

Table of Contents

Cryptographic Randomness Analysis on Simon32/64	1
Isma Norshahila Mohammad Shah, Hazlin Abdul Rani, Miza Mumtaz Ahmad & Eddie Shahril Ismail	
Rabin-p Key Encapsulation Mechanism for CyberSecurity Malaysia MySEAL Initiative	19
Muhammad Asyraf Asbullah, Muhammad Rezal Kamel Ariffin, & Zahari Mahad	
Enhanced Statistical Analysis Evaluation Using CSM Randomness Test Tool	52
Abdul Alif Zakaria, Hazlin Abdul Rani, & Nik Azura Nik Abdullah	
LED and SIMECK FPGA Implementation	76
Jun-Hoe Phoon, Denis C.-K. Wong & Wai-Kong Lee	
New Vulnerabilities Upon Pomaranch Boolean Function Through Fault Injection Analysis (FIA)	90
Wan Zariman Omar@Othman, Muhammad Rezal Kamel Ariffin , Solahuddin Shamsuddin, Zahari Mahad & Suhairi Mohd Jawi	