

Table of Contents

Invited Talks

Linear Complexity and Related Complexity Measures for Sequences	1
<i>H. Niederreiter</i>	

Forensic Computing	18
<i>X. Li and J. Seberry</i>	

Stream Cipher

Hiji-bij-bij: A New Stream Cipher with a Self-synchronizing Mode of Operation	36
<i>P. Sarkar</i>	

Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator	52
<i>S. Paul and B. Preneel</i>	

Block Cipher

Nonlinearity Properties of the Mixing Operations of the Block Cipher IDEA	68
<i>H.M. Yildirim</i>	

Impossible Differential Cryptanalysis for Block Cipher Structures	82
<i>J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, and S. Sung</i>	

Impossible Differential Attack on 30-Round SHACAL-2	97
<i>S. Hong, J. Kim, G. Kim, J. Sung, C. Lee, and S. Lee</i>	

Boolean Function

Construction of Perfect Nonlinear and Maximally Nonlinear Multi-output Boolean Functions Satisfying Higher Order Strict Avalanche Criteria	107
<i>K.C. Gupta and P. Sarkar</i>	

Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria	121
<i>S. Kavut and M.D. Yücel</i>	

Secret Sharing

On Multiplicative Linear Secret Sharing Schemes	135
<i>V. Nikov, S. Nikova, and B. Preneel</i>	
A New $(2, n)$ -Visual Threshold Scheme for Color Images	148
<i>A. Adhikari and S. Sikdar</i>	
On the Power of Computational Secret Sharing	162
<i>V. Vinod, A. Narayanan, K. Srinathan, C.P. Rangan, and K. Kim</i>	

Bilinear Pairing

Identity-Based Broadcasting	177
<i>Y. Mu, W. Susilo, and Y.-X. Lin</i>	
Efficient Verifiably Encrypted Signature and Partially Blind Signature from Bilinear Pairings	191
<i>F. Zhang, R. Safavi-Naini, and W. Susilo</i>	
Extending Joux's Protocol to Multi Party Key Agreement	205
<i>R. Barua, R. Dutta, and P. Sarkar</i>	

Public Key

Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups	218
<i>P.J. Abisha, D.G. Thomas, and K.G. Subramanian</i>	
Prime Numbers of Diffie-Hellman Groups for IKE-MODP	228
<i>I. Yie, S. Lim, S. Kim, and D. Kim</i>	
Polynomial Equivalence Problems and Applications to Multivariate Cryptosystems	235
<i>F. Levy-dit-Vehel and L. Perret</i>	

Signature Scheme

Security Analysis of Several Group Signature Schemes	252
<i>G. Wang</i>	
Forking Lemmas for Ring Signature Schemes	266
<i>J. Herranz and G. Sáez</i>	

Protocol

Practical Mental Poker Without a TTP Based on Homomorphic Encryption	280
<i>J. Castellà-Roca, J. Domingo-Ferrer, A. Riera, and J. Borrell</i>	

Lightweight Mobile Credit-Card Payment Protocol	295
<i>S. Kungpisdan, B. Srinivasan, and P.D. Le</i>	

Elliptic Curve & Algebraic Geometry

On the Construction of Prime Order Elliptic Curves	309
<i>E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis</i>	
Counting Points on an Abelian Variety over a Finite Field	323
<i>F.A. Izadi and V.K. Murty</i>	

Implementation & Digital Watermarking

Side Channel Attack on Ha-Moon's Countermeasure of Randomized Signed Scalar Multiplication	334
<i>K. Okeya and D.-G. Han</i>	
Systolic and Scalable Architectures for Digit-Serial Multiplication in Fields $GF(p^m)$	349
<i>G. Bertoni, J. Guajardo, and G. Orlando</i>	
Cryptanalysis of Block Based Spatial Domain Watermarking Schemes . . .	363
<i>T.K. Das</i>	

Authentication

More Efficient Password Authenticated Key Exchange Based on RSA	375
<i>D.S. Wong, A.H. Chan, and F. Zhu</i>	
A Password-Based Authenticator: Security Proof and Applications	388
<i>Y. Hitchcock, Y.S.T. Tin, J.M. Gonzalez-Nieto, C. Boyd, and P. Montague</i>	
Stronger Security Bounds for OMAC, TMAC, and XCBC	402
<i>T. Iwata and K. Kurosawa</i>	
Progressive Verification: The Case of Message Authentication	416
<i>M. Fischlin</i>	

Author Index	431
------------------------	-----

Progress in Cryptology -- INDOCRYPT 2003

4th International Conference on Cryptology in India,
New Delhi, India, December 8-10, 2003, Proceedings

Johansson, Th.; Maitra, S. (Eds.)

2003, XII, 436 p., Softcover

ISBN: 978-3-540-20609-5