational learning theoretic cryptanalysis of language theoretic cryptosystems</i>	<i>28</i>
Takeshi Koshihara	

<i>A language for specifying sequences of authorization transformations and its applications</i>	<i>39</i>
Yun Bai and Vijay Varadharajan	

Session 2: Secret Sharing

<i>On the decomposition constructions for perfect secret sharing schemes</i>	<i>50</i>
Hung-Min Sun and Bor-Liang Chen	

<i>Traceable visual cryptography</i>	<i>61</i>
Ingrid Biehl and Susanne Wetzal	

<i>Remarks on the multiple assignment secret sharing scheme</i>	<i>72</i>
Hossein Ghodosi, Josef Pieprzyk and Rei Safavi-Naini	

<i>Secret sharing in hierarchical groups</i>	<i>81</i>
Chris Charnes, Keith Martin, Josef Pieprzyk and Rei Safavi-Naini	

Session 3: Network Security

<i>Stateless connections</i>	<i>87</i>
Tuomas Aura and Pekka Nikander	

<i>Design of a security platform for CORBA based application</i>	<i>98</i>
Rakman Choi, Jungchan Na, Kwonil Lee, Eunmi Kim and Wooyong Han	

<i>Secure document management and distribution in an open network environment</i>	<i>109</i>
Antonio Liyo, Fabio Maino and Marco Mezzalama	

Session 4: Authentication and Identification

<i>A² - code = Affine resolvable + BIBD</i>	<i>118</i>
Satoshi Obana and Kaoru Kurosawa	

<i>Multisender authentication systems with unconditional security</i>	130
K. M. Martin and Rei Safavi-Naini	

<i>Proposal of user identification scheme using mouse</i>	144
Kenichi Hayashi, Eiji Okamoto and Masahiro Mambo	

Session 5: Boolean Functions and Stream Ciphers

<i>An effective genetic algorithm for finding highly nonlinear Boolean Functions</i>	149
William Millan, Andrew Clark and Ed Dawson	

<i>Duality of Boolean functions and its cryptographic significance</i>	159
Xiao-Mo Zhang, Yuliang Zheng and Hideki Imai	

<i>Construction of correlation immune Boolean functions</i>	170
Ed Dawson and Chuan-Kun Wu	

<i>An improved key stream generator based on the programmable cellular automata</i>	181
Miodrag J. Mihaljević	

Session 6: Security Evaluation

<i>A Trust policy framework</i>	192
Audun Jøsang	

<i>Critical analysis of security in voice hiding techniques</i>	203
Liwu Chang and Ira S. Moskowitz	

Session 7: Signatures

<i>Two efficient RSA multisignature schemes</i>	217
Sangjoon Park, Sangwoo Park, Kwangjo Kim and Dongho Won	

<i>Proxy signatures, Revisited</i>	223
Seungjoo Kim, Sangjoon Park and Dongho Won	

Session 8: Block Ciphers

<i>Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X NewDES, RC2, and TEA</i>	233
John Kelsey, Bruce Schneier and David Wagner	

<i>A multiplication-addition structure against differential attack</i>	247
Feng Zhu and Bao-An Guo	

<i>On strict estimation method of provable security against differential</i>	258
Yasuyoshi Kaneko, Shiho Moriai and Kazuo Ohta	

<i>Improved fast software implementation of block ciphers</i>	269
Takeshi Shimoyama, Seiichi Amada and Shiho Moriai	

<i>Security comments on the Hwang-Chen algebraic-code cryptosystem</i>	274
Mohssen M. Alabbadi	

Session 9: Public Key Systems I

<i>Efficient elliptic curve exponentiation</i>	282
Atsuko Miyaji, Takatoshi Ono and Henri Cohen	

<i>Efficient construction of secure hyperelliptic discrete logarithm problems</i>	292
Jinhui Chao, Nori Matsuda and Shigeo Tsujii	

Session 10: Cryptanalysis of Public Key Systems

<i>A new and optimal chosen-message attack on RSA-type cryptosystems</i>	302
Daniel Bleichenbacher, Marc Joye and Jean-Jacques Quisquater	

<i>On weak RSA-keys produced from Pretty Good Privacy</i>	314
Yasuyuki Sakai, Kouichi Sakurai and Iiokazu Ishizuka	

Session 11: Subliminal Channels

<i>Self-synchronized message randomization methods for subliminal channels</i>	325
Kazukuni Kobara and Hideki Imai	

<i>Hiding the Hidden: A software system for concealing ciphertext as innocuous text</i>	335
Mark Chapman and George Davida	

Session 12: Public Key Systems II

<i>Digital signature and public key cryptosystem in a prime order subgroup of Z_n^*</i>	346
Colin Boyd	

<i>Trapdoor one-way permutations and multivariate polynomials</i>	356
Jacques Patarin and Louis Goubin	

<i>Asymmetric cryptography with S-Boxes</i>	369
Jacques Patarin and Louis Goubin	

<i>On the powerline system</i>	381
Paul Camion and Hervé Chabanne	

Session 13: Key Recovery/ Fair Cryptosystem

<i>Making unfair a “fair” blind signature scheme</i>	386
Jacques Traoré	
<i>Enforcing traceability in software</i>	398
Colin Boyd	
<i>Publicly verifiable partial key escrow</i>	409
Wenbo Mao	

Session 14: Intellectual Property Protection

<i>A secure code for recipient watermarking against conspiracy attacks by all users</i>	414
Hajime Watanabe and Tadao Kasami	

Session 15: Protocols

<i>Protocols for issuing public-key certificates over the Internet</i>	424
James W. Gray, III and Kin Fai Epsilon IP	
<i>Distributed cryptographic function application protocols</i>	435
André Postma, Thijs Krol and Egbert Molenkamp	
<i>Fault tolerant anonymous channel</i>	440
Wakaha Ogata, Kaoru Kurosawa, Kazue Sako and Kazunori Takatani	
<i>An implementable scheme for secure delegation of computing and data</i>	445
Josep Domingo - Ferrer and Ricardo X. Sanchez del Castillo	

Session 16: Electronic Commerce

<i>Electronic commerce with secure intelligent trade agent</i>	452
Jaco van der Merwe and S. H. von Solms	
<i>Efficient scalable fair cash with off-line extortion prevention</i>	463
Holger Peterson and Guillaume Poupard	
<i>An anonymous and undeniable payment scheme</i>	478
Liquan Chen and Chris J. Mitchell	
<i>Author Index</i>	483