

CONTENTS

SECTION I: SEQUENCES AND LINEAR COMPLEXITY

In Memoriam Tore Herlestam (1929-1986).....	3
<i>James L. Massey</i>	
Alternating Step Generators	
Controlled by De Bruijn Sequences.....	5
<i>C.G. Günther</i>	
Generation of Binary Sequences with Controllable	
Complexity and Ideal r -Tupel Distribution	15
<i>Thomas Siegenthaler, Amstein Walthert Kleiner, and Réjane Forré</i>	
Some Remarks on the Cross Correlation Analysis	
of Pseudo Random Generators.....	25
<i>Sibylle Mund, Dieter Gollmann, and Thomas Beth</i>	
Sequences with Almost Perfect Linear Complexity Profile	37
<i>Harald Niederreiter</i>	
When Shift Registers Clock Themselves.....	53
<i>Rainer A. Rueppel</i>	
Finite State Machine Modelling	
of Cryptographic Systems in Loops.....	65
<i>Franz Pichler</i>	

SECTION II: HARDWARE TOPICS

Random Sources for Cryptographic Systems	77
<i>G.B. Agnew</i>	
Physical Protection of Cryptographic Devices	83
<i>Andrew J. Clark</i>	
The RSA Cryptography Processor.....	95
<i>Holger Sedlak</i>	

SECTION III: PUBLIC KEY TOPICS

Extension of Brickell's Algorithm for Breaking High Density Knapsacks	109
<i>F. Jorissen, J. Vandewalle, and R. Govaerts</i>	
On Privacy Homomorphisms (Extended Abstract)	117
<i>Ernest F. Brickell and Yacov Yacobi</i>	
An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations	127
<i>David Chaum, Jan-Hendrik Evertse, and Jeroen van de Graaf</i>	
A Public Key Analog Cryptosystem	143
<i>George I. Davida and Gilbert G. Walter</i>	

SECTION IV: AUTHENTICATION AND SECURE TRANSACTIONS

Message Authentication with Arbitration of Transmitter/Receiver Disputes	151
<i>Gustavus J. Simmons</i>	
Perfect and Essentially Perfect Authentication Schemes (Extended Abstract)	167
<i>Albrecht Beutelspacher</i>	
Message Authentication and Dynamic Passwords.....	171
<i>H.J. Beker and G.M. Cole</i>	
IC-Cards in High-Security Applications.....	177
<i>I. Schaumüller-Bichl</i>	

SECTION V: HASH FUNCTIONS AND SIGNATURES

Collision Free Hash Functions and Public Key Signature Schemes.....	203
<i>Ivan Bjerre Damgård</i>	
Hash-Functions Using Modulo-N Operations.....	217
<i>Marc Girault</i>	
Blinding for Unanticipated Signatures.....	227
<i>David Chaum</i>	

SECTION VI: SYMMETRIC CIPHERS: THEORY

Non-Expanding, Key-Minimal, Robustly-Perfect, Linear and Bilinear Ciphers.....	237
<i>James L. Massey, Ueli Maurer, and Muzhong Wang</i>	
Linear Structures in Blockciphers.....	249
<i>Jan-Hendrik Evertse</i>	
Fast Data Encipherment Algorithm FEAL.....	267
<i>Akihiro Shimizu and Shoji Miyaguchi</i>	

SECTION VII: SYMMETRIC CIPHERS: APPLICATION

Modes of Blockcipher Algorithms and their Protection Against Active Eavesdropping.....	281
<i>Cees J.A. Jansen and Dick E. Boeke</i>	
Security Considerations in the Design and Implementation of a New DES Chip.....	287
<i>Ingrid Verbauwhede, Frank Hoornaert, Joos Vandewalle, and Hugo De Man</i>	
High-Performance Interface Architectures for Cryptographic Hardware.....	301
<i>David P. Anderson and P. Venkat Rangan</i>	
Author Index.....	311
Keyword Index.....	313