Contents

Cryptograph

An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map .......................... 3  
Yuzhen Li, Xiaodong Li, Xin Jin, Geng Zhao, Shiming Ge, Yulu Tian,  
Xiaokun Zhang, Kejun Zhang, and Ziyi Wang

An Improved Cloud-Based Revocable Identity-Based Proxy  
Re-encryption Scheme ................................................................. 14  
Changji Wang, Jian Fang, and Yuan Li

Cryptographic Public Key Length Prediction ................................. 27  
M. Amain and L.M. Batten

An Image Encryption Algorithm Based on Chua’s Chaos  
and Baker’s Transformation .......................................................... 36  
Chupei Chen, Jing Li, and Hongmin Deng

Quantum Differential Cryptanalysis to the Block Ciphers .................. 44  
Hongwei Li and Li Young

An Enhanced Authentication Scheme for Virtual Private Network Access  
Based on Platform Attributes of Multi-level Classification ................. 52  
Xun Chen, Jiqiang Liu, Yanfeng Shi, and Zhen Han

Public Key Timed-Release Attribute-Based Encryption ..................... 65  
Ke Yuan, Nan Shen, Yonghang Yan, Zheli Liu, and Chufu Jia

Color Image Encryption in CIE L*a*b* Space ................................ 74  
Xin Jin, Yingya Chen, Shiming Ge, Kejun Zhang, Xiaodong Li,  
Yuzhen Li, Yan Liu, Kui Guo, Yulu Tian, Geng Zhao, Xiaokun Zhang,  
and Ziyi Wang

Evaluation, Standards and Protocols

Discover Abnormal Behaviors Using HTTP Header Fields Measurement .... 89  
Quan Bai, Gang Xiong, Yong Zhao, and Zhenzhen Li

Reconstruction of Potential Attack Scenarios of the OpenID Protocol  
Towards Network Forensics Analysis ............................................ 101  
Dongyao Ji, Junliang Liu, and Gang Yao
A Lightweight Code-Based Authentication Protocol for RFID Systems . . . . . 114
   Zhuohua Liu, Wei Zhang, and Chuankun Wu

An Overview of Ad Hoc Network Security . . . . . . . . . . . . . . . . . . . . . . . . 129
   Fan Yang, Yulan Zheng, and Ping Xiong

Trust Computing and Privacy Protection

Structural Analysis of IWA Social Network . . . . . . . . . . . . . . . . . . . . . . . . 141
   Wenpeng Liu, Yanan Cao, Diying Li, Wenjia Niu, Jianlong Tan, Yue Hu,
   and Li Guo

A Differentially Private Method for Reward-Based Spatial Crowdsourcing . . 153
   Lefeng Zhang, Xiaodan Lu, Ping Xiong, and Tianqing Zhu

Do Applications Perform Its Original Design? A Preliminary Analysis
   from Internet Big Data . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 165
   Lei Qian, Yinlong Liu, and Yanfei Zhang

Trust Prediction with Trust Antecedent Framework Regularization . . . . . . 177
   Haiyang He, Yong Wang, and Guoyong Cai

Trust Prediction Based on Interactive Relations Strength . . . . . . . . . . . . . . 189
   Guoyong Cai, Liyuan Wang, and Haiyang He

Cloud Security and Applications

You Can’t Hide: A Novel Methodology to Defend DDoS Attack
   Based on Botcloud . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 203
   Baohui Li, Wenjia Niu, Kefu Xu, Chuang Zhang, and Peng Zhang

Quantitative Evaluation Method of Cloud Security . . . . . . . . . . . . . . . . . . 215
   Xinlong Zhao, Weishi Zhang, and Wei Ma

A Large-Scale Distributed Sorting Algorithm Based on Cloud Computing . . 226
   Na Pang, Dali Zhu, Zheming Fan, Wenjing Rong, and Weimiao Feng

Analysis and Exploit of Directory Traversal Vulnerability on VMware . . . . 238
   Yuanyuan Bai and Zhi Chen

OpenStack Vulnerability Detection and Analysis . . . . . . . . . . . . . . . . . . . . 245
   Li Lu, Zhen Han, and Zhi Chen

Tools and Methodologies

RICS-DFA: Reduced Input Character Set DFA for Memory-Efficient
   Regular Expression Matching . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 255
   Qiu Tang, Lei Jiang, Qiong Dai, Majing Su, and Hongtao Xie
A Clustering Approach for Detecting Auto-generated Botnet Domains

Yang Pu, Xiaojun Chen, Yiguo Pu, and JinQiao Shi

Modeling of Mobile Communication Systems by Electromagnetic Theory
in the Direct and Single Reflected Propagation Scenario

Guo Sheng, Shuping Dang, Nadim Hossain, and Xu Zhang

Bayesian Reliability Assessment Method for Single NC Machine Tool
Under Zero Failures

Hongzhou Li, Fei Chen, Zhaojun Yang, Yingnan Kan, and Liding Wang

MIRD: Trigram-Based Malicious URL Detection Implanted with Random
Domain Name Recognition

Cuixen Xiong, Pengxiao Li, Peng Zhang, Qingyun Liu, 
and Jianlong Tan

A Novel NB-SVM-Based Sentiment Analysis Algorithm in Cross-Cultural
Communication

Yuemei Xu, Zihou Wang, and Yuji Chen

Time-Varying Impulsive Anticontrol of Discrete-Time System

Qian Wang, Wei Xiong, and Ya Shuang Deng

Leakage Prevention Method for Unstructured Data Based on Classification

Hao Li, Zewu Peng, Xinyao Feng, and Hongxia Ma

System Design and Implementations

Decryption and Forensic System for Encrypted iPhone Backup Files
Based on Parallel Random Search

Liang Ge and Lianhai Wang

The Method and System Implementation of Unstructured Data Tracking
and Forensics

Guangyu Gu, Shujuan Zhang, Xuefei Wang, Xiang Cai, and Sheng Chen

The Design and Implementation of Data Security Management
and Control Platform

Hong Zou, Yang Qian, Yanshuai Zhao, and Kun Ding

A Data Recovery Method for NTFS Files System

Zewu Peng, Xinyao Feng, Liangliang Tang, and Meijie Zhai

Design and Implementation of Aircraft Pan-Tilt Control System
Based on Mobile Terminal

Minghai Shao, Yingding Zhao, and Jianlong Tan

Author Index
Applications and Techniques in Information Security
6th International Conference, ATIS 2015, Beijing, China,
November 4-6, 2015, Proceedings
Niu, W.; Li, G.; Liu, J.; Tan, J.; Guo, L.; Han, Z.; Batten, L.
(Eds.)
2015, XVII, 398 p. 147 illus. in color., Softcover