

# Contents

## Cryptograph

An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map . . . . .	3
<i>Yuzhen Li, Xiaodong Li, Xin Jin, Geng Zhao, Shiming Ge, Yulu Tian, Xiaokun Zhang, Kejun Zhang, and Ziyi Wang</i>	
An Improved Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme . . . . .	14
<i>Changji Wang, Jian Fang, and Yuan Li</i>	
Cryptographic Public Key Length Prediction . . . . .	27
<i>M. Amain and L.M. Batten</i>	
An Image Encryption Algorithm Based on Chua's Chaos and Baker's Transformation . . . . .	36
<i>Chupei Chen, Jing Li, and Hongmin Deng</i>	
Quantum Differential Cryptanalysis to the Block Ciphers . . . . .	44
<i>Hongwei Li and Li Yang</i>	
An Enhanced Authentication Scheme for Virtual Private Network Access Based on Platform Attributes of Multi-level Classification . . . . .	52
<i>Xun Chen, Jiqiang Liu, Yanfeng Shi, and Zhen Han</i>	
Public Key Timed-Release Attribute-Based Encryption . . . . .	65
<i>Ke Yuan, Nan Shen, Yonghang Yan, Zheli Liu, and Chufu Jia</i>	
Color Image Encryption in CIE L*a*b* Space . . . . .	74
<i>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</i>	

## Evaluation, Standards and Protocols

Discover Abnormal Behaviors Using HTTP Header Fields Measurement . . . .	89
<i>Quan Bai, Gang Xiong, Yong Zhao, and Zhenzhen Li</i>	
Reconstruction of Potential Attack Scenarios of the OpenID Protocol Towards Network Forensics Analysis . . . . .	101
<i>Dongyao Ji, Junliang Liu, and Gang Yao</i>	

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. . . . . 269  
*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 . . . . . 280  
*Guo Sheng, Shuping Dang, Nadim Hossain, and Xu Zhang*

Bayesian Reliability Assessment Method for Single NC Machine Tool  
Under Zero Failures . . . . . 291  
*Hongzhou Li, Fei Chen, Zhaojun Yang, Yingnan Kan, and Liding Wang*

MIRD: Trigram-Based Malicious URL Detection Implanted with Random  
Domain Name Recognition . . . . . 303  
*Cuiwen Xiong, Pengxiao Li, Peng Zhang, Qingyun Liu,  
and Jianlong Tan*

A Novel NB-SVM-Based Sentiment Analysis Algorithm in Cross-Cultural  
Communication. . . . . 315  
*Yuemei Xu, Zihou Wang, and Yuji Chen*

Time-Varying Impulsive Anticontrol of Discrete-Time System . . . . . 326  
*Qian Wang, Wei Xiong, and Ya Shuang Deng*

Leakage Prevention Method for Unstructured Data Based on Classification. . . 337  
*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 . . . . . 347  
*Liang Ge and Lianhai Wang*

The Method and System Implementation of Unstructured Data Tracking  
and Forensics . . . . . 359  
*Guangyu Gu, Shujuan Zhang, Xuefei Wang, Xiang Cai, and Sheng Chen*

The Design and Implementation of Data Security Management  
and Control Platform . . . . . 368  
*Hong Zou, Yang Qian, Yanshuai Zhao, and Kun Ding*

A Data Recovery Method for NTFS Files System . . . . . 379  
*Zewu Peng, Xinyao Feng, Liangliang Tang, and Meijie Zhai*

Design and Implementation of Aircraft Pan-Tilt Control System  
Based on Mobile Terminal . . . . . 387  
*Minghai Shao, Yingding Zhao, and Jianlong Tan*

**Author Index** . . . . . 397



<http://www.springer.com/978-3-662-48682-5>

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

ISBN: 978-3-662-48682-5