

Contents

Authentication

On the relation between A-codes and codes correcting independent errors

T. Johansson, G. Kabatianskii, B. Smeets 1

Optimal authentication systems

R. Safavi-Naini, L. Tombak 12

Public Key

Factoring integers using SIMD sieves

B. Dixon, A.K. Lenstra 28

A new elliptic curve based analogue of RSA

N. Demytko 40

Weaknesses of a public-key cryptosystem based on factorizations of finite groups

S. Blackburn, S. Murphy, J. Stern 50

Block Ciphers

Differentially uniform mappings for cryptography

K. Nyberg 55

On almost perfect nonlinear permutations

T. Beth, C. Ding 65

Two new classes of bent functions

C. Carlet 77

Boolean functions satisfying a higher order strict avalanche criterion

T.W. Cusick 102

Secret Sharing

Size of shares and probability of cheating in threshold schemes

M. Carpentieri, A. De Santis, U. Vaccaro 118

Nonperfect secret sharing schemes and matroids

K. Kurosawa, K. Okada, K. Sakano, W. Ogata, S. Tsujii 126

Stream ciphers

From the memoirs of a Norwegian cryptologist

E. Selmer 142

On the linear complexity of products of shift-register sequences

R. Göttert, H. Niederreiter 151

Resynchronization weaknesses in synchronous stream ciphers

J. Daemen, R. Govaerts, J. Vandewalle 159

Blind synchronization of m -sequences with even span

R. A. Games, J. J. Rushanan 168

On constructions and nonlinearity of correlation immune functions

J. Seberry, X.-M. Zhang, Y. Zheng 181

Digital signatures

Practical and provably secure release of a secret and exchange of signatures

I.B. Damgård 200

Subliminal communication is easy using the DSA

G.J. Simmons 218

Can O.S.S. be Repaired?

—Proposal for a new practical signature scheme—

D. Naccache 233

Protocols I

On a limitation of BAN logic

C. Boyd, W. Mao 240

Efficient anonymous channel and all/nothing election scheme

C. Park, K. Itoh, K. Kurosawa 248

Untransferable rights in a client-independent server environment

J. Domingo-Ferrer 260

Interactive hashing simplifies zero-knowledge protocol design

R. Ostrovsky, R. Venkatesan, M. Yung 267

Hash Functions

<i>One-way accumulators: A decentralized alternative to digital signatures</i>	
J. Benaloh, M. de Mare	274
<i>The breaking of the AR hash function</i>	
I. B. Damgård, L. R. Knudsen	286
<i>Collisions for the compression function of MD5</i>	
B. den Boer, A. Bosselaers	293
<i>How to find and avoid collisions for the knapsack hash function</i>	
J. Patarin	305

Payment Systems

<i>Single term off-line coins</i>	
N. Ferguson	318
<i>Improved privacy in wallets with observers</i>	
R. J. F. Cramer, T. P. Pedersen	329
<i>Distance-bounding protocols</i>	
S. Brands, D. Chaum	344

Cryptanalysis

<i>On the distribution of characteristics in bijective mappings</i>	
L. O'Connor	360
<i>On the security of the IDEA block cipher</i>	
W. Meier	371
<i>Linear cryptanalysis method for DES cipher</i>	
M. Matsui	386
<i>New types of cryptanalytic attacks using related keys</i>	
E. Biham	398

Protocols II

<i>Secret key reconciliation by public discussion</i>	
G. Brassard, L. Salvail	410
<i>Global, unpredictable bit generation without broadcast</i>	
D. Beaver, N. So	424

Rump Session

<i>On Schnorr's preprocessing for digital signature schemes</i>	
P. de Rooij	435
<i>Cryptanalysis of the Chang-Wu-Chen key distribution system</i>	
M. Burmester	440
<i>An alternate explanation of two BAN-logic "failures"</i>	
P. C. van Oorschot	443
<i>The consequences of trust in shared secret schemes</i>	
G. J. Simmons	448
<i>Markov ciphers and alternating groups</i>	
G. Hornauer, W. Stephan, R. Wernsdorf	453
<i>On key distribution and authentication in mobile radio networks</i>	
C. Park, K. Kurosawa, T. Okamoto, S. Tsujii	461
List of Authors	467