Table of Contents

Encryption Schemes

New Semantically Secure Public-Key Cryptosystems from the RSA-Primitive 1
Kouichi Sakurai (Kyushu University, Japan), Tsuyoshi Takagi (Technische Universität Darmstadt, Germany)

Optimal Chosen-Ciphertext Secure Encryption of Arbitrary-Length Messages 17
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)

On Sufficient Randomness for Secure Public-Key Cryptosystems 34
Takeshi Koshiba (Fujitsu Laboratories Ltd, Japan)

Multi-recipient Public-Key Encryption with Shortened Ciphertext 48
Kaoru Kurosawa (Ibaraki University, Japan)

Signature Schemes

Efficient and Unconditionally Secure Digital Signatures and a Security Analysis of a Multireceiver Authentication Code 64
Goichiro Hanaoka (University of Tokyo, Japan), Junji Shikata (University of Tokyo, Japan), Yuliang Zheng (UNC Charlotte, USA), Hideki Imai (University of Tokyo, Japan)

Formal Proofs for the Security of Signcryption 80
Joonsang Baek (Monash University, Australia), Ron Steinfeld (Monash University, Australia), Yuliang Zheng (UNC Charlotte, USA)

A Provably Secure Restrictive Partially Blind Signature Scheme 99
Greg Maitland (Queensland University of Technology, Australia), Colin Boyd (Queensland University of Technology, Australia)

Protocols I

$M+1$-st Price Auction Using Homomorphic Encryption 115
Masayuki Abe (NTT ISP Labs, Japan), Koutarou Suzuki (NTT ISP Labs, Japan)

Client/Server Tradeoffs for Online Elections 125
Ivan Damgård (Aarhus University, Denmark), Mads Jurik (Aarhus University, Denmark)

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
Tetsuya Izu (Fujitsu Labs Ltd, Japan), Tsuyoshi Takagi (Technische Universität Darmstadt, Germany)

Invited Talk

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

ECC Implementations

An Improved Method of Multiplication on Certain Elliptic Curves 310
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)

An Alternate Decomposition of an Integer for Faster Point Multiplication
on Certain Elliptic Curves 323
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)

Weierstraß Elliptic Curves and Side-Channel Attacks 335
Éric Brier (Gemplus, France), Marc Joye (Gemplus, France)

Applications

One-Way Cross-Trees and Their Applications 346
Marc Joye (Gemplus, France), Sung-Ming Yen (National Central University, Taiwan)

RSA Key Generation with Verifiable Randomness 357
Ari Juels (RSA Laboratories, USA), Jorge Guajardo (Ruhr-Universität Bochum, Germany)

New Minimal Modified Radix-r Representation
with Applications to Smart Cards 375
Marc Joye (Gemplus, France), Sung-Ming Yen (National Central University, Taiwan)

Author Index 385