

# Table of Contents

## Encryption Schemes

New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive <i>Kouichi Sakurai (Kyushu University, Japan), Tsuyoshi Takagi (Technische Universität Darmstadt, Germany)</i>	1
Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages <i>Jean-Sébastien Coron (Gemplus, France), Helena Handschuh (Gemplus, France), Marc Joye (Gemplus, France), Pascal Paillier (Gemplus, France), David Pointcheval (École Normale Supérieure, France), Christophe Tymen (Gemplus, France)</i>	17
On Sufficient Randomness for Secure Public-Key Cryptosystems <i>Takeshi Koshihara (Fujitsu Laboratories Ltd, Japan)</i>	34
Multi-recipient Public-Key Encryption with Shortened Ciphertext <i>Kaoru Kurosawa (Ibaraki University, Japan)</i>	48

## Signature Schemes

Efficient and Unconditionally Secure Digital Signatures and a Security Analysis of a Multireceiver Authentication Code <i>Goichiro Hanaoka (University of Tokyo, Japan), Junji Shikata (University of Tokyo, Japan), Yuliang Zheng (UNC Charlotte, USA), Hideki Imai (University of Tokyo, Japan)</i>	64
Formal Proofs for the Security of Signcryption <i>Joonsang Baek (Monash University, Australia), Ron Steinfield (Monash University, Australia), Yuliang Zheng (UNC Charlotte, USA)</i>	80
A Provably Secure Restrictive Partially Blind Signature Scheme <i>Greg Maitland (Queensland University of Technology, Australia), Colin Boyd (Queensland University of Technology, Australia)</i>	99

## Protocols I

$M + 1$ -st Price Auction Using Homomorphic Encryption <i>Masayuki Abe (NTT ISP Labs, Japan), Koutarou Suzuki (NTT ISP Labs, Japan)</i>	115
Client/Server Tradeoffs for Online Elections <i>Ivan Damgård (Aarhus University, Denmark), Mads Jurik (Aarhus University, Denmark)</i>	125

Self-tallying Elections and Perfect Ballot Secrecy . . . . . 141  
*Aggelos Kiayias (Graduate Center, CUNY, USA), Moti Yung (CertCo, USA)*

**Protocols II**

Efficient 1-Out-n Oblivious Transfer Schemes . . . . . 159  
*Wen-Guey Tzeng (National Chiao Tung University, Taiwan)*

Linear Code Implies Public-Key Traitor Tracing . . . . . 172  
*Kaoru Kurosawa (Ibaraki University, Japan), Takuya Yoshida (Tokyo Institute of Technology, Japan)*

Design and Security Analysis  
of Anonymous Group Identification Protocols . . . . . 188  
*Chan H. Lee (City University of Hong Kong, China), Xiaotie Deng (City University of Hong Kong, China), Huafei Zhu (Zhejiang University, China)*

On the Security of the Threshold Scheme  
Based on the Chinese Remainder Theorem . . . . . 199  
*Michaël Quisquater (Katholieke Universiteit Leuven, Belgium), Bart Preneel (Katholieke Universiteit Leuven, Belgium), Joos Vandewalle (Katholieke Universiteit Leuven, Belgium)*

**Cryptanalysis**

Solving Underdefined Systems of Multivariate Quadratic Equations . . . . . 211  
*Nicolas Courtois (SchlumbergerSema, France), Louis Goubin (SchlumbergerSema, France), Willi Meier (FH Aargau, Switzerland), Jean-Daniel Tacier (FH Aargau, Switzerland)*

Selective Forgery of RSA Signatures with Fixed-Pattern Padding . . . . . 228  
*Arjen K. Lenstra (Citibank, USA, and Tech. Univ. Eindhoven, The Netherlands), Igor E. Shparlinski (Macquarie University, Australia)*

New Chosen-Plaintext Attacks on the One-Wayness  
of the Modified McEliece PKC Proposed at Asiacrypt 2000 . . . . . 237  
*Kazukuni Kobara (University of Tokyo, Japan), Hideki Imai (University of Tokyo, Japan)*

**Side Channels**

SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation . . 252  
*Roman Novak (Jozef Stefan Institute, Slovenia)*

A Combined Timing and Power Attack . . . . . 263  
*Werner Schindler (BSI, Germany)*

A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks .....	280
<i>Tetsuya Izu (Fujitsu Labs Ltd, Japan), Tsuyoshi Takagi (Technische Universität Darmstadt, Germany)</i>	

## Invited Talk

New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report .....	297
<i>Bart Preneel (Katholieke Universiteit Leuven, Belgium)</i>	

## ECC Implementations

An Improved Method of Multiplication on Certain Elliptic Curves .....	310
<i>Young-Ho Park (CIST, Korea University, Korea), Sangho Oh (CIST, Korea University., Korea), Sangjin Lee (CIST, Korea University, Korea), Jongin Lim (CIST, Korea University, Korea), Maenghee Sung (KISA, Korea)</i>	
An Alternate Decomposition of an Integer for Faster Point Multiplication on Certain Elliptic Curves .....	323
<i>Young-Ho Park (CIST, Korea University, Korea), Sangtae Jeong (Seoul National University, Korea), Chang Han Kim (CAMIS, Semyung University, Korea), Jongin Lim (CIST, Korea University, Korea)</i>	
Weierstraß Elliptic Curves and Side-Channel Attacks .....	335
<i>Éric Brier (Gemplus, France), Marc Joye (Gemplus, France)</i>	

## Applications

One-Way Cross-Trees and Their Applications .....	346
<i>Marc Joye (Gemplus, France), Sung-Ming Yen (National Central University, Taiwan)</i>	
RSA Key Generation with Verifiable Randomness .....	357
<i>Ari Juels (RSA Laboratories, USA), Jorge Guajardo (Ruhr-Universität Bochum, Germany)</i>	
New Minimal Modified Radix- $r$ Representation with Applications to Smart Cards .....	375
<i>Marc Joye (Gemplus, France), Sung-Ming Yen (National Central University, Taiwan)</i>	
<b>Author Index</b> .....	385



<http://www.springer.com/978-3-540-43168-8>

Public Key Cryptography

5th International Workshop on Practice and Theory in

Public Key Cryptosystems, PKC 2002, Paris, France,

February 12-14, 2002 Proceedings

Paillier, P.; Naccache, D. (Eds.)

2002, XI, 384 p. 1 illus., Softcover

ISBN: 978-3-540-43168-8