

Table of Contents

Encryption Schemes

New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive	1
<i>Kouichi Sakurai (Kyushu University, Japan), Tsuyoshi Takagi (Technische Universität Darmstadt, Germany)</i>	
Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages	17
<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 Tychen (Gemplus, France)</i>	
On Sufficient Randomness for Secure Public-Key Cryptosystems	34
<i>Takeshi Koshihara (Fujitsu Laboratories Ltd, Japan)</i>	
Multi-recipient Public-Key Encryption with Shortened Ciphertext	48
<i>Kaoru Kurosawa (Ibaraki University, Japan)</i>	

Signature Schemes

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

Protocols I

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

Self-tallying Elections and Perfect Ballot Secrecy	141
<i>Aggelos Kiayias (Graduate Center, CUNY, USA), Moti Yung (CertCo, USA)</i>	

Protocols II

Efficient 1-Out-n Oblivious Transfer Schemes	159
<i>Wen-Guey Tzeng (National Chiao Tung University, Taiwan)</i>	
Linear Code Implies Public-Key Traitor Tracing	172
<i>Kaoru Kurosawa (Ibaraki University, Japan), Takuya Yoshida (Tokyo Institute of Technology, Japan)</i>	
Design and Security Analysis of Anonymous Group Identification Protocols	188
<i>Chan H. Lee (City University of Hong Kong, China), Xiaotie Deng (City University of Hong Kong, China), Huafei Zhu (Zhejiang University, China)</i>	
On the Security of the Threshold Scheme Based on the Chinese Remainder Theorem	199
<i>Michaël Quisquater (Katholieke Universiteit Leuven, Belgium), Bart Preneel (Katholieke Universiteit Leuven, Belgium), Joos Vandewalle (Katholieke Universiteit Leuven, Belgium)</i>	

Cryptanalysis

Solving Underdefined Systems of Multivariate Quadratic Equations	211
<i>Nicolas Courtois (SchlumbergerSema, France), Louis Goubin (SchlumbergerSema, France), Willi Meier (FH Aargau, Switzerland), Jean-Daniel Tacier (FH Aargau, Switzerland)</i>	
Selective Forgery of RSA Signatures with Fixed-Pattern Padding	228
<i>Arjen K. Lenstra (Citibank, USA, and Tech. Univ. Eindhoven, The Netherlands), Igor E. Shparlinski (Macquarie University, Australia)</i>	
New Chosen-Plaintext Attacks on the One-Wayness of the Modified McEliece PKC Proposed at Asiacrypt 2000	237
<i>Kazukuni Kobara (University of Tokyo, Japan), Hideki Imai (University of Tokyo, Japan)</i>	

Side Channels

SPA-Based Adaptive Chosen-Ciphertext Attack on RSA Implementation ..	252
<i>Roman Novak (Jozef Stefan Institute, Slovenia)</i>	
A Combined Timing and Power Attack	263
<i>Werner Schindler (BSI, Germany)</i>	

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>	
Author Index	385

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