

Contents

A New Type of “Magic Ink” Signatures — Towards Transcript-Irrelevant Anonymity Revocation	1
<i>Feng Bao and Robert H. Deng (Kent Ridge Digital Labs, Singapore)</i>	
A New Aspect of Dual Basis for Efficient Field Arithmetic	12
<i>Chang-Hyi Lee (SAIT, Korea)</i> <i>Jong-In Lim (Korea Uni)</i>	
On the Security of Random Sources	29
<i>Jean-Sébastien Coron (ENS and Gemplus, France)</i>	
Anonymous Fingerprinting Based on Committed Oblivious Transfer	43
<i>Josep Domingo-Ferrer (Uni Rovira i Virgili, Spain)</i>	
How to Enhance the Security of Public-Key Encryption at Minimum Cost	53
<i>Eiichiro Fujisaki and Tatsuaki Okamoto (NTT, Japan)</i>	
Encrypted Message Authentication by Firewalls	69
<i>Chandana Gamage, Jussipekka Leiwo and Yuliang Zheng (Monash Uni, Australia)</i>	
A Relationship between One-Wayness and Correlation Intractability	82
<i>Satoshi Hada and Toshiaki Tanaka (KDD, Japan)</i>	
Message Recovery Fair Blind Signature	97
<i>Hyung-Woo Lee and Tai-Yun Kim (Korea Uni)</i>	
On Quorum Controlled Asymmetric Proxy Re-encryption	112
<i>Markus Jakobsson (Bell Labs, USA)</i>	
Mini-Cash: A Minimalistic Approach to E-Commerce	122
<i>Markus Jakobsson (Bell Labs, USA)</i>	
Preserving Privacy in Distributed Delegation with Fast Certificates	136
<i>Pekka Nikander (Ericsson, Finland)</i> <i>Yki Kortesniemi and Jonna Partanen (Helsinki Uni of Tech, Finland)</i>	
Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol	154
<i>Simon Blake-Wilson (Certicom, Canada)</i> <i>Alfred Menezes (Uni of Waterloo, Canada)</i>	

Toward Fair International Key Escrow – An Attempt by Distributed Trusted Third Agencies with Threshold Cryptography –	171
<i>Shingo Miyazaki (Kyushu Univ, Japan)</i>	
<i>Ikuko Kuroda (NTT, Japan)</i>	
<i>Kouichi Sakurai (Kyushu Univ, Japan)</i>	
How to Copyright a Function ?	188
<i>David Naccache (Gemplus, France)</i>	
<i>Adi Shamir (Weizmann Inst of Sci, Israel)</i>	
<i>Julien P. Stern (UCL, Belgium, and Uni de Paris-Sud, France)</i>	
On the Security of RSA Screening	197
<i>Jean-Sébastien Coron (ENS and Gemplus, France)</i>	
<i>David Naccache (Gemplus, France)</i>	
The Effectiveness of Lattice Attacks Against Low-Exponent RSA	204
<i>Christophe Coupé (ENS de Lyon, France)</i>	
<i>Phong Nguyen and Jacques Stern (ENS Paris, France)</i>	
A Trapdoor Permutation Equivalent to Factoring	219
<i>Pascal Paillier (Gemplus and ENST, France)</i>	
Low-Cost Double-Size Modular Exponentiation or How to Stretch Your Cryptoprocessor	223
<i>Pascal Paillier (Gemplus and ENST, France)</i>	
Evaluating Differential Fault Analysis of Unknown Cryptosystems	235
<i>Pascal Paillier (Gemplus and ENST, France)</i>	
Removing Interoperability Barriers Between the X.509 and EDIFACT Public Key Infrastructures: The DEDICA Project	245
<i>Montse Rubia, Juan Carlos Cruellas and</i>	
<i>Manel Medina (Polytech Uni of Catalonia, Spain)</i>	
Hash Functions and the MAC Using All-or-Nothing Property	263
<i>Sang Uk Shin and Kyung Hyune Rhee (PuKyong Nat Uni, Korea)</i>	
<i>Jae Woo Yoon (ETRI, Korea)</i>	
Decision Oracles are Equivalent to Matching Oracles	276
<i>Helena Handschuh (Gemplus and ENST, France)</i>	
<i>Yiannis Tsiounis (GTE Labs, USA)</i>	
<i>Moti Yung (CertCo, USA)</i>	
Shared Generation of Random Number with Timestamp: How to Cope with the Leakage of the CA's Secret	290
<i>Yuji Watanabe and Hideki Imai (Uni of Tokyo, Japan)</i>	

Auto-Recoverable Cryptosystems with Faster Initialization and the Escrow Hierarchy	306
<i>Adam Young (Columbia Uni, USA)</i>	
<i>Moti Yung (CertCo, USA)</i>	
A Secure Pay-per-View Scheme for Web-Based Video Service	315
<i>Jianying Zhou (Kent Ridge Digital Labs, Singapore)</i>	
<i>Kwok-Yan Lam (Nat Uni of Singapore)</i>	
Author Index	327

Public Key Cryptography

Second International Workshop on Practice and Theory

in Public Key Cryptography, PKC'99, Kamakura, Japan,

March 1-3, 1999, Proceedings

Imai, H.; Zheng, Y. (Eds.)

1999, X, 334 p., Softcover

ISBN: 978-3-540-65644-9