

CONTENTS

SECTION I: GENERAL THEORY, CLASSICAL METHODS

Cryptology and Complexity Theories.....	3
G. RUGGIU	
On Cryptosystems based on Polynomials and Finite Fields.....	10
R. LIDL	
Algebraical Structures of Cryptographic Transformations.....	16
J.P. PIEPRZYK	
Non-Linear, Non-Commutative Functions for Data Integrity.....	25
S. HARARI	
Wire-Tap Channel II.....	33
L.H. OZAROW, A.D. WYNER	
Equivocations for Homophonic Ciphers.....	51
A. SGARRO	
Propagation Characteristics of the DES.....	62
M. DAVIO, Y. DESMEDT, J.J. QUISQUATER	
Linear Ciphers and Random Sequence Generators with Multiple Clocks.....	74
J.L. MASSEY, R.A. RUEPPEL	
The Stop-and-go Generator.....	88
T. BETH, F.C. PIPER	
Pseudo Random Properties of Cascade Connections of Clock Controlled Shift Registers.....	93
D. GOLLMAN	
On the Linear Complexity of Cascaded Sequences.....	99
R. VOGEL	

SECTION II: PUBLIC-KEY SYSTEMS

RSA-Bits are $0.5 + \epsilon$ Secure.....	113
C.P. SCHNORR, W. ALEXI	
On the Number of Close-and-equal Pairs of Bits in a String....	127
O. GOLDBREICH	

Fast Cryptanalysis of the Matsumoto-Imai Public Key Scheme.....	142
V. DESMEDT, P. DELSARTE, A. ODLYZKO, P. PIRET	
A New Trapdoor Knapsack Public-Key Cryptosystem.....	150
R.M.F. GOODMAN, A.J.MC AULEY	
RSA Chips (Past/Present/Future).....	159
R. RIVEST	

SECTION III: NUMBER THEORETICAL PAPERS

The Quadratic Sieve Factoring Algorithm.....	169
C. POMERANCE	
Status Report on Factoring (At the Sandia National Labs).....	183
J.A. DAVIS, D.B. HOLDRIDGE, G.J. SIMMONS	
Strong Primes are Easy to Find.....	216
J.A. GORDON	
Discrete Logarithms in Finite Fields and their Cryptographic Significance.....	224
A.M. ODLYZKO	

SECTION IV: CHANNELS, NETWORKS, KEY DISTRIBUTION, PROTOCOLS

User Functions for the Generation and Distribution of Encipherment Keys.....	317
R.W. JONES	
An Optimal Class of Symmetric Key Generation Systems.....	335
R. BLOM	
On the Use of the Binary Multiplying Channel in a Private Communication System.....	339
B.J.M. SMEETS	
Secrecy and Privacy in a Local Area Network Environment.....	349
G.B. AGNEW	
The Subliminal Channel and Digital Signatures.....	364
G.J. SIMMONS	
A Provably Secure Oblivious Transfer Protocol.....	379
R. BERGER, R. PERALTA, T. TEDRICK	
On Concurrent Identification Protocols.....	387
O. GOLDBREICH	

SECTION V : APPLICATIONS

Time-division Multiplexing Scramblers: Selecting Permutations and Testing the Systems.....	399
A. ECKER	
Security of Transportable Computerized Files.....	416
A. BOUCKAERT	
Encryption and Key Management for the ECS Satellite Service.....	426
S.C. SERPELL, C.B. BROOKSON	
An Encryption and Authentication Procedure for Tele-surveillance Systems.....	437
W. WOLFOWICZ, O. BRUGIA, S. IMPROTA	
A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques.....	446
I. SCHAU Mueller, E. PILLER	

SECTION VI: SMART CARDS

Introductory Remarks.....	457
A. TURBAT	
Smart Card Applications in Security and Data Protection.....	459
J. GOUTAY	
Bull CP8 Smart Card Uses in Cryptology.....	464
V. GIRARDOT	
Estimation of Some Encryption Functions Implemented into Smart Cards.....	470
H. GROSCOT	
Smart Cards and Conditional Access.....	480
L. GUILLON	
AUTHOR INDEX.....	491