Table of Contents

Invited Lecture

Cryptographic Functions and Design Criteria for Block Ciphers 1
A. Canteaut

Hashing

Mobile Agent Route Protection through Hash-Based Mechanisms 17
J. Domingo-Ferrer

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

A Parallel Algorithm for Extending Cryptographic Hash Functions 40
P. Sarkar and P.J. Schellenberg

Incremental Hash Function
Based on Pair Chaining & Modular Arithmetic Combining 50
B.-M. Goi, M.U. Siddiqi, and H.-T. Chuah

Algebraic Schemes

Multiples of Primitive Polynomials over GF(2) 62
K.C. Gupta and S. Maitra

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

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

Elliptic Curves

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

Elliptic Curves of Prime Order over Optimal Extension Fields
for Use in Cryptography 99
H. Baier

A Secure Family of Composite Finite Fields
Suitable for Fast Implementation of Elliptic Curve Cryptography 108
M. Ciet, J.-J. Quisquater, and F. Sica

Coding Theory

Frameproof and IPP Codes ... 117
P. Sarkar and D.R. Stinson

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

Applications – I

Selective Receipt in Certified E-Mail ... 136
S. Kremer and O. Markowitch

Spatial Domain Digital Watermarking with Buyer Authentication ... 149
S. Maitra and D.P. Mukherjee

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

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

Cryptanalysis

Cryptananlysis of the Nonlinear FeedForward Generator ... 188
S.S. Bedi and N.R. Pillai

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

Cryptanalysis of Imai and Matsumoto Scheme B Asymmetric Cryptosystem ... 214
A. Youssef and G. Gong

Distributed Cryptography

Robust and Secure Broadcasting ... 223
Y. Mu and V. Varadharajan

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

Boolean Functions

Autocorrelation Properties of Correlation Immune Boolean Functions ... 242
S. Maitra

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

Digital Signatures

A Twin Algorithm for Efficient Generation of Digital Signatures 267
D. Ramesh

Efficient "on the Fly" Signature Schemes Based on Integer Factoring 275
T. Okamoto, M. Tada, and A. Miyaji

Shift Registers

Clock-Controlled Shift Registers and Generalized Geffe Key-Stream Generator 287
A. Kholosha

Efficient Software Implementation of Linear Feedback Shift Registers 297
S. Chowdhury and S. Maitra

Comments on a Signature Scheme Based on the Third Order LFSR Proposed at ACISP2001 308
S. Lim, S. Kim, I. Yie, and J. Kim

Applications – II

Pseudo-random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream-Cipher Cryptography 316
L. Shujun, M. Xuanqin, and C. Yuanlong

Re-dividing Complexity between Algorithms and Keys (Key Scripts) 330
G. Samid

A Tool Box of Cryptographic Functions Related to the Diffie-Hellman Function 339
E. Kiltz

Author Index 351