

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
<i>Yiannis Tsiounis (GTE Labs, USA) and Moti Yung (CertCo, USA)</i>	
An authenticated Diffie-Hellman key agreement protocol secure against active attacks	135
<i>Showichi Hirose and Susumu Yoshida (Kyoto Uni, Japan)</i>	
On the security of Girault's identification scheme	149
<i>Shahrokh Saeednia (Uni Libre de Bruxelles, Belgium) and Rei Safavi-Naini (Uni of Wollongong, Australia)</i>	
A scheme for obtaining a message from the digital multisignature	154
<i>Chin-Chen Chang, Jyh-Jong Leu, Pai-Cheng Huang and Wei-Bin Lee (Nat Chung Cheng Uni, Taiwan)</i>	
Secure hyperelliptic cryptosystems and their performance	164
<i>Yasuyuki Sakai (MELCO, Japan), Kowichi Sakurai (Kyushu Uni, Japan) and Hirokazu Ishizuka (MELCO, Japan)</i>	
A practical implementation of elliptic curve cryptosystems over GF(p) on a 16 bit microcomputer	182
<i>Toshio Hasegawa, Junko Nakajima and Mitsuru Matsui (MELCO, Japan)</i>	
Two efficient algorithms for arithmetic of elliptic curves using Frobenius map	195
<i>Jung Hee Cheon, Sungmo Park, Sangwoo Park and Daeho Kim (ETRI, Korea)</i>	
Public-key cryptosystems using the modular group	203
<i>Akihiro Yamamura (TAO, Japan)</i>	
A cellular automaton based fast one-way hash function suitable for hardware implementation	217
<i>Miodrag Mihaljević (Acad of Sci and Arts, Yugoslavia), Yuliang Zheng (Monash Uni, Australia) and Hideki Imai (Uni of Tokyo, Japan)</i>	
A new hash function based on MDx-family and its application to MAC	234
<i>Sang Uk Shin, Kyung Hyune Rhee (Pukyong Nat Uni, Korea), Dae Hyun Ryu and Sang Jin Lee (Elect and Telec Res Inst, Korea)</i>	

Recent Results

Security issues for contactless smart cards	247
<i>Michael W. David (CUBIC, USA) and Kowichi Sakurai (Kyushu Uni, Japan)</i>	
Parameters for secure elliptic curve cryptosystem – improvements on Schoof’s algorithm	253
<i>Tetsuya Izu, Jun Kogure, Masayuki Noro and Kazuhiro Yokoyama (Fujitsu, Japan)</i>	
A note on the complexity of breaking Okamoto-Tanaka ID-based key exchange scheme	258
<i>Masahiro Mambo and Hiroki Shizuya (Tohoku Uni, Japan)</i>	
Author Index	263