

# Contents

A Practical and Secure Fault-Tolerant Conference-Key Agreement Protocol .....	1
<i>Wen-Guey Tzeng (Nat Chiao Tung Uni, Taiwan)</i>	
An Efficient NICE-Schnorr-Type Signature Scheme .....	14
<i>Detlef Hühnlein, and Johannes Merkle (secunet, Germany)</i>	
Identification of Bad Signatures in Batches .....	28
<i>Jarostaw Pastuszak, Dariusz Michatek (Polish Acad of Sci, Poland), Josef Pieprzyk, and Jennifer Seberry (Uni of Wollongong, Australia)</i>	
Some Remarks on a Fair Exchange Protocol .....	46
<i>Jianying Zhou, Robert Deng, and Feng Bao (Kent Ridge Digital Labs, Singapore)</i>	
Gaudry's Variant against $C_{ab}$ Curves .....	58
<i>Seigo Arita (NEC, Japan)</i>	
An Identification Scheme Based on Sparse Polynomials .....	68
<i>William D. Banks, Daniel Lieman (Uni of Missouri, USA), and Igor E. Shparlinski (Macquarie Uni, Australia)</i>	
A State-Based Model for Certificate Management Systems .....	75
<i>Chuchang Liu, Maris A. Ozols, Marie Henderson, and Tony Cant (DSTO, Australia)</i>	
Confidence Valuation in a Public-Key Infrastructure Based on Uncertain Evidence .....	93
<i>Reto Kohlas, and Ueli Maurer (ETH, Switzerland)</i>	
The Composite Discrete Logarithm and Secure Authentication .....	113
<i>David Pointcheval (ENS, France)</i>	
Chosen-Ciphertext Security for Any One-Way Cryptosystem .....	129
<i>David Pointcheval (ENS, France)</i>	
Short Proofs of Knowledge for Factoring .....	147
<i>Guillaume Poupard, and Jacques Stern (ENS, France)</i>	
Secure and Practical Tree-Structure Signature Schemes Based on Discrete Logarithms .....	167
<i>X.Y.Wang (Uni of Hong Kong, and Shandong Uni, China), L.C.Hui, K.P.Chow, W.W.Tsang, C.F.Chong, and H.W.Chan (Uni of Hong Kong, China)</i>	

All-or-Nothing Transform and Remotely Keyed Encryption Protocols ..... 178  
*Sang Uk Shin, Weon Shin, and Kyung Hyune Rhee (PuKyong Nat Uni, Korea)*

Security of Public Key Certificate Based Authentication Protocols ..... 196  
*Wu Wen, Takamichi Saito, and Fumio Mizoguchi (Sci Uni of Tokyo, Japan)*

Efficient Implementation of Schoof’s Algorithm  
in Case of Characteristic 2 ..... 210  
*Tetsuya Izu, Jun Kogure, and Kazuhiro Yokoyama (Fujitsu Labs, Japan)*

Key Recovery in Third Generation Wireless Communication Systems ..... 223  
*Juanma González Nieto (QUT, Australia), DongGook Park (QUT, Australia, and Korea Telecom), Colin Boyd, and Ed Dawson (QUT, Australia)*

Elliptic Curves with the Montgomery-Form  
and Their Cryptographic Applications ..... 238  
*Katsuyuki Okeya, Hiroyuki Kurumatani (Hitachi, Japan), and Kouichi Sakurai (Kyushu Uni, Japan)*

Certificates of Recoverability with Scalable Recovery Agent Security ..... 258  
*Eric R. Verheul (PricewaterhouseCoopers, The Netherlands)*

Design Validations for Discrete Logarithm Based Signature Schemes ..... 276  
*Ernest Brickell (Intel, USA), David Pointcheval (ENS, France), Serge Vaudenay (EPFL, Switzerland), and Moti Yung (Certco, USA)*

Optimally Efficient Accountable Time-Stamping ..... 293  
*Ahto Buldas, Helger Lipmaa (Küberneetika AS, Estonia), and Berry Schoenmakers (Eindhoven Uni of Tech, The Netherlands)*

“Pseudorandom Intermixing”: A Tool for Shared Cryptography ..... 306  
*Yair Frankel (CertCo, USA), Philip MacKenzie (Bell Labs, USA), and Moti Yung (CertCo, USA)*

RSA-Based Auto-recoverable Cryptosystems ..... 326  
*Adam Young (Columbia Uni, USA), and Moti Yung (CertCo, USA)*

Efficient and Fresh Certification ..... 342  
*Irene Gassko (Bell Labs, USA), Peter S. Gemmell (Uni of New Mexico, USA), and Philip MacKenzie (Bell Labs, USA)*

Efficient Zero-Knowledge Proofs of Knowledge Without Intractability Assumptions .....	354
<i>Ronald Cramer (ETH, Switzerland), Ivan Damgård (Aarhus Uni, Denmark), and Philip MacKenzie (Bell Labs, USA)</i>	
Cryptographic Approaches to Privacy in Forensic DNA Databases .....	373
<i>Philip Bohannon, Markus Jakobsson (Bell Labs, USA), and Sukamol Srikwan (Chulalongkorn Uni, Thailand)</i>	
Making Hash Functions from Block Ciphers Secure and Efficient by Using Convolutional Codes .....	391
<i>Toru Inoue (AMSL, Japan), and Kouichi Sakurai (Kyushu Uni, Japan)</i>	
Fast Implementation of Elliptic Curve Arithmetic in $\text{GF}(p^n)$ .....	405
<i>Chae Hoon Lim, and Hyo Sun Hwang (Future Systems, Korea)</i>	
An Auction Protocol Which Hides Bids of Losers .....	422
<i>Kazue Sako (NEC, Japan)</i>	
Forward Secrecy and Its Application to Future Mobile Communications Security .....	433
<i>DongGook Park (QUT, Australia, and Korea Telecom), Colin Boyd (QUT, Australia), and Sang-Jae Moon (Kyungpook Nat Uni, Korea)</i>	
Selecting Cryptographic Key Sizes .....	446
<i>Arjen K. Lenstra (Citibank, USA), and Eric R. Verheul (PricewaterhouseCoopers, The Netherlands)</i>	
A Structured ElGamal-Type Multisignature Scheme .....	466
<i>Mike Burmester (Royal Holloway, Uni of London, UK), Yvo Desmedt (Florida State Uni, USA), Hiroshi Doi (Okayama Uni, Japan), Masahiro Mambo (Tohoku Uni, Japan), Eiji Okamoto (Uni of Wisconsin, Milwaukee, USA), Mitsuru Tada, and Yuko Yoshifuji (JAIST, Japan)</i>	
<b>Author Index .....</b>	<b>485</b>