Contents

A New Type of “Magic Ink” Signatures — Towards Transcript-Irrelevant Anonymity Revocation .......................... 1
Feng Bao and Robert H. Deng (Kent Ridge Digital Labs, Singapore)

A New Aspect of Dual Basis for Efficient Field Arithmetic ................ 12
Chang-Hyi Lee (SAIT, Korea)
Jong-In Lim (Korea Uni)

On the Security of Random Sources ........................................ 29
Jean-Sébastien Coron (ENS and Gemplus, France)

Anonymous Fingerprinting Based on Committed Oblivious Transfer ...................................................... 43
Josep Domingo-Ferrer (Uni Rovira i Virgili, Spain)

How to Enhance the Security of Public-Key Encryption at Minimum Cost ............................................. 53
Eiichiro Fujisaki and Tatsuaki Okamoto (NTT, Japan)

Encrypted Message Authentication by Firewalls ................................................ 69
Chandana Gamage, Jussipekka Leiwo and Yuliang Zheng (Monash Uni, Australia)

A Relationship between One-Wayness and Correlation Intractability ..................................................... 82
Satoshi Hada and Toshiaki Tanaka (KDD, Japan)

Message Recovery Fair Blind Signature ................................................. 97
Hyung-Woo Lee and Tai-Yun Kim (Korea Uni)

On Quorum Controlled Asymmetric Proxy Re-encryption ......................... 112
Markus Jakobsson (Bell Labs, USA)

Mini-Cash: A Minimalistic Approach to E-Commerce .......................... 122
Markus Jakobsson (Bell Labs, USA)

Preserving Privacy in Distributed Delegation with Fast Certificates .................. 136
Pekka Nikander (Ericsson, Finland)
Yki Kortesniemi and Jonna Partanen (Helsinki Uni of Tech, Finland)

Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol ........ 154
Simon Blake-Wilson (Certicom, Canada)
Alfred Menezes (Uni of Waterloo, Canada)
Toward Fair International Key Escrow – An Attempt by Distributed Trusted Third Agencies with Threshold Cryptography – 171
Shingo Miyazaki (Kyushu Univ, Japan)
Ikuko Kuroda (NTT, Japan)
Kouichi Sakurai (Kyushu Univ, Japan)

How to Copyright a Function? 188
David Naccache (Gemplus, France)
Adi Shamir (Weizmann Inst of Sci, Israel)
Julien P. Stern (UCL, Belgium, and Uni de Paris-Sud, France)

On the Security of RSA Screening 197
Jean-Sébastien Coron (ENS and Gemplus, France)
David Naccache (Gemplus, France)

The Effectiveness of Lattice Attacks Against Low-Exponent RSA 204
Christophe Couplé (ENS de Lyon, France)
Phong Nguyen and Jacques Stern (ENS Paris, France)

A Trapdoor Permutation Equivalent to Factoring 219
Pascal Paillier (Gemplus and ENST, France)

Low-Cost Double-Size Modular Exponentiation
or How to Stretch Your Cryptoprocessor 223
Pascal Paillier (Gemplus and ENST, France)

Evaluating Differential Fault Analysis of Unknown Cryptosystems 235
Pascal Paillier (Gemplus and ENST, France)

Removing Interoperability Barriers Between the X.509 and
EDIFACT Public Key Infrastructures: The DEDICA Project 245
Montse Rubia, Juan Carlos Cruellas and
Manel Medina (Polytech Uni of Catalonia, Spain)

Hash Functions and the MAC Using All-or-Nothing Property 263
Sang Uk Shin and Kyung Hyune Rhee (PuKyong Nat Uni, Korea)
Jae Woo Yoon (ETRI, Korea)

Decision Oracles are Equivalent to Matching Oracles 276
Helena Handschuh (Gemplus and ENST, France)
Yiannis Tsiounis (GTE Labs, USA)
Moti Yung (CertCo, USA)

Shared Generation of Random Number with Timestamp:
How to Cope with the Leakage of the CA’s Secret 290
Yuji Watanabe and Hideki Imai (Univ of Tokyo, Japan)
Auto-Recoverable Cryptosystems with Faster Initialization
and the Escrow Hierarchy .................................................... 306
Adam Young (Columbia Uni, USA)
Moti Yung (CertCo, USA)

A Secure Pay-per-View Scheme for Web-Based Video Service .......... 315
Jianying Zhou (Kent Ridge Digital Labs, Singapore)
Kwok-Yan Lam (Nat Uni of Singapore)

Author Index ................................................................. 327
Public Key Cryptography
Imai, H.; Zheng, Y. (Eds.)
1999, X, 334 p., Softcover
ISBN: 978-3-540-65644-9