

# Contents

## Secret Sharing

Visual cryptography . . . . .	1
<i>Moni Naor and Adi Shamir</i>	
The size of a share must be large . . . . .	13
<i>L. Csirmaz</i>	
A linear construction of perfect secret sharing schemes . . . . .	23
<i>M. van Dijk</i>	
On the dealer's randomness required in secret sharing schemes . . . . .	35
<i>C. Blundo, A. Giorgio Gaggia and D. R. Stinson</i>	

## Hash functions

Black box cryptanalysis of hash networks based on multipermutations . .	47
<i>C. P. Schnorr and S. Vaudenay</i>	
A practical attack against knapsack based hash functions . . . . .	58
<i>A. Joux and L. Granboulan</i>	

## Signatures I

The blinding of weak signatures . . . . .	67
<i>M. Franklin and M. Yung</i>	
Can D.S.A. be improved? Complexity trade-offs with the digital signature standard . . . . .	77
<i>D. Naccache, D. M'Raihi, S. Vaudenay and D. Raphaëli</i>	
Designated confirmer signatures . . . . .	86
<i>D. Chaum</i>	

## Cryptosystems

Optimal asymmetric encryption . . . . .	92
<i>M. Bellare and P. Rogaway</i>	
A multiple-iterated trapdoor for dense compact knapsacks . . . . .	112
<i>G. Orton</i>	
On the security of some cryptosystems based on error-correcting codes . .	131
<i>F. Chabaud</i>	

## Zero-Knowledge and Protocol Methodology

Parallel divertibility of proofs of knowledge . . . . .	140
<i>L. Chen, I.B. Damgård and T.P. Pedersen</i>	
Methodology for digital money based on general cryptographic tools . . .	156
<i>S. D'Amiano and G. Di Crescenzo</i>	

## Signatures II

New group signature schemes . . . . .	171
<i>L. Chen and T.P. Pedersen</i>	
Message recovery for signature schemes based on the discrete logarithm problem . . . . .	182
<i>K. Nyberg and R. A. Rueppel</i>	
Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders . . . . .	194
<i>C.-M. Li, T. Hwang and N.-Y. Lee</i>	

## Pseudorandom Generators

The self-shrinking generator . . . . .	205
<i>W. Meier and O. Staffelbach</i>	
Feedback registers based on ramified extensions of the 2-adic numbers . .	215
<i>M. Goresky and A. Klapper</i>	

A general lower bound for the linear complexity of the product of shift-register sequences . . . . .	223
<i>R. Göttert and H. Niederreiter</i>	
Embedding and probabilistic correlation attacks on clock-controlled shift registers . . . . .	230
<i>J. Dj. Golić and L. O'Connor</i>	

## Authentication Codes

Near optimal unconditionally secure authentication . . . . .	244
<i>R. Taylor</i>	
Authentication codes in plaintext and chosen-content attacks . . . . .	254
<i>R. Safavi-Naini and L. Tombak</i>	

## Key Agreement and Key Distribution

Linking information reconciliation and privacy amplification . . . . .	266
<i>C. Cachin and U. M. Maurer</i>	
A secure and efficient conference key distribution system . . . . .	275
<i>M. Burmester and Y. Desmedt</i>	
Space requirements for broadcast encryption . . . . .	287
<i>C. Blundo and A. Cresti</i>	
How to break and repair Leighton and Micali's key agreement protocol . .	299
<i>Y. Zheng</i>	

## Protocols

Single-term divisible electronic coins . . . . .	306
<i>T. Eng and T. Okamoto</i>	
Formal requirements for key distribution protocols . . . . .	320
<i>P. Syverson and C. Meadows</i>	
Breaking an efficient anonymous channel . . . . .	332
<i>B. Pfitzmann</i>	

## Cryptanalysis and Block Ciphers

On Matsui's linear cryptanalysis . . . . .	341
<i>E. Biham</i>	
Links between differential and linear cryptanalysis . . . . .	356
<i>F. Chabaud and S. Vaudenay</i>	
On correlation between the order of S-boxes and the strength of DES . . .	366
<i>M. Matsui</i>	
Relationships among nonlinearity criteria . . . . .	376
<i>J. Seberry, X.-M. Zhang and Y. Zheng</i>	

## Number Theory and Algorithms

Efficient exponentiation using precomputation and vector addition chains	389
<i>P. de Rooij</i>	
MIMD-factorisation on hypercubes . . . . .	400
<i>F. Damm, F.-P. Heider and G. Wambach</i>	

## Rump Session

New attacks on all double block length hash functions of hash rate 1, including the parallel-DM . . . . .	410
<i>L. R. Knudsen and X. Lai</i>	
New potentially 'weak' keys for DES and LOKI . . . . .	419
<i>L. R. Knudsen</i>	
Blackmailing using undeniable signatures . . . . .	425
<i>M. Jakobsson</i>	
Blind signatures based on the discrete logarithm problem . . . . .	428
<i>J. L. Camenisch, J.-M. Piveteau and M. A. Stadler</i>	
Comments on soviet encryption algorithm . . . . .	433
<i>C. Charnes, L. O'Connor, J. Pieprzyk, R. Safavi-Naini and Y. Zheng</i>	
Linear approximation of block ciphers . . . . .	439
<i>K. Nyberg</i>	

Memory efficient variants of public-key schemes for smart card applications . . . . .	445
<i>A. Shamir</i>	
A systematic attack on clock controlled cascades . . . . .	450
<i>R. Menicocci</i>	
On $A^2$ -codes including arbiter's attacks . . . . .	456
<i>T. Johansson and B. Smeets</i>	
An improvement of Davies' attack on DES . . . . .	461
<i>E. Biham and A. Biryukov</i>	
Q-deformed quantum cryptography . . . . .	468
<i>J. Hruby</i>	
 <b>Author Index . . . . .</b>	 473

Advances in Cryptology - EUROCRYPT '94  
Workshop on the Theory and Application of  
Cryptographic Techniques, Perugia, Italy, May 9 - 12,  
1994. Proceedings  
DeSantis, A. (Ed.)  
1995, XIII, 477 p., Softcover  
ISBN: 978-3-540-60176-0