Contents

Invited Talks

Distributed public key cryptosystems 1
Yair Frankel and Moti Yung (CertCo, USA)

How (not) to design RSA signature schemes 14
Jean-François Misarsky (France Telecom)

Overview of elliptic curve cryptography 29
Kiyomichi Araki (Tokyo Inst of Tech, Japan),
Takakazu Satoh (Saitama Uni, Japan) and
Shinji Miura (Sony, Japan)

Special Talk

Lattices and cryptography: An overview 50
Jacques Stern (ENS, France)

Regular Contributions

A signcryption scheme with signature directly verifiable by public key 55
Feng Bao and Robert H. Deng (Nat Uni of Singapore)

Guaranteed correct sharing of integer factorization with off-line shareholders 60
Wenbo Mao (HP Labs Bristol, UK)

Lower bounds on term-based divisible cash systems 72
Tatsuaki Okamoto (NTT, Japan) and Moti Yung (CertCo, USA)

Certifying trust 83
Ilari Lehti and Pekka Nikander (Helsinki Uni of Tech, Finland)

On the security of server-aided RSA protocols 99
Johannes Merkle and Ralph Werchner (Uni of Frankfurt, Germany)

On the security of ElGamal-based encryption 117
Yiannis Tsiounis (GTE Labs, USA) and
Moti Yung (CertCo, USA)

An authenticated Diffie-Hellman key agreement protocol
secure against active attacks 135
Shouichi Hirose and Susumu Yoshida (Kyoto Uni, Japan)

On the security of Girault's identification scheme 149
Shahrokh Saeednia (Uni Libre de Bruxelles, Belgium) and
Rei Safavi-Naini (Uni of Wollongong, Australia)

A scheme for obtaining a message from the digital multisignature 154
Chin-Chen Chang, Jyh-Jong Leu, Pai-Cheng Huang and
Wei-Bin Lee (Nat Chung Cheng Uni, Taiwan)

Secure hyperelliptic cryptosystems and their performance 164
Yasuyuki Sakai (MELCO, Japan),
Kouichi Sakurai (Kyushu Uni, Japan) and
Hirokazu Ishizuka (MELCO, Japan)

A practical implementation of elliptic curve cryptosystems
over GF(p) on a 16 bit microcomputer 182
Toshio Hasegawa, Junko Nakajima and
Mitsuru Matsui (MELCO, Japan)

Two efficient algorithms for arithmetic of elliptic curves
using Frobenius map 195
Jung Hee Cheon, Sungmo Park,
Sangwoo Park and Daeho Kim (ETRI, Korea)

Public-key cryptosystems using the modular group 203
Akihiro Yamamura (TAO, Japan)

A cellular automaton based fast one-way hash function
suitable for hardware implementation 217
Miodrag Mihaljević (Acad of Sci and Arts, Yugoslavia),
Yuliang Zheng (Monash Uni, Australia) and
Hideki Imai (Uni of Tokyo, Japan)

A new hash function based on MDx-family and
its application to MAC 234
Sang Uk Shin, Kyung Hyune Rhee (Pukyong Nat Uni, Korea),
Dae Hyun Ryu and Sang Jin Lee (Elect and Telec Res Inst, Korea)

Recent Results

Security issues for contactless smart cards ... 247
Michael W. David (CUBIC, USA) and
Kouichi Sakurai (Kyushu Uni, Japan)

Parameters for secure elliptic curve cryptosystem – improvements on Schoof's algorithm ... 253
Tetsuya Izu, Jun Kogure, Masayuki Noro and
Kazuhiro Yokoyama (Fujitsu, Japan)

A note on the complexity of breaking Okamoto-Tanaka ID-based key exchange scheme ... 258
Masahiro Mambo and Hiroki Shizuya (Tohoku Uni, Japan)

Author Index ... 263

Springer

http://www.springer.com/978-3-540-64693-8

Public Key Cryptography
First International Workshop on Practice and Theory in
Public Key Cryptography, PKC'98, Pacifico Yokohama,
Japan, February 5-6, 1998, Proceedings
Imai, H.; Zheng, Y. (Eds.)
1998, XIII, 271 p., Softcover

ISBN: 978-3-540-64693-8