

CONTENTS

SECTION I: KEY DISTRIBUTION

Key Agreements Based on Function Composition	3
<i>Rainer A. Rueppel</i>	
Security of Improved Identity-Based Conference	
Key Distribution Systems	11
<i>Kenji Koyama, Kazuo Ohta</i>	

SECTION II: AUTHENTICATION

Subliminal-Free Authentication and Signature	23
<i>Yvo G. Desmedt</i>	
Zero-Knowledge Proofs of Identity and Veracity of Transaction Receipts	35
<i>Gustavus J. Simmons, George B. Purdy</i>	
Authentication Codes with Multiple Arbiters	51
<i>Ernest F. Brickell, Doug R. Stinson</i>	
Some Constructions for Authentication-Secrecy Codes	57
<i>Marijke De Soete</i>	
Efficient Zero-Knowledge Identification Scheme	
for Smart Cards	77
<i>Thomas Beth</i>	

SECTION III: SIGNATURES

A Smart Card Implementation of the Fiat-Shamir Identification Scheme	87
<i>Hans-Joachim Knobloch</i>	
Manipulations and Errors, Detection and Localization	97
<i>Ph. Godlewski, P. Camion</i>	
Privacy Protected Payments - Realization of a Protocol that Guarantees Payer Anonymity	107
<i>Svein J. Knapskog</i>	
A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory	123
<i>Louis C. Guillou, Jean-Jacques Quisquater</i>	
A Generalized Birthday Attack	129
<i>Marc Girault, Robert Cohen, Mireille Campana</i>	

SECTION IV: PROTOCOLS

An Interactive Data Exchange Protocol Based on Discrete Exponentiation	159
<i>G. B. Agnew, R. C. Mullin, S. A. Vanstone</i>	
Anonymous and Verifiable Registration in Databases	167
<i>Jørgen Brandt, Ivan Bjerre Damgård, Peter Landrock</i>	
Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA	177
<i>David Chaum</i>	
Passports and Visas Versus ID's	183
<i>George I. Davida, Yvo G. Desmedt</i>	

SECTION V: COMPLEXITY AND NUMBER THEORY

The Probabilistic Theory of Linear Complexity	191
<i>Harald Niederreiter</i>	
A Probabilistic Primality Test Based on the Properties of Certain Generalized Lucas Numbers	211
<i>Adina Di Porto, Piero Filippini</i>	
On the Construction of Random Number Generators and Random Function Generators	225
<i>C. P. Schnorr</i>	

SECTION VI: NUMERICAL METHODS

Factorization of Large Integers on a Massively Parallel Computer	235
<i>James A. Davis, Diane B. Holdridge</i>	
A Fast Modular Arithmetic Algorithm Using a Residue Table	245
<i>Shin-ichi Kawamura, Kyoko Hirano</i>	
Fast Exponentiation in $GF(2^n)$	251
<i>G. B. Agnew, R. C. Mullin, S. A. Vanstone</i>	
Fast RSA-Hardware: Dream or Reality?	257
<i>Frank Hoornaert, Marc Decroos, Joos Vandewalle, René Govaerts</i>	

SECTION VII: CRYPTANALYSIS

Properties of the Euler Totient Function Modulo 24 and Some of its Cryptographic Implications	267
<i>Raouf N. Gorgui-Naguib, Satnam S. Dlay</i>	
An Observation on the Security of McEliece's Public-Key Cryptosystem ...	275
<i>P. J. Lee, E. F. Brickell</i>	
How to Break Okamoto's Cryptosystem by Reducing Lattice Bases	281
<i>Brigitte Vallée, Marc Girault, Philippe Toffin</i>	
Cryptanalysis of F. E. A. L.	293
<i>Bert Den Boer</i>	
Fast Correlation Attacks on Stream Ciphers	301
<i>Willi Meier, Othmar Staffelbach</i>	

SECTION VIII: RUNNING-KEY CIPHERS

A New Class of Nonlinear Functions for Running-Key Generators	317
<i>Shu Tezuka</i>	
Windmill Generators: A Generalization and an Observation of How Many There Are	325
<i>B. J. M. Smeets, W. G. Chambers</i>	
Lock-in Effect in Cascades of Clock-Controlled Shift-Registers	331
<i>William G. Chambers, Dieter Gollmann</i>	
Proof of Massey's Conjectured Algorithm	345
<i>Cunsheng Ding</i>	
Linear Recurring m-Arrays	351
<i>Dongdai Lin, Mulan Liu</i>	

SECTION IX: CIPHER THEORY AND THRESHOLD

Substantial Number of Cryptographic Keys and its Application to Encryption Designs	361
<i>Eiji Okamoto</i>	
A Measure of Semiequivocation	375
<i>Andrea Sgarro</i>	
Some New Classes of Geometric Threshold Schemes	389
<i>Marijke De Soete, Klaus Vedder</i>	

SECTION X: NEW CIPHERS

A Universal Algorithm for Homophonic Coding	405
<i>Christoph G. Günther</i>	
A New Probabilistic Encryption Scheme	415
<i>He Jingmin, Lu Kaicheng</i>	
Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption	419
<i>Tsutomu Matsumoto, Hideki Imai</i>	
Some Applications of Multiple Key Ciphers	455
<i>Colin Boyd</i>	
Author Index	469
Keyword Index	471