

Table of Contents

A New Public Key Cryptosystem Based on IFS	1
Nadia M. G. AL-Saidi & Mohamad Rushdan Md. Said	
A k-Resilient Identity-Based Identification Scheme in the Standard Model	15
Swee-Huay Heng & Ji-Jian Chin	
Bias in the Nonlinear Filter Generator Output Sequence	27
Sui-Guan Teo, Leonie Simpson & Ed Dawson	
Security Analysis of the Step (D, K) Generator Respect to its Parameters	39
Mehdi M. Hassanzadeh & Tor Helleseth	
Algebraic Analysis of Small Scale LEX-BES	51
Muhammad Reza Zaba, Kenneth Koon-Ho Wong, Ed Dawson & Leonie Simpson	
Conditional Probability Based Camera Identification	63
Ainuddin Wahid Abdul Wahab & Philip Bateman	
One Megabit Random Ambience	73
Nur Azman Abu & Shahrin Sahib	
Detecting Attacks in Encrypted Networks using Secret-sharing Schemes	89
Vik Tor Goh, Jacob Zimmermann & Mark Looi	
FPGA Implementation of Duo- Key- Dependent AES	101
Feng Ying Ying & Bok-Min Goi	