

Table of Contents

Invited Lecture

Cryptographic Functions and Design Criteria for Block Ciphers	1
<i>A. Canteaut</i>	

Hashing

Mobile Agent Route Protection through Hash-Based Mechanisms	17
<i>J. Domingo-Ferrer</i>	

A New Anonymous Fingerprinting Scheme with High Enciphering Rate	30
<i>M. Kuribayashi and H. Tanaka</i>	

A Parallel Algorithm for Extending Cryptographic Hash Functions	40
<i>P. Sarkar and P.J. Schellenberg</i>	

Incremental Hash Function

Based on Pair Chaining & Modular Arithmetic Combining	50
<i>B.-M. Goi, M.U. Siddiqi, and H.-T. Chuah</i>	

Algebraic Schemes

Multiples of Primitive Polynomials over $GF(2)$	62
<i>K.C. Gupta and S. Maitra</i>	

Fast Generation of Cubic Irreducible Polynomials for XTR	73
<i>J.M. Kim, I. Yie, S.I. Oh, H.D. Kim, and J. Ryu</i>	

Cheating Prevention in Secret Sharing over $GF(p^t)$	79
<i>J. Pieprzyk and X.-M. Zhang</i>	

Elliptic Curves

An Application of Sieve Methods to Elliptic Curves	91
<i>S.A. Miri and V.K. Murty</i>	

Elliptic Curves of Prime Order over Optimal Extension Fields

for Use in Cryptography	99
<i>H. Baier</i>	

A Secure Family of Composite Finite Fields

Suitable for Fast Implementation of Elliptic Curve Cryptography	108
<i>M. Ciet, J.-J. Quisquater, and F. Sica</i>	

Coding Theory

Frameproof and IPP Codes	117
<i>P. Sarkar and D.R. Stinson</i>	

Linear Authentication Codes: Bounds and Constructions	127
<i>R. Safavi-Naini, H. Wang and C. Xing</i>	

Applications – I

Selective Receipt in Certified E-Mail	136
<i>S. Kremer and O. Markowitch</i>	

Spatial Domain Digital Watermarking with Buyer Authentication	149
<i>S. Maitra and D.P. Mukherjee</i>	

Efficient Public Auction with One-Time Registration and Public Verifiability	162
<i>B. Lee, K. Kim, and J. Ma</i>	

An Analysis of Integrity Services in Protocols	175
<i>K. Viswanathan, C. Boyd, and E. Dawson</i>	

Cryptanalysis

Cryptanalysis of the Nonlinear FeedForward Generator	188
<i>S.S. Bedi and N.R. Pillai</i>	

Analysis of the GHS Weil Descent Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree	195
<i>M. Maurer, A. Menezes, and E. Teske</i>	

Cryptanalysis of Imai and Matsumoto Scheme B Asymmetric Cryptosystem	214
<i>A. Youssef and G. Gong</i>	

Distributed Cryptography

Robust and Secure Broadcasting	223
<i>Y. Mu and V. Varadharajan</i>	

Toward Optimal Player Weights in Secure Distributed Protocols	232
<i>K. Srinathan, C.P. Rangan, and V. Kamakoti</i>	

Boolean Functions

Autocorrelation Properties of Correlation Immune Boolean Functions	242
<i>S. Maitra</i>	

On the Constructing of Highly Nonlinear Resilient Boolean Functions by Means of Special Matrices	254
<i>M. Fedorova and Y. Tarannikov</i>	

Digital Signatures

A Twin Algorithm for Efficient Generation of Digital Signatures	267
<i>D. Ramesh</i>	
Efficient “on the Fly” Signature Schemes Based on Integer Factoring	275
<i>T. Okamoto, M. Tada, and A. Miyaji</i>	

Shift Registers

Clock-Controlled Shift Registers and Generalized Geffe Key-Stream Generator	287
<i>A. Kholosha</i>	
Efficient Software Implementation of Linear Feedback Shift Registers	297
<i>S. Chowdhury and S. Maitra</i>	
Comments on a Signature Scheme Based on the Third Order LFSR Proposed at ACISP2001	308
<i>S. Lim, S. Kim, I. Yie, and J. Kim</i>	

Applications – II

Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-Cipher Cryptography	316
<i>L. Shujun, M. Xuanqin, and C. Yuanlong</i>	
Re-dividing Complexity between Algorithms and Keys (Key Scripts)	330
<i>G. Samid</i>	
A Tool Box of Cryptographic Functions Related to the Diffie-Hellman Function	339
<i>E. Kiltz</i>	
Author Index	351

Progress in Cryptology - INDOCRYPT 2001

Second International Conference on Cryptology in India,

Chennai, India, December 16-20, 2001

Rangan, C.P.; Ding, C. (Eds.)

2001, XIV, 358 p., Softcover

ISBN: 978-3-540-43010-0