

CONTENTS

SECTION 1: PUBLIC-KEY CRYPTOSYSTEMS

The implementation of elliptic curve cryptosystems <i>Alfred Menezes, Scott A. Vanstone</i>	2
Direct demonstration of the power to break public-key cryptosystems <i>Kenji Koyama</i>	14

SECTION 2: PSEUDORANDOMNESS AND SEQUENCES I

Continued fractions and Berlekamp-Massey algorithm <i>Zongduo Dai, Kencheng Zeng</i>	24
Nonlinear generators of binary sequences with controllable complexity and double key <i>Gong Guang</i>	32
K-M sequence is forwardly predictable <i>Yang Yi Xian</i>	37
Lower bounds on the weight complexities of cascaded binary sequences <i>Cunsheng Ding</i>	39

SECTION 3: NETWORK SECURITY

Secure user access control for public networks <i>Pil Joong Lee</i>	46
Formal specification and verification of secure communication protocols <i>Svein J. Knapskog</i>	58
Network security policy models <i>Vijay Varadharajan</i>	74
KEYMEX: an expert system for the design of key management schemes <i>J. C. A. van der Lubbe, Dick E. Boeke</i>	96

SECTION 4: AUTHENTICATION

On the formal analysis of PKCS authentication protocols <i>Klaus Gaarder, Einar Snekkenes</i>	106
Some remarks on authentication systems <i>Martin H. G. Anthony, Keith M. Martin, Jennifer Seberry, Peter Wild</i>	122

Meet-in-the-middle attack on digital signature schemes <i>Kazuo Ohta, Kenji Koyama</i>	140
---	-----

SECTION 5: PSEUDORANDOMNESS AND SEQUENCES II

A binary sequence generator based on Ziv-Lempel source coding <i>Cees J. Jansen, Dick E. Boeke</i>	156
A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence <i>Miodrag J. Mihaljević, Jovan D. Golić</i>	165
Parallel generation of pseudo-random sequences <i>Reihaneh Safavi-Naini</i>	176
Large primes in stream cipher cryptography <i>Kencheng Zeng, C. H. Yang, T. R. N. Rao</i>	194

SECTION 6: BLOCK CIPHERS

Comparison of block ciphers <i>Helen Gustafson, Ed Dawson, Bill Caelli</i>	208
Key scheduling in DES type cryptosystems <i>Lawrence Brown, Jennifer Seberry</i>	221
LOKI — a cryptographic primitive for authentication and secrecy applications <i>Lawrence Brown, Josef Pieprzyk, Jennifer Seberry</i>	229
Permutation generators of alternating groups <i>Josef Pieprzyk, Xian Mo Zhang</i>	237

SECTION 7: ZERO-KNOWLEDGE PROTOCOLS

Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms <i>David Chaum</i>	246
A (non-practical) three-pass identification protocol using coding theory <i>Marc Girault</i>	265
Demonstrating possession without revealing factors and its application <i>Hiroki Shizuya, Kenji Koyama, Toshiya Itoh</i>	273
Anonymous one-time signatures and flexible untraceable electronic cash <i>Barry Hayes</i>	294

SECTION 8: THEORY

Dyadic matrices and their potential significance in cryptography <i>Yang Yi Xian</i>	308
A note on strong Fibonacci pseudoprimes <i>Rudolf Lidl, Winfried B. Müller</i>	311
On the significance of the directed acyclic word graph in cryptology <i>Cees J. Jansen, Dick E. Boeke</i>	318
Solving equations in sequences <i>Kencheng Zeng, Mingqiang Huang</i>	327

SECTION 9: APPLICATIONS

The practical application of state of the art security in real environments <i>Ronald Ferreira</i>	334
RSA as a benchmark for multiprocessor machines <i>Rodney H. Cooper, Wayne Patterson</i>	356
Range equations and range matrices: a study in statistical database security <i>V. S. Alagar</i>	360
Record encryption in distributed databases <i>Thomas Hardjono</i>	386

SECTION 10: IMPLEMENTATIONS

VLSI design for exponentiation in $GF(2^n)$ <i>W. Geiselmann, D. Gollmann</i>	398
A fast modular-multiplication module for smart cards <i>Hikaru Morita</i>	406
Minos: extended user authentication <i>Michael Newberry</i>	410

SECTION 11: RUMP SESSION

Universal logic sequences <i>Ed Dawson, Bruce Goldberg</i>	426
The three faces of information security <i>John M. Carroll</i>	433
Secure cryptographic initialization <i>Mark Ames</i>	451