Table of Contents

A New Blind Signature Scheme Based On Factoring and Discrete Logarithms **1**

N. M. F. Tahat, E. S. Ismail & R. R. Ahmad

A New Online/Offline Signature Scheme without Key Exposure in the Standard Model **11**

Zhiwei Wang, Shihui Zheng & Yixian Yang

Java Implementation for Identity-Based Identification **21**

Syh-Yuan Tan, Swee-Huay Heng, Bok-Min Goi & Ji-Jian Chin

Garbage-Man-In-The-Middle Attack on the Luc$_4$ Cryptosystem **33**

Wong Tze Jin, Mohamad Rushdan Md. Said, Mohamed Othman & Kamel Ariffin Mohd. Atan

A Method of SSO IN P2P Networks with the Capability of Adaptation at Network Topology Change **43**

Mohammad Reza Sohizadeh Abyaneh, S.Amir Hossein A.E.Tabatabaei & Mahmoud Salmasizadeh

Design Flaws of a Secure Watermarking Scheme for Buyer-Seller Identification and Copyright Protection **55**

Geong Sen Poh & Keith M. Martin

Random Walk Algorithm Based Design Technique for S-Box **65**

S. Kazmi & N. Ikram

Differential Distinguishing Attack of Shannon Stream Cipher **73**

Yaser Esmaeili Salehani, Elham Shakour & S. Mehdi M. Hassanzadeh

Conditions for Counter Measures Against One Time Pad Attack on Baptista Type Chaotic Cryptosystem **93**

M.R.K.Ariffin & M.S.M.Noorani

Crazy: A New 256-Bit Compression Function for Hash Algorithm **103**

Zhimin Li, Bo Yang, Lin Li, Shihui Zheng, Yixian Yang & Zhihui Zhang