

Table of Contents

On the Security of a Williams Based Public Key Encryption Scheme	1
<i>Siguna Müller (Univ. of Klagenfurt, Austria)</i>	
Semantically Secure McEliece Public-Key Cryptosystems	
– Conversions for McEliece PKC –	19
<i>Kazukuni Kobara and Hideki Imai (Univ. of Tokyo, Japan)</i>	
IND-CCA Public Key Schemes Equivalent to Factoring $n = pq$	36
<i>Kaoru Kurosawa, Wakaha Ogata, Toshihiko Matsuo, and Shuichi Makishima, (Tokyo Inst. of Tech., Japan)</i>	
Identification, Signature and Signcryption	
Using High Order Residues Modulo an RSA Composite	48
<i>Yuliang Zheng (Monash Univ., Australia)</i>	
On the Security of Lenstra’s Variant of DSA without Long Inversions	64
<i>Arjen K. Lenstra (Citibank, USA) and Igor E. Shparlinski (Macquarie Univ., Australia)</i>	
Fast Irreducibility and Subgroup Membership Testing in XTR	73
<i>Arjen K. Lenstra (Citibank, USA) and Eric R. Verheul (PricewaterhouseCoopers, Netherlands)</i>	
A New Aspect for Security Notions: Secure Randomness in Public-Key Encryption Schemes	87
<i>Takeshi Koshihara (Fujitsu, Japan)</i>	
The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes	104
<i>Tatsuaki Okamoto (NTT, Japan) and David Pointcheval (ENS, France)</i>	
A Generalisation, a Simplification and Some Applications of Paillier’s Probabilistic Public-Key System	119
<i>Ivan Damgård and Mads Jurik (Univ. of Aarhus, Denmark)</i>	
Marking: A Privacy Protecting Approach Against Blackmailing	137
<i>Dennis Kügler and Holger Vogt (Darmstadt Univ. of Tech., Germany)</i>	
Cryptanalysis of Two Sparse Polynomial Based Public Key Cryptosystems	153
<i>Feng Bao, Robert H. Deng (Kent Ridge Digital Labs, Singapore), Willi Geiselmann (Univ. of Karlsruhe, Germany), Claus Schnorr (Frankfurt Univ., Germany), Rainer Steinwandt (Univ. of Karlsruhe, Germany), and Hongjun Wu (Kent Ridge Digital Labs, Singapore)</i>	
Cryptanalysis of PKP: A New Approach	165
<i>Éliane Jaulmes and Antoine Joux (DCSSI, France)</i>	

Cryptanalysis of a Digital Signature Scheme on ID-Based Key-Sharing Infrastructures	173
<i>Hongjun Wu, Feng Bao,</i> <i>and Robert H. Deng (Kent Ridge Digital Labs, Singapore)</i>	
Loopholes in Two Public Key Cryptosystems Using the Modular Group	180
<i>Rainer Steinwandt (Univ. of Karlsruhe, Germany)</i>	
Efficient Revocation in Group Signatures	190
<i>Emmanuel Bresson and Jacques Stern (ENS, France)</i>	
A Public-Key Traitor Tracing Scheme with Revocation Using Dynamic Shares	207
<i>Wen-Guey Tzeng</i> <i>and Zhi-Jia Tzeng (Nat. Chiao Tung Univ., Taiwan)</i>	
Efficient Asymmetric Self-Enforcement Scheme with Public Traceability	225
<i>Hiroataka Komaki, Yuji Watanabe, Goichiro Hanaoka,</i> <i>and Hideki Imai (Univ. of Tokyo, Japan)</i>	
Adaptive Security for the Additive-Sharing Based Proactive RSA	240
<i>Yair Frankel (Ecash Tech., USA),</i> <i>Philip D. MacKenzie (Bell Labs, USA),</i> <i>and Moti Yung (CertCo, USA)</i>	
Robust Forward-Secure Signature Schemes with Proactive Security	264
<i>Wen-Guey Tzeng</i> <i>and Zhi-Jia Tzeng (Nat. Chiao Tung Univ., Taiwan)</i>	
Equitability in Retroactive Data Confiscation versus Proactive Key Escrow	277
<i>Yvo Desmedt (Florida State Univ., USA),</i> <i>Mike Burmester (Royal Holloway Univ. of London, UK),</i> <i>and Jennifer Seberry (Univ. of Wollongong, Australia)</i>	
A PVSS as Hard as Discrete Log and Shareholder Separability	287
<i>Adam Young (Columbia Univ., USA) and Moti Yung (CertCo, USA)</i>	
One Round Threshold Discrete-Log Key Generation without Private Channels	300
<i>Pierre-Alain Fouque and Jacques Stern (ENS, France)</i>	
Remarks on Mix-Network Based on Permutation Networks	317
<i>Masayuki Abe and Fumitaka Hoshino (NTT, Japan)</i>	
New Key Recovery in WAKE Protocol	325
<i>Chong Hee Kim and Pil Joong Lee (POSTECH, Korea)</i>	
Redundant Representation of Finite Fields	339
<i>Willi Geiselmann</i> <i>and Harald Lukhaub (Univ. of Karlsruhe, Germany)</i>	

Compact Encoding of Non-adjacent Forms with Applications to Elliptic Curve Cryptography	353
<i>Marc Joye and Christophe Tymen (Gemplus, France)</i>	
Efficient Implementation of Elliptic Curve Cryptosystems on the TI MSP430x33x Family of Microcontrollers	365
<i>Jorge Guajardo (WPI, USA), Rainer Blümel, Uwe Krieger (Cryptovision, Germany), and Christof Paar (WPI, USA)</i>	
Secure Server-Aided Signature Generation	383
<i>Markus Jakobsson and Susanne Wetzel (Bell Labs, USA)</i>	
Efficient Long-Term Validation of Digital Signatures	402
<i>Arne Ansper, Ahto Buldas, Meelis Roos, and Jan Willemsen (Cybernetica, Estonia)</i>	
A Novel Systolic Architecture for an Efficient RSA Implementation	416
<i>Nikos K. Moshopoulos and K. Z. Pekmestzi (Nat. Tech. Univ. of Athens, Greece)</i>	
Author Index	423