

Table of Contents

LILI to Dragon: from Bit-Based to Word-Based Stream Ciphers	129
Ed Dawson & Leonie Simpson	
AA_β-Cryptosystem: A Chaos Based Public Key Cryptosystem	149
M.R.K. Ariffin & N.A. Abu	
RSA Decryption Techniques and the Underlying Mathematical Concepts	165
Hailiza Kamarul Haili & Norfadhilah Basir	
GCD Attack on the LUC_4 Cryptosystem	179
Wong Tze Jin, Mohamad Rushdan Md. Said, Mohamed Othman & Kamel Ariffin Mohd. Atan	
A New Cryptosystem Analogous to LUCCELG and Cramer-Shoup	191
Norliana Muslim & Mohamad Rushdan Md. Said	
The Beta-Transformation: A Case Study for Chaos Base Cryptography	205
M.R.K.Ariffin & M.S.M.Noorani	
A Faster Version of Rijndael Cryptographic Algorithm Using Cyclic Shift and Bit Wise Operations	215
Fakariah Hani Mohd Ali, Ramlan Mahmod, Mohammad Rushdan & Ismail Abdullah	
Hardware Implementation of RC4A Stream Cipher	225
Abdullah Al Noman, Roslina Mohd. Sidek & Abdul Rahman Ramli	
Improving Security Performance with Parallel Crypto Operations in SSL Bulk Data Transfer	235
Hashem Mohammed Alaidaros, Mohamed Othman & Mohd Fadlee A. Rasid	
A Shift Column with Different Offset for Better Rijndael Security	245
Ramlan Mahmod, Sherif Abdulbari Ali & Abdul Azim Abd.Ghani	