

Contents

Public Key Cryptosystems

Generating RSA Moduli with a Predetermined Portion	1
<i>Arjen K. Lenstra (Citibank, USA)</i>	
Generation of Shared RSA Keys by Two Parties.....	11
<i>Guillaume Poupard, Jacques Stern (ENS, France)</i>	
An Attack on RSA Given a Small Fraction of the Private Key Bits.....	25
<i>Dan Boneh, Glenn Durfee (Stanford Univ., USA)</i>	
<i>Yair Frankel (Certco, USA)</i>	
C_{+}^{*} and HM: Variations Around Two Schemes of T.Matsumoto and H.Imai.....	35
<i>Jacques Patarin, Louis Goubin (BULL, France),</i>	
<i>Nicolas Courtois (Univ. de Toulon, France)</i>	

Invited Talk

ECC/DLP and Factoring-Based Cryptography: A Tale of Two Families.....	50
<i>Burt S. Kaliski Jr. (RSA Labs., USA)</i>	

Elliptic Curve Cryptosystems

Efficient Elliptic Curve Exponentiation Using Mixed Coordinates.....	51
<i>Henri Cohen (Univ. Bordeaux I, France),</i>	
<i>Atsuko Miyaji (MEI., Japan),</i>	
<i>Takatoshi Ono (MISRLNC., Japan)</i>	
Efficient Implementation of Schoof's Algorithm.....	66
<i>Tetsuya Izu, Jun Kogure, Masayuki Noro,</i>	
<i>Kazuhiro Yokoyama (Fujitsu Labs, LTD., Japan)</i>	
Design of Hyperelliptic Cryptosystems in Small Characteristic and a Software Implementation over F_2^n	80
<i>Yasuyuki Sakai (MEC., Japan)</i>	
<i>Kouichi Sakurai (Kyushu Univ., Japan)</i>	
Construction of Secure Elliptic Cryptosystems Using CM Tests and Liftings.....	95
<i>Jinkui Chao, Osamu Nakamura, Kohji Sobataka,</i>	
<i>Shigeo Tsujii (Chuo Univ., Japan)</i>	

Elliptic Curve Discrete Logarithms and the Index Calculus.....	110
<i>Joseph H. Silverman (Brown Univ., USA)</i>	
<i>Joe Suzuki (Osaka Univ., Japan)</i>	

Cryptanalysis 1

Cryptanalysis of Rijmen-Preneel Trapdoor Cipher.....	126
<i>Hongjun Wu (Nat. Univ. of Singapore),</i>	
<i>Feng Bao, Robert H.Deng (Kent Ridge Digital Labs., Singapore),</i>	
<i>Qin-Zhong Ye (Nat. Univ. of Singapore)</i>	

Improved Truncated Differential Attacks on SAFER.....	133
<i>Hongjun Wu (Nat. Univ. of Singapore),</i>	
<i>Feng Bao, Robert H.Deng (Kent Ridge Digital Labs., Singapore),</i>	
<i>Qin-Zhong Ye (Nat. Univ. of Singapore)</i>	

Optimal Resistance Against the Davis and Murphy Attack.....	148
<i>Thomas Pornin (ENS, France)</i>	

Signature

A Group Signature Scheme with Improved Efficiency.....	160
<i>Jan Camenisch (Univ. of Aarhus, Denmark)</i>	
<i>Markus Michels (r3 security engineering, Switzerland)</i>	

A Study on the Proposed Korean Digital Signature Algorithm.....	175
<i>Chae Hoon Lim (Future Systems Inc., Korea)</i>	
<i>Pil Joong Lee (POSTECH, Korea)</i>	

Cryptanalysis 2

Cryptanalysis of the Original McEliece Cryptosystem.....	187
<i>Anne Canteaut, Nicolas Sendrier (INRIA Project CODES, France)</i>	

Improving the Security of the McEliece Public-Key Cryptosystem.....	200
<i>Hung-Min Sun (Chaoyang Univ. of Tech., Taiwan)</i>	

Cryptanalysis in Prime Order Subgroups of Z_n^*	214
<i>Wenbo Mao (Hewlett-Packard Labs., UK)</i>	
<i>Chae Hoon Lim (Future Systems Inc., Korea)</i>	

Finite Automata

Weak Invertibility of Finite Automata and Cryptanalysis on FAPKC.....	227
<i>Zongduo Dai (SKLOIS, China)</i>	
<i>Ding Feng Ye, Kwok Yan Lam (Nat. Univ. of Singapore, Singapore)</i>	

Authentication Codes

Bounds and Constructions for Multireceiver Authentication Codes.....	242
<i>Rei Safavi-Naini, Huaxiong Wang (Univ. of Wollongong, Australia)</i>	

Electronic Cash

FairOff-Line e-Cash Made Easy.....	257
<i>Yair Frankel (CertCo, USA)</i>	
<i>Yiannis Tsiounis (GTE Labs., USA)</i>	
<i>Moti Yung (CertCo, USA)</i>	
Off-Line Fair Payment Protocols Using Convertible Signatures.....	271
<i>Colin Boyd, Ernest Foo (Queensland Univ. of Tech., Australia)</i>	
Efficient Fair Exchange with Verifiable Confirmation of Signatures.....	286
<i>Liqun Chen (Hewlett-Packard Labs., UK)</i>	
Adaptively Secure Oblivious Transfer.....	300
<i>Donald Beaver (Transarc Corp. USA)</i>	

Stream Ciphers

ML-Sequences over Rings $\mathbb{Z}/(2^n)$	315
<i>Wenfeng Qi (ZIEI, China)</i>	
<i>Junhui Yang (Academia Sinica, China)</i>	
<i>Jingjun Zhou (ZIEI, China)</i>	
Analysis Methods for (Alleged) RC4.....	327
<i>Lars R. Knudsen (Univ. of Bergen, Belgium)</i>	
<i>Willi Meier (HTL Brugg-Windisch, Belgium)</i>	
<i>Bart Preneel, Vincent Rijmen, Sven Verdoolaege (ESAT, K. U. Leuven, Belgium)</i>	
Reduced Complexity Correlation Attacks on Two Clock-Controlled Generators	342
<i>Thomas Johansson (Lund Univ., Sweden)</i>	

Cryptographic Protocols

A New and Efficient All-Or-Nothing Disclosure of Secrets Protocol	357
<i>Julien P. Stern (UCL Crypto Group, Belgium)</i>	

The Béguin-Quisquater Server-Aided RSA Protocol fom Crypto'95 is Not secure	372
<i>Phong Nguyen, Jacques Stern (ENS, France)</i>	

Key Escrow

Equitable Key Escrow with Limited Time Span (or How to Enforce Time Expiration Cryptographically).....	380
<i>Mike Burmester (Univ. of London, UK)</i>	
<i>Yvo Desmedt (Univ. of Wisconsin-Milwaukee, USA),</i>	
<i>Jennifer, Seberry (Univ. of Wollongong, Australia)</i>	

New Cryptography

Audio and Optical Cryptography.....	392
<i>Yvo Desmedt, Shuang Hou (Univ. of Wisconsin-Milwaukee, USA),</i>	
<i>Jean-Jacques Quisquater (Univ. Catholique de Louvain, Belgium)</i>	

Information Theory

Strong Security Against Active Attacks in Information-Theoretic Secret-Key Agreement.....	405
<i>Stefan Wolf (ETH, Switzerland)</i>	
Some Bounds and a Construction for Secure Broadcast Encryption.....	420
<i>Kaoru Kurosawa, Takuya Yoshida (Tokyo Institute of Technology, Japan)</i>	
<i>Yvo Desmedt, (Univ. of Wisconsin-Milwaukee, USA)</i>	
<i>M.Burmester(Univ. of London, UK)</i>	

Author Index	435
---------------------------	-----

Advances in Cryptology — ASIACRYPT'98
International Conference on the Theory and Application
of Cryptology and Information Security, Beijing, China,
October 18–22, 1998, Proceedings
Ohta, K.; Pei, D. (Eds.)
1998, XII, 436 p. 2 illus., Softcover
ISBN: 978-3-540-65109-3