Contents

Public Key Cryptosystems

Generating RSA Moduli with a Predetermined Portion …………………………… 1
Arjen K. Lenstra (Citibank, USA)

Generation of Shared RSA Keys by Two Parties…………………………………... 11
Guillaume Poupard, Jacques Stern (ENS, France)

An Attack on RSA Given a Small Fraction of the Private Key Bits……………….. 25
Dan Boneh, Glenn Durfee (Stanford Univ., USA)
Yair Frankel (Certco, USA)

C^*_{-+} and HM: Variations Around Two Schemes of T.Matsumoto and H.Imai......... 35
Jacques Patarin, Louis Goubin (BULL, France),
Nicolas Courtois (Univ. de Toulon, France)

Invited Talk

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

Elliptic Curve Cryptosystems

Efficient Elliptic Curve Exponentiation Using Mixed Coordinates......................... 51
Henri Cohen (Univ. Bordeaux I, France),
Atsuko Miyaji (MEI., Japan),
Takatoshi Ono (MISRLNC., Japan)

Efficient Implementation of Schoof’s Algorithm………………………………….. 66
Tetsuya Izu, Jun Kogure, Masayuki Noro,
Kazuhiro Yokoyama (Fujitsu Labs, LTD., Japan)

Design of Hyperelliptic Cryptosystems in Small Characteristic and a Software Implementation over F_2 n ……………………………………………………… 80
Yasuyuki Sakai (MEC., Japan)
Kouichi Sakurai (Kyushu Univ., Japan)

Construction of Secure Elliptic Cryptosystems Using CM Tests and Liftings......... 95
Jinkui Chao, Osamu Nakamura, Kohji Sobataka,
Shigeo Tsujii (Chuo Univ., Japan)

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

Cryptanalysis 1

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

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

Optimal Resistance Against the Davis and Murphy Attack…………………..….. 148
Thomas Pornin (ENS, France)

Signature

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

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

Cryptanalysis 2

Cryptanalysis of the Original McEliece Cryptosystem………………………….. 187
Anne Canteaut, Nicolas Sendrier (INRIA Project CODES, France)

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

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

Finite Automata

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

Authentication Codes

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

Electronic Cash

FairOff-Line e-Cash Made Easy………………………………………………… 257
Yair Frankel (CertCo, USA)
Yiannis Tsiounis (GTE Labs., USA)
Moti Yung (CertCo, USA)

Off-Line Fair Payment Protocols Using Convertible Signatures………………… 271
Colin Boyd, Ernest Foo (Queensland Univ. of Tech., Australia)

Efficient Fair Exchange with Verifiable Confirmation of Signatures…………… 286
Liqun Chen (Hewlett-Packard Labs., UK)

Adaptively Secure Oblivious Transfer……………………………………….. 300
Donald Beaver (Transarc Corp. USA)

Steam Ciphers

ML-Sequences over Rings Z/(2^n)……………………………………….......... 315
Wenfeng Qi (ZIEI, China)
Junhui Yang (Academia Sinica, China)
Jingjun Zhou (ZIEI, China)

Analysis Methods for (Alleged) RC4…………………………………………… 327
Lars R.Knudsen (Univ. of Bergen, Belgium)
Willi Meier (HTL Brugg-Windisch, Belgium)
Bart Preneel, Vincent Rijmen, Sven Verdoolaege (ESAT, K. U. Leuven, Belgium)

Reduced Complexity Correlation Attacks on Two Clock-Controlled Generators ……………………………………………………….……. 342
Thomas Johansson (Lund Univ., Sweden)

Cryptographic Protocols

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

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

Key Escrow

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

New Cryptography

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

Information Theory

Strong Security Against Active Attacks in Information-Theoretic Secret-Key Agreement……………………………………………………………….. 405
Stefan Wolf (ETH, Switzerland)

Some Bounds and a Construction for Secure Broadcast Encryption…………… 420
Kaoru Kurosawa, Takuya Yoshida (Tokyo Institute of Technology, Japan)
Yvo Desmedt, (Univ. of Wisconsin-Milwaukee, USA)
M.Burmester(Univ. of London, UK)

Author Index ………………………………………………………… 435